tait
communications

TB9100 Base Station
P25 CG Console Gateway
P25 TAG Trunked Analog Gateway

Customer Service Software User's Manual

MBA-00003-21 · Issue 21 · July 2016

Contact Information

Tait Communications
Corporate Head Office

Tait Limited
P.O. Box 1645
Christchurch
New Zealand

For the address and telephone number of regional offices, refer to our website: www.taitradio.com

Copyright and Trademarks

Disclaimer

There are no warranties extended or granted by this document. Tait Limited accepts no responsibility for damage arising from use of the information contained in the document or of the equipment and software it describes. It is the responsibility of the user to ensure that use of such information, equipment and software complies with the laws, rules and regulations of the applicable jurisdictions.

Enquiries and Comments

If you have any enquiries regarding this document, or any comments, suggestions and notifications of errors, please contact your regional Tait office.

Updates of Manual and Equipment

In the interests of improving the performance, reliability or servicing of the equipment, Tait Limited reserves the right to update the equipment or this document or both without prior notice.

Intellectual Property Rights

This product may be protected by one or more patents or designs of Tait Limited together with their international equivalents, pending patent or design applications, and registered trade marks: NZ409837, NZ409838, NZ415277, NZ415278, NZ508806, NZ519742/NZ516280, NZ524369, NZ524378, NZ524509, NZ530819, NZ534475, NZ547713, NZ569985, NZ577009, NZ579051, NZ579364, NZ584534, NZ586889, NZ592624, NZ593888, NZ600346, NZ610563, NZ615954, NZ629167, NZ630718, NZ700387, NZ700908, NZ708662, NZ710766, NZ711325, NZ714188, AU2004216984, AU2015215962, AU339127, AU339391, AU2015904806, EU000915475-0001, EU000915475-0002, UK1518031.8, US 8301682, US13/542147, US14/032876, US14/495334, US14/725922, US14/818712, US14/832420, US62/128101, US62/128129, US640974, US640977, US698339, US702666, US7758996, US7937661, US8902804, US9107231.

This product may also be made under license under one or more of the following U.S. Patents: 5,146,497, 5,148,482, 5,164,986, 5,185,795, 5,185,796, 5,271,017, 5,377,229 and 5,502,767.
The AMBE+2™ voice coding Technology embodied in this product is protected by intellectual property rights including patent rights, copyrights and trade secrets of Digital Voice Systems, Inc. This voice coding Technology is licensed solely for use within this Communications Equipment. The user of this Technology is explicitly prohibited from attempting to decompile, reverse engineer, or disassemble the Object Code, or in any other way convert the Object Code into a human-readable form. Protected by U.S. Patents 5,870,405, 5,826,222, 5,754,974, 5,701,390, 5,715,365, 5,649,050, 5,630,011, 5,581,656, 5,517,511, 5,491,772, 5,247,579, 5,226,084 and 5,195,166.

Environmental Responsibilities

Tait Limited is an environmentally responsible company which supports waste minimization, material recovery and restrictions in the use of hazardous materials.

The European Union's Waste Electrical and Electronic Equipment (WEEE) Directive requires that this product be disposed of separately from the general waste stream when its service life is over. For more information about how to dispose of your unwanted Tait product, visit the Tait WEEE website at www.taitradio.com/weee. Please be environmentally responsible and dispose through the original supplier, or contact Tait Limited.

Tait Limited also complies with the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) Directive in the European Union.

In China, we comply with the Measures for Administration of the Pollution Control of Electronic Information Products. We will comply with environmental requirements in other markets as they are introduced.

Contents

Preface

Welcome to the TB9100 Customer Service Software User's Manual. This manual provides information about the Tait TB9100 Customer Service Software in PDF format. You can view it online or print it to obtain a paper copy. It describes how to use Version 3.91 of the Customer Service Software.

- New users should begin at Part B: Getting Started.
- For explanations of essential concepts, look in Part A: Introduction.
- The rest of the manual assumes that you are familiar with Part C: Basic Tasks.

Associated Documentation

The current set of TB9100 product documentation is provided in PDF format on the product CD. Updates are made available on the Tait support web. Print copies of the documentation are available on request.

Online Help. The CSS also has online Help. It contains more or less the same information as this manual. To view it, start the CSS, then press F1 or click the Help icon on the toolbar. If you are in a dialog box, click the Help button. The Calibration Software also has online Help.

Technical notes are published from time to time to describe applications for Tait products, to provide technical details not included in manuals, and to offer solutions for any problems that arise. The product CD includes technical notes that were available at the time of release. Look for new or updated technical notes on Tait's technical support website.

Typographical Conventions

'File > Open' means 'click File on the menu bar, and then click Open on the list of commands that pops up'. 'Monitor > Module Details > Channel Module' means 'click the Monitor icon on the toolbar, then in the navigation pane find the Module Details group, and select Channel Module from it.'

Please follow exactly any instruction that appears in the text as an alert. An alert provides necessary safety information as well as instruction in the proper use of the product. This manual uses the following types of alert:

This alert is used to warn about the risk of data loss or corruption.

This alert is used to highlight significant information that may be required to ensure procedures are performed correctly, or draw your attention to ways of doing things that can improve your efficiency or effectiveness.

Publication Record

Version	Date	Description
01	January 2005	First release. Describes version 01.00 of the CSS.
07	March 2007	Describes version 3.05 of the CSS. This adds support for the digital fixed station interface, for the P25 console gateway, for RF linking, for the channel coordinator, for monitoring the TCCP interface, and for centralized voting. Updates to feature licenses.
08	November 2007	Describes version 3.12 of the CSS. This adds support for simulcast, trunking interface enhancements, and failsoft mode. Smaller changes include the addition of custom alarms, the ability to set the severity level of heartbeat messages, and the option to stop logging call records.
09	March 2008	Smaller changes for version 3.20 of the CSS. AutoReply option for calling profiles. Synchronized transmit test improvements.
10	April 2008	Describes version 3.25 of the CSS. Revert to Run mode. Subaudible signaling can be superimposed on or included in Tx deviation level. Remembering network element passwords is configurable at install time. Clock synchronization using NTP. CSS command line switches. Allow loopback check box for RF linking.
11	January 2009	Describes version 3.31 of the CSS. Support for the P25 TAG trunked analog gateway. Monitoring and configuring the CSSI interface. Selecting the product type.
12	September 2009	Describes version 3.36 of the CSS and also many version 3.40 features: multiple CTCSS tones or DCS codes, hang time enhancement for digital P25 mode.
13	February 2010	Describes version 3.50 of the CSS. Enhanced CSSI interface for multiple RFSS controllers. Packet data timers.
14	October 2010	Describes version 3.54 (for Trunked) and 3.60 (for conventional) of the CSS. **Version 3.54**: Delaying the decoding of MDC1200 signaling from the analog line is now enabled in the calling profile so that the dispatcher can turn this off and on. Changes to failsoft mode: both failsoft repeaters and failsoft gateways can be in failsoft mode. **Version 3.60**: The data gateway. Configuring and monitoring the data gateway for OTAR (non-DLI OTAR) communications. Querying the data gateway for information about registered radios. **Both versions**: Converter temperatures added to PMU monitoring screen.
15	July 2011	Describes version 3.70 (for Trunked). Monitoring and configuring gateway key management using OTAR. Aux power output on by default when under Task Manager control. Support for system calls. ISSI profiles. CSSI transmission test for trunked analog gateways. Task Manager action to key transmitter. Can carry out transmission test and signal level test simultaneously. Automatic CWID does not pre-empt voice. Group call diagnostics (trunked analog gateway).
16	October 2012	Describes version 3.90 (for use with v3.90 Trunked Analog Gateway only). Static and dynamic channel group views. Changes to CSSI interface monitoring and configuring for the trunked analog gateway to support standard CSSI as well as privileged RFSSs (Group Control Tree and RFSS Voice Protocol). Choice of MIB. Improved NTP information.

Version	Date	Description
17	April 2013	Describes version 3.80 (for Conventional). Unrestricted Wideband software feature license. Other feature license changes. Disabling the MDC1200 mapping table or allowing overlapping ranges. Distributed and switched voting no longer selectable. 1 PPS absent alarm threshold configurable.
18	August 2013	Describes version 3.91 (for Trunked). Transmit if isolated check box. QoS jitter alarm can be triggered by an RF fade. Supplementary services check box is now "Channel Seize After MDC1200" in calling profile. Minor corrections and additions.
19	March 2015	Describes version 3.95 (for Trunked). Added information about satellite and central voter to Transmit if isolated check box.
20	February 2016	Describes version 3.97 (for Trunked). Added Collision Manager field to Network Interfaces > Trunking. Added Console priority field to Network Interfaces > CSSI.
21	July 2016	Describes version 4.00. Changed the descriptopn of the PTT request timeout field in Network Interfaces > CSSI.

Part A Introduction

The Customer Service Software (CSS) is Windows-based software that makes it easy to monitor and configure Tait TB9100 base stations and other Tait P25 network elements. The CSS can also carry out diagnostic tests and update firmware.

The introduction explains fundamental concepts. You need to understand them before you can use the CSS effectively.

Topics

Network Elements

The Tait Customer Service Software is primarily designed to work with TB9100 base stations but it can also work with P25 CG console gateways and with P25 TAG trunked analog gateways. The CSS and its documentation refers to these three items as network elements or as products.

Before connecting to a network element or working with a configuration file, you must click Product on the toolbar and indicate which type of network element the CSS is dealing with. The selected type appears on the status bar and the menu tree disables any items that do not apply.

Different network elements have different interfaces, as shown in the following table. Note that base stations use different interfaces, depending on whether they are in a conventional or a trunked system.

Interface	Base Station (Conventional)	Base Station (Trunked)	P25 Console Gateway	Trunked Analog Gateway
RF	Y	Y	N	N
Channel group	Y	Y	Y	N
Trunking	N	Y	N	Y
Failsoft	N	O	O	N
Analog line	O	N	Y	Y
DFSI	O	N	N	N
CSSI	N	N	N	Y
Key: Y = Yes, N = No, O = Optional				

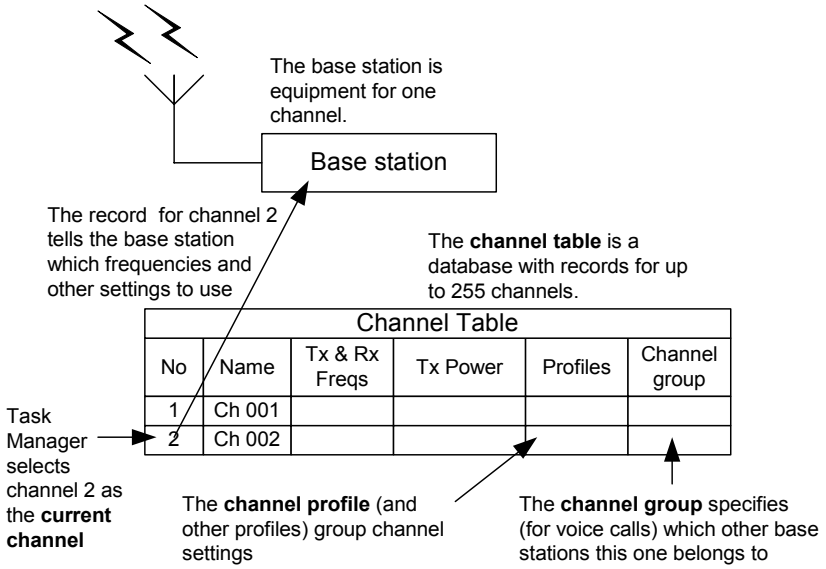
Different network elements also consist of different modules.

Network Element	Channel Module	PMU	PA
Base station	Reciter	O	Y
P25 console gateway	Gateway module	O	N
Trunked analog gateway	Gateway module	O	N
Key: Y = Yes, N = No, O = Optional			

For more information, see "Working With Different Network Elements" on page 41.

Channels

A TB9100 base station consists of the equipment needed to operate on just one channel. However, using the CSS you can program up to 255 channels into a single base station. This is confusing, until you realize that 'channel' has different meanings. The one channel is the transmit and receive frequency pair and the 255 channels are different channel configurations, each with its own number and name. Task Manager selects one of these channel configurations and the base station operates according to the settings in it. These consist of a transmit and receive frequency pair and many other settings, grouped into a number of profiles. The presence of many channels means that base station operation can be modified in any of a large number of ways simply by changing to a channel with the desired settings.



Channel table

Each base station has a channel table. This is the database that stores the channel configurations. It is a good idea to maintain a single channel table for the whole network of TB9100 base stations. This means that almost the same configuration file can be used for all base stations. To configure a new or replacement base station, all you need to do is copy the standard configuration file and make a few modifications, for example to the Task Manager statements that select the current channel. Working from one configuration file simplifies maintenance.

Current channel

The current channel is the channel that the base station is actually operating on. Task Manager action or dispatcher command can select the current channel and Monitor > Interfaces > RF Interface displays it.

Channels in other network elements

All Tait network elements have a channel table and a current channel, even though gateways have no RF interface.

Profiles

Profiles are groups of settings that configure a network element interface.

Channel and signaling profiles

These profiles configure the RF interface. The channel profile determines which modes the receiver supports and (for analog mode) receiver gating and channel properties. The signaling profile determines the NAC, any subaudible signaling, and transmit tail timers.

Calling profile

The calling profile determines the properties of the analog line as a virtual SU: the mode it uses when transmitting, its individual ID, and the group or individual that calls are addressed to. The groups it listens to are determined by the group membership assigned to the calling profile. The calling profile also determines whether calls are encrypted and what key is used.

Channel group

The channel group specifies the group of network elements that this network element belongs to. It determines the multicast IP address that the network element sends to and receives from. It also configures voting.

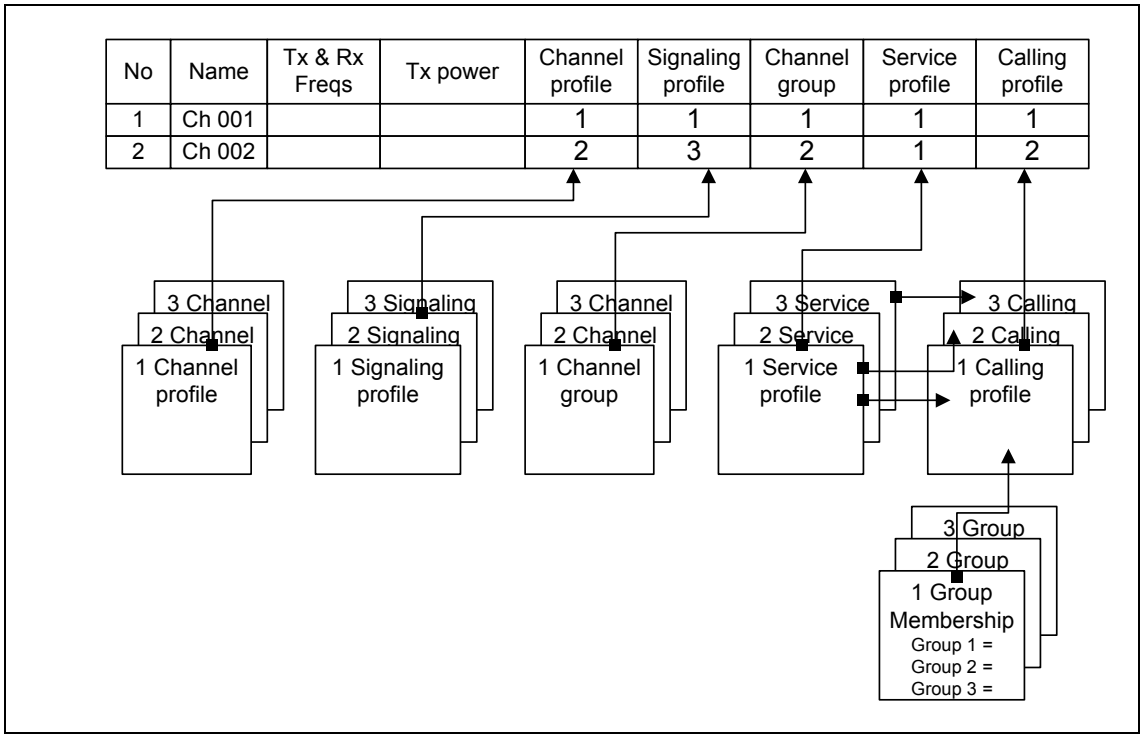
Service profile

The service profile determines which digital P25 services are allowed. One service profile can be applied to the RF input and another to the analog line input.

Assigning profiles to a channel

Each channel in the channel table must be assigned a set of profiles. Using profiles simplifies the work of defining channels. Channels have a large number of configuration settings. Instead of configuring them all each time you set up a channel, you configure sets of them in profiles. Whenever a different setting of a particular configuration parameter is needed, create a new profile. In this way, you establish several profiles for each profile type, any of which can be selected when defining a channel. Figure 1 shows how different profiles could be assigned to channel 2 in the channel table.

Figure 1: Profiles assigned to a channel in the channel table



Receiver Squelch

The base station supports three basic types of squelch operation. In normal squelch, the receiver unmutes if the voice signal has the correct Network Access Code (NAC) or subaudible signaling. Selective squelch unmutes only if the voice signal is addressed to a specific group or individual. Monitor squelch unmutes to almost anything. In addition, for normal and selective squelch in analog FM mode, the receiver only unmutes if the voice signal exceeds the configured RSSI and/or SINAD levels. You set these levels in channel profiles (Receiver gating area).

The following describes the different types of squelch operation and how to configure the TB9100 for them.

Normal squelch

In digital P25 mode, the receiver accepts one particular NAC. When an incoming signal has that NAC, the receiver unmutes. In analog FM mode, the receiver is configured with subaudible signaling (see "Subaudible Signaling" on page 9). The receiver only unmutes if it detects the specified CTCSS tone or DCS code. You select the NAC, CTCSS, and DCS in signaling profiles.

Selective squelch

The base station as a whole does not apply selective squelch. The analog line can, in digital P25 mode. This is necessary, because analog console systems cannot understand P25 signaling. Accordingly, in the analog line's calling profile you can choose selective squelch.

In analog FM mode, selective squelch can be achieved in subscriber units by MDC1200 or Selcall signaling. The analog line simply passes this signaling through. The connected analog console system must provide the selective squelch, only responding if a configured MDC1200 or Selcall address is received.

Monitor squelch

Monitor squelch lets the dispatcher monitor the channel. For received analog FM signals, monitor squelch simply provides the demodulated output, irrespective of its subaudible signaling. For received digital P25 signals, monitor squelch provides any recognizable voice signal addressed to any group or individual. To set up monitor squelch, define a calling profile with normal squelch and use Task Manager to lock the decoding of the NAC and subaudible signaling, so that these squelch mechanisms are bypassed.

Subaudible Signaling

In analog FM mode, the base station can transmit and receive using subaudible signaling. Both CTCSS tones and DCS codes are supported. CTCSS attaches a subaudible tone to the carrier signal. DCS attaches a digital code.

CTCSS tones and DCS codes are referred to collectively as subtones. Both receiver and transmitter can each be configured with up to four different subtones. Subtones make it possible for different groups of users to operate on the same channel without hearing or disturbing each other. The base station and the SUs that use it need to be programmed with the same subtone(s).

In some parts of the world, the use of subtones is regulated. Confirm with the relevant regulatory authority whether and how you can apply subtones.

Assigning subtones

You assign sets of receive and transmit subtones to signaling profiles, then assign a signaling profile to a channel by editing the channel table. When the base station is operating on that channel, it opens the receiver gate to calls if they have a matching subtone and repeats them using the transmit subtone configured for that receive subtone.

Matching DCS codes

Matching the base station's DCS code to the code programmed into a group of SUs can be tricky. This is because the polarity of a DCS code can become inverted. For example, a SU has a DCS code of 017 but the base station may need to be programmed with 050 (017 inverted). Use simple trial and error to see which code works.

Advanced options

When using DCS, the base station always transmits a DCS end tone for muting the receive audio, but transmitting a CTCSS reverse tone burst is optional and configurable.

RF Repeat Function

A repeater re-transmits what it has received on its RF interface. In the base station, this repeat function is enabled by default but it can be disabled or put under the control of the dispatcher. When the repeat function is enabled, a standalone TB9100 repeats what it receives, unless it is handling a call from the dispatcher or the maintainer at the control panel microphone.

Repeat function of a channel group

If the base station is part of a channel group, the repeat function is modified. Instead of only repeating what it receives on its RF interface, the base station repeats the vote-winning signal out of all the valid RF signals that the base stations in the channel group receive. A voting process (each base station has its own built-in voter) selects the signal to repeat. In effect, the channel group is a wide-area repeater; each base station in the channel group repeats the same signal.

If a dispatcher call is in progress, the channel group broadcasts it and does not repeat any SU calls. However, if the channel group is duplex, the vote-winning SU call is forwarded to the dispatcher.

Configuring the repeat function

The repeat function can be enabled or disabled in the channel table.

Alternatively, the repeat function can be put under dispatcher control, so that the dispatcher can turn it on and off as needed. If the dispatch equipment connects via the analog line, the command is a tone remote function tone. A Task Manager task is needed to detect the tone and enable the repeat. If the dispatch equipment is digital and connected via a DFSI, the dispatch command operates directly. For dispatcher control of RF repeat in channel groups, see the TaitNet P25 Conventional System Manual.

It is not possible to configure a TB9100 base station in a channel group to repeat only locally received RF; it must repeat the vote winner. Normally, all base stations in the channel group have the same repeat setting. However, it is possible to generally enable repeat yet disable it in individual base stations (for example, those on solar-powered sites) without disrupting channel group operation.

If pin 1 of the system interface is configured for antenna relay and the receive and transmit frequencies are the same, the base station will not attempt to repeat.

Task Manager

Task Manager is a powerful processing engine that adds intelligence to each network element, enhancing its flexibility and configurability. Part of the firmware running on the channel module's digital board, Task Manager is able to respond to various inputs or operating parameters. Task Manager monitors a wide range of network element parameters. If one of them changes, Task Manager can take appropriate action, for example by changing channel, setting the digital output, or locking a function. A locked function cannot operate.

What action (if any) Task Manager takes depends on the tasks it has been given. Using the CSS, you are able to define these tasks. Tasks are statements in a very simple programming language. Tasks say what action is to be carried out when a monitored parameter changes. All tasks have one of two forms:

IF input, THEN action

IF NOT input THEN action.

For example:

IF **Tone remote detected (550)** THEN **Go to Channel 3**.

This means that when the analog line receives a tone remote function tone of 550 Hz, the network element changes to channel 3.

To define a task, you combine an input with an action, using an intuitive set of drop-down menus. No programming expertise is required. The list of tasks, defined in this way, is the 'computer code' that Task Manager processes. In effect, this means that you can modify the network element's firmware-based operation without needing to compile new firmware.

Task Manager is often used for selecting a channel. Task Manager actions can select a channel whenever the base station enters Run mode, when a tone remote function tone is received from the console system, or when the combined value of selected digital inputs changes.

Task Manager only operates when the network element is in Run mode.

Alarms

The network element monitors a large number of conditions. When a condition rises above or falls below a defined threshold, the network element generates an alarm and stores it in its log. Using the CSS, you can view the current status of all alarms (Monitor > Alarms > Status) and a log containing recent alarms (Monitor > Data Logging > System Log).

You can also disable any alarms that you do not want (Configure > Alarms > Control). Disabled alarms are disabled in the Alarm status form and do not turn on the control panel alarm LED. However, they still generate a syslog message (at the level of Notice) and are inputs into Task Manager.

Most alarms indicate a fault condition, but some are generated by conditions external to the network element, such as mains power failure or high BER on the RF input.

The network element can send alarm (and other) messages to a central message collector.

All alarms are inputs into Task Manager. You can create tasks that tell the network element what to do when an alarm is triggered.

Data Logging

The network element logs events such as alarms, calls, Task Manager actions, and signaling events in syslog format. The **system log** (up to 1000 records) stores events at level Notice and above. The **trace log** (up to 1000 records) stores events at Information level. The CSS can view these logs and save them to a file.

If the TaitNet P25 digital network is set up with a PC running syslog collector software, you can configure the network element to send syslog messages to the syslog collector. In the CSS (Configure > Alarms > Logging), specify the IP address of that PC and select a significance level. Messages with that level or higher are sent and messages below that level are not.

In addition, the CSS has its own log: Application.log (the log of the previous CSS session is Previous application.log). These log files are in the Log Files folder and you can view them in a text editor.

Analog Line

The analog line is a 4-wire E & M interface that is usually used to connect analog dispatch equipment to a single base station, to a P25 console gateway that is part of a channel group, or to a trunked analog gateway that is connected to a trunking controller. The analog line can also be used to connect another base station, external voting equipment, or recording equipment.

TB9100 base stations and gateways have an analog line. The analog line can serve as an encryption/decryption point.

If a network element will use its analog line in digital P25 mode, it needs an analog line license. Additional licenses are required for MDC1200 signaling and for encryption. A P25 console gateway only needs an additional license for AES encryption.

Install-time configuration of the analog line determines the following:

- The type of signaling that is used (E & M, keytone, tone remote function tones, MDC1200).
- The expected characteristics of keytone and tone remote function tones

Calling profiles (assigned to channels but also selectable by the dispatcher) determine the operating configuration:

- Whether calls originating from the analog line are transmitted as analog FM or digital P25 calls.
- What source ID is given to calls originating from the analog line, when they are transmitted in digital P25 mode.
- Which calls are passed to the analog line (which individual ID and group IDs are assigned to the analog line).
- Whether calls are encrypted and which encryption key is used (applies only to gateways).

From the point of view of the radio network, the analog line can be thought of as a logical P25 subscriber unit. It is an end-point for calls. It has an individual ID and can belong to a number of talk groups (however, the trunked analog gateway can only belong to one talk group at a time).

Network Element Security

Security is protected at the network element and at the CSS. The network element is protected through a password. The CSS is protected through access codes to privileges. Both protections are optional.

By default, a network element has no password, but you can use the CSS to give it one. The CSS then optionally remembers the password. Each time you connect to the the network element, the CSS must authenticate itself.

The CSS has three different privileges: Guest, Maintainer, and Administrator. On starting the CSS, you automatically have the Guest privilege. If access codes have been set, when you try to carry out an operation requiring the Maintainer or the Administrator privilege, the CSS asks for the corresponding access code. If access codes have not been set, you automatically have all privileges. An icon on the toolbar indicates your current privileges.

Access codes can be set at installation time or during any CSS session.

The following operations require Maintainer or Administrator privileges:

Operation	**Maintainer**	**Administrator**
Save configuration files	X	
Program configuration	X	
Change mode	X	
Perform diagnostics	X	
Change network element password		X
Reset network element	X	
Edit connections file	X	
Download firmware	X	
Enable additional features	X	
Change privilege access codes		X
Zeroize encryption keys	X	

All other operations only require Guest privilege.

Software Feature Licensing

TB9100 base stations and gateways have many capabilities, but some of them require a license before you can use them. Without any licenses at all, these network elements can communicate with the CSS but can only operate in Standby mode. Using the CSS, you can enable (license) the additional features that are required.

Licensing a feature allows the use of that feature. However, you often need to also enable the feature in configuration using the CSS before that feature becomes operative. The CSS will let you enable or configure a feature even if you do not have a license for it, but the feature will not work.

The following features are available:

Default Radio System The default radio system feature allows the base station to transmit and receive analog FM transmissions.

P25 Common Air Interface The P25 common air interface feature allows the base station to transmit and receive P25 digital voice transmissions.

If neither of the above features are licensed, the network element cannot operate in Run mode.

Analog Line The analog line feature allows the base station to make digital P25 speech calls from the analog line and to pass received digital P25 calls to the analog line. It allows gateways to pass calls between the analog line and the channel group or CSSI interface. This feature is not needed for analog FM mode, for tone remote signaling, or for TSBKs.

Conventional Packet Data Services This feature allows a base station or a P25 console gateway to function as a data gateway in a conventional network, passing packet data between radios and a data server that is connected to the data gateway via a mobile IP router or switch.

MDC1200 Signaling on Analog Line The MDC1200 signaling on analog line feature allows the conversion between MDC1200 signaling and P25 TSBKs. Console systems can then use MDC1200 for ANI and other subscriber signaling to and from SUs that are operating in P25 digital mode. (In analog FM mode, network elements pass MDC1200 on transparently and do not need this feature.)

Transmit Enable TB9100 base stations normally have the transmit enable feature. This allows the reciter to provide a signal for transmitting. Receive-only base stations do not need this feature. Gateways cannot be licensed to transmit.

P25 Trunking Operation The P25 trunking operation feature allows a TB9100 base station to participate in a trunking system. Without this feature, the TB9100 base station cannot provide a control or a status connection to a trunking site controller and it cannot function as a control or traffic channel. The availability of this feature license is restricted.

P25 Base Encryption and Key Loading	The P25 base encryption and key loading feature allows gateways to encrypt and decrypt speech using the DES algorithm.
P25 AES Encryption	The P25 AES encryption feature allows a gateway with a base encryption feature to also encrypt and decrypt speech using the AES algorithm.
SNMP	The SNMP feature allows the TB9100 base station to accept SNMP requests from an SNMP network manager. The TB9100 base station can then provide information from its management information base (MIB) to an external management system.
Digital Fixed Station Interface	The digital fixed station interface feature allows a DFSI connection to a digital dispatch system (fixed station host) in conventional systems. The TB9100 base station or P25 console gateway can then be an interface between its channel group and a digital dispatch system.
Central Voter	The central voter feature allows the network element to act as a central voter within its channel group. This feature also allows voice networking. Only network elements that will centrally vote (normally the central voter and its backup) need this feature. A standard trunked base station (standalone without fill-in repeaters or other channel group members) can function as a master or a failsoft repeater without this license.
Simulcast Transmitter	The simulcast transmitter feature is required in TB9100 base stations that have transmitters and belong to a simulcast network.
Failsoft for P25 Trunking	The failsoft for P25 trunking feature allows trunked channels that become isolated from a site controller to perform simple conventional operation and to interface to a digital dispatch system. If a trunked channel consists of several TB9100 base stations in a channel group, only the central voter (normally the master) needs this license. It is then able to become the failsoft repeater for that channel group.
CSSI Connection	The CSSI connection feature is needed by trunked analog gateways. It allows the gateway to connect to an RFSS controller using the CSSI interface.
Analog FM VoIP Networking and Voting	This feature allows base stations operating in analog FM mode to work together as a channel group. It is an alternative to the other networking licenses for installations that currently do not use digital P25.
Transceiver Network	This feature allows base stations to network together to form a channel group.
20/25 kHz Unrestricted Wideband	The 20/25 kHz Unrestricted Wideband feature license enables the base station to transmit in mid-bandwidth and wide bandwidth channels in the 150-174 MHz and 421-470 MHz frequency bands. The base station is unable to transmit in this way without this feature license, to comply with FCC regulations. This feature license is available to any customer who is not subject to the relevant FCC regulations or has an FCC waiver. Transceiver network "20/25 kHz Unrestricted wideband

Part B Getting Started

To establish a CSS session with a TB9100 base station, connect to it using the CSS software. If the CSS PC is physically connected to a TaitNet P25 digital network, you can connect remotely to any base station in the network.

In a CSS session, you can monitor the base station and carry out diagnostic tests. You can also view and modify its configuration.

The CSS can also work with P25 console gateways and with trunked analog gateways.

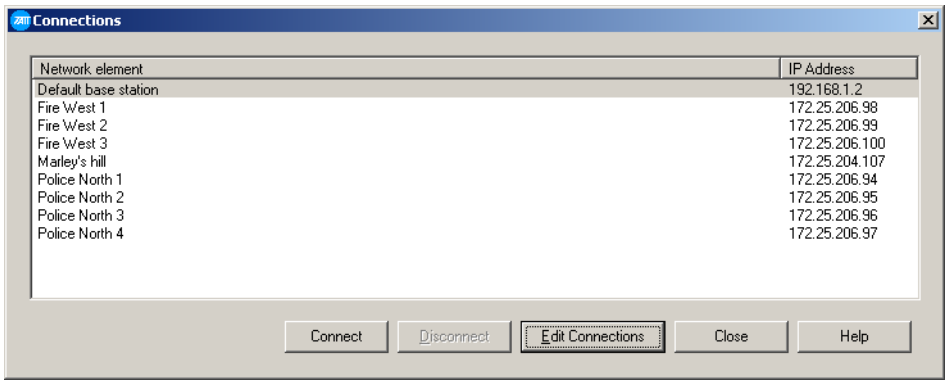
Topics

Connecting

The following instructions describe how to routinely connect a CSS to a TB9100 base station. If you are connecting to a gateway, follow the instructions in "Connecting" on page 29. If you are connecting to a network element for the first time, follow the instructions in the Installation and Operation Manual instead. This manual is available in PDF format on the product CD.

To connect to a TB9100 base station

1. If the CSS is not already running, select Start > Programs > Tait Applications > TB9100 CSS *n.nn.nn* > TB9100 CSS, where *n.nn.nn* is the current CSS version number.
2. Select Product > Base Station to configure the CSS for working with a base station.
3. Make sure that the PC running the CSS is connected via an Ethernet cable to a hub on the TaitNet P25 digital network or directly to the base station's Ethernet interface.
4. On the toolbar, click the **Connect** icon. The Connections dialog box appears.



5. Select a row in the list of network elements. If the base station's IP address has not been changed, select 'Default network element.'
6. Click **Connect**.

   If the CSS asks for a password for the base station and one hasn't been set, just click OK.

   If connecting doesn't work, see "Connecting" on page 29 for more details and for troubleshooting assistance.

   If the CSS establishes a connection to the selected network element, the Status bar displays 'Connected.'

You can now monitor the network element, conduct diagnostic tests, and read and modify the configuration.

Viewing Alarms

When the CSS is connected to a TB9100 base station, it regularly polls the base station for alarms. If an alarm is detected, a flashing Alarms icon appears in the status bar. If the Alarms icon disappears, the CSS has detected that the alarm was cleared.

To monitor alarms

1. Check the status bar. If it has a flashing Alarms icon, click the Alarms button on the toolbar. This opens the Status form.

2. Look to see which LED is flashing red. A flashing LED means that the alarm is on. One problem can set off more than one alarm. A gray LED means that the alarm has been disabled (Configure > Alarms > Control) or that the function it monitors is unavailable.

Many monitoring forms have an Alarm status LED, which indicates whether the module has any active alarms.

Monitoring

Once the CSS is connected to a TB9100 base station, you can monitor various aspects of it.

To view a monitoring form

1. On the toolbar, click **Monitor**. The navigation pane displays a menu of options.
2. In the navigation pane, click a subheading (for example 'Channel Module').

   The main part of the CSS window displays information relevant to the subheading.

Options

- To view the current status of all base station alarms, select Monitor > Alarms > Status.
- To see what is happening at an interface, select an item under Interfaces.
- To see what is happening inside a module, select an item under Modules.
- To see the voting behavior and configuration settings of all channel group members, select Monitor > Channel Group > Status.
- To view the contents of a log that the base station has recorded, select an item under Data Logging.

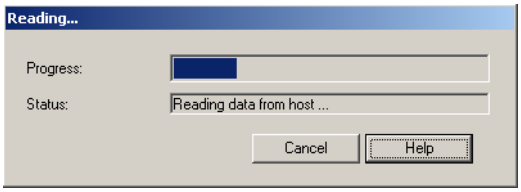
Viewing Configuration Settings

From the CSS, you can view a TB9100 base station's configuration settings. Connect to the base station and then instruct the CSS to read the configuration.

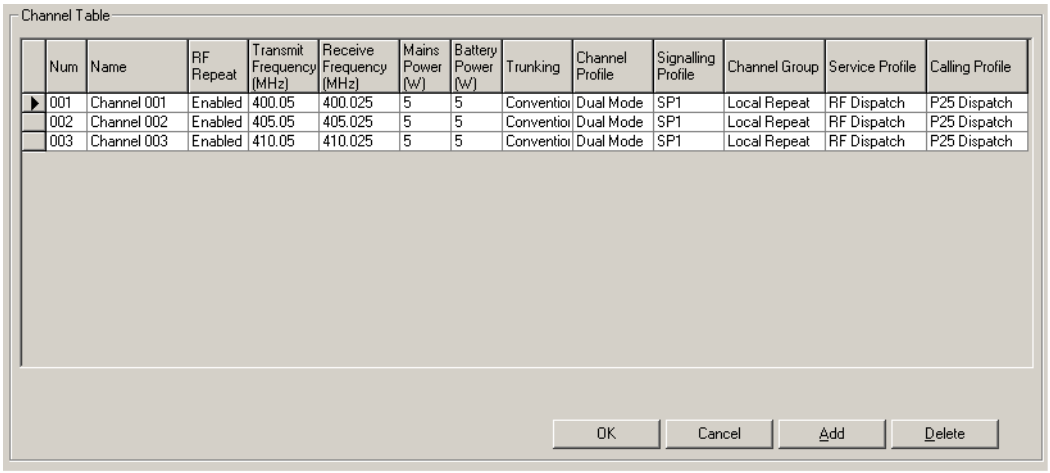
To view configuration settings

1. On the toolbar, click **Read**.

   The Reading dialog box displays progress.



2. On the toolbar, click **Configure**. The navigation pane displays a menu of options.
3. In the navigation pane, click a subheading (for example 'Channel Table'); the main part of the CSS window changes to display the corresponding form.



In this way, you can view any aspect of the base station's current configuration.

Diagnosing Problems

From the CSS, you can carry out a variety of tests on aspects of the base station you are connected to. These can help diagnose any problems you may be experiencing.

To carry out a diagnostic test

1. On the toolbar, click **Diagnose**. The navigation pane displays a menu of options.
2. In the navigation pane, click a subheading (for example 'Transmission Tests'); the main part of the CSS window changes to reflect your selection.
3. If the rectangle beside the **Start Test** button is yellow and gray, click **Standby** on the toolbar to put the base station in Standby mode.
4. Click **Start Test**. View the results of the test on-screen.
5. If necessary, click **Stop Test**.
6. Return the base station to Run mode.

Part C Basic Tasks

Before getting down to the real work on a TB9100 base station or gateway, you need to know how to carry out basic tasks such as setting up a connection, changing mode, and reading configuration information.

The Basic Tasks section explains in detail how to do these and other preliminary tasks.

Topics

Using the Customer Service Software

The following topics describe starting the CSS, the application window, the toolbar and the status bar.

Starting the CSS

To start the CSS software, select Start > Programs > Tait Applications > TB9100 CSS *n.nn.nn* > TB9100 CSS, where *n.nn.nn* is the current CSS version number.

Tip: Run multiple instances of the CSS software on your PC and use them for example to simultaneously monitor alarms at several network elements.

Command Line Options

Command line parameters can be supplied that instruct the CSS to open a configuration file or connect to a particular network element. This makes it possible to write scripts that enable a maintainer to launch the CSS from a network management system and have it connect to the network element of interest.

Option	Action
`CSS.exe /?` or `CSS.exe /h`	Displays information about the command options
`CSS.exe "filename"`	Runs the CSS and opens the configuration file with the specified name. The filename must be enclosed by quote characters. You probably need to include a path with the filename, for example, "C:\Documents and Settings*username*\My Documents\Tait Applications\TB9100 CSS 3.25.00-en\Configurations\config1.apc"
`CSS.exe /I <IP-address> [:<port number>]`	Runs the CSS and connects to the network element with the specified IP address. (`I` = upper case i.) Specifying the port number is optional but is needed, for example, if a router accepts one port number and redirects to another. If a port is not specified, the CSS attempts to connect using the default port 27100.

Selecting the Product Type

The first step in working with a network element or with a configuration file is to select the type of product. This enables the items on the Monitor, Configure, and Diagnose menu trees that apply to the product and disables the others. It has no effect on individual parameters that do not apply to the product.

To select the product

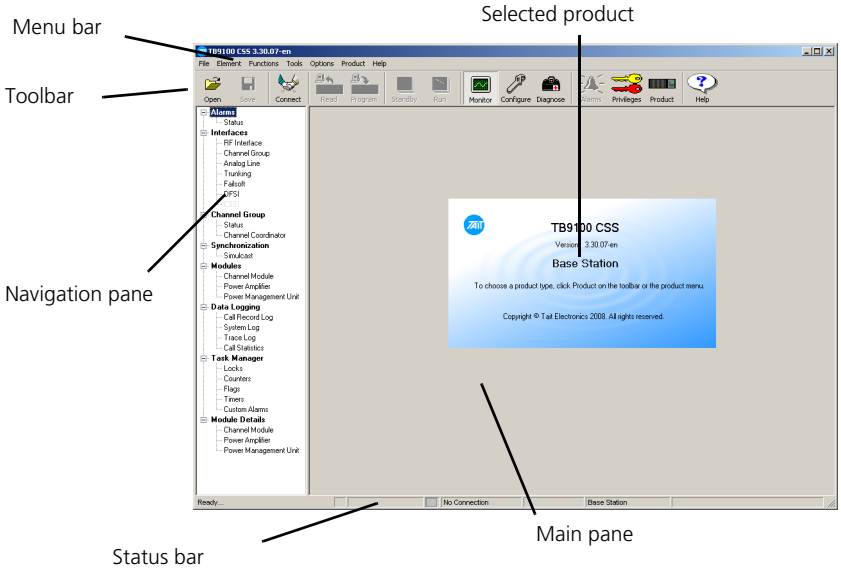
1. Click Product on the toolbar.
2. Select one of the options displayed.

   The type of product you selected appears in the status bar on the bottom of the application window and on the splash screen.

The CSS does not warn you if you select one product type and then connect to a different type.

Application window

When you start the CSS, a splash screen appears, followed by the application window.



By default, the Monitor icon on the toolbar is selected and the navigation pane displays options for monitoring. Click an item in the navigation pane and the main pane displays the corresponding form.

Toolbar

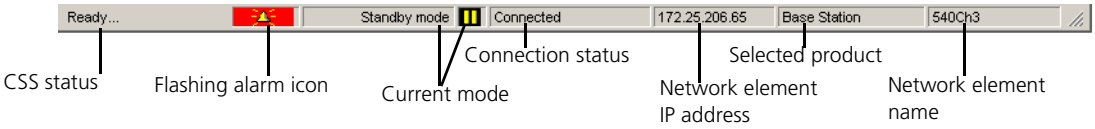
The toolbar gives quick access to commonly used menu commands. For example, instead of selecting Functions > Configure, click the Configure icon on the toolbar.

Open	Opens a dialog box that lets you open a configuration file that is stored on the CSS computer.
Save	Saves the open configuration. When saving a configuration file for the first time, you are asked to give it a name.
Connect	Opens a dialog box that lets you connect to a network element. See also "Connecting" on page 29. If you are connected, this icon displays 'Disconnect.' Click it to disconnect from the network element.
Read	Reads in the configuration information of the network element you are connected to. See also "Working with Configurations" on page 37.
Program	Sends the whole set of configuration information in the CSS to the network element. The network element must be in Standby mode. Once the configuration has been programmed, the network element operates using that configuration. See also "Working with Configurations" on page 37.
Standby	Puts the connected network element into Standby mode.
Run	Puts the connected network element into Run mode.
Monitor	Displays the Monitoring navigation pane so that you can monitor the connected network element. See also "Monitoring" on page 21.
Configure	Displays the Configuration navigation tree, so that you can view and edit configuration information. If a configuration is not already selected, you are first given the option of creating a new configuration, opening an existing one, or reading the network element's current configuration. See also "Viewing Configuration Settings" on page 22.
Diagnose	Displays the Diagnose navigation tree, so that you can carry out diagnostic tests on the connected network element. See also "Diagnosing Problems" on page 23.
Alarms	Turns red when any network element alarm is triggered. Click Alarms to display the current status of all network element alarms. See also "Monitoring Alarms" on page 199.
Privileges	Displays the current privileges. If the keys have the background color, you have Guest privilege. If the upper key is yellow, you have Maintainer privilege. If the lower key is red, you have Administrator privilege. Click Privileges to change privileges. See "Changing Privileges" on page 53.
Product	Displays the different product types that the CSS can work with. Selecting a product type configures the CSS to work with that type. Inapplicable items on the menu tree are disabled. See "Selecting the Product Type" on page 25.

Help	Displays a Help topic for the current form.

Status Bar

The status bar provides useful information that supplements the display in the main pane.



Panels in the status bar provide the following:

- CSS status information, for example whether the CSS is reading or programming a configuration. 'Ready' means that the CSS has completed the last user request and is ready to respond to another request.
- Flashing alarm icon (when an alarm is triggered).
- The mode that the network element is currently in (Run or Standby).
- Whether the CSS is connecting, connected, or not connected to a network element.
- The IP address of the network element.
- The product (network element type) that the CSS is currently configured to work with.
- The name of the network element.

Network Element Operations

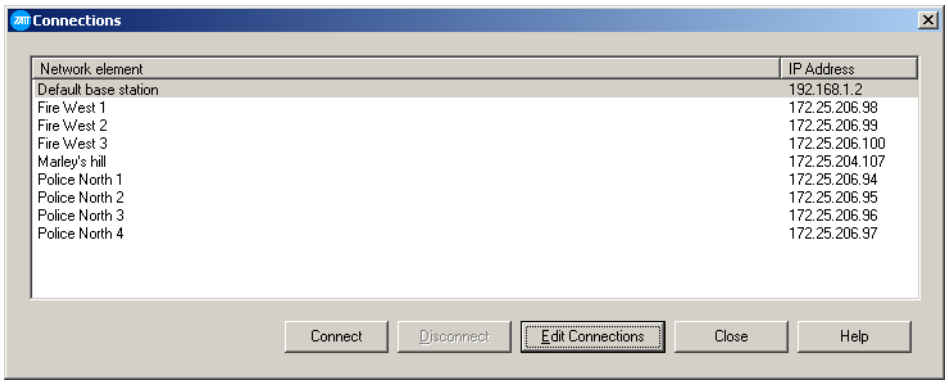
The CSS can connect to any base station or Tait gateway in the TaitNet P25 digital network. Once the CSS is connected, you can change the network element's operating mode or its password. If the network element is not operating correctly, you can reset it.

Connecting

Before you can work with a network element, the CSS must connect to it. A connection establishes a communication session with the network element. Data can go back and forth, for example, to display monitoring information or to carry out a diagnostic test. However, a further step is necessary before you can work with configuration information: you must read the network element or open a configuration file, even to view the configuration forms.

To connect to a network element

1. Make sure that the CSS PC is connected physically to the network element. It can be connected by an Ethernet cable to a hub on the TaitNet P25 digital network or directly to the network element's Ethernet line. For the direct connection, an ordinary or a crossover Ethernet cable can be used; the Ethernet interface supports both.
2. Make sure that the CSS PC has a suitable IP address and subnet mask. The network administrator can help with this. You may need to vary the settings of your local area connection, depending on whether you are on site or in the office. See also "Connecting a Networked PC to a Network Element" on page 31. You may also need to tell the PC how to route to the TaitNet P25 digital network, see "Defining Routes for a Networked PC" on page 30.
3. Run the CSS software.
4. Select the type of product you want to connect to (see "Selecting the Product Type" on page 25).
5. On the CSS toolbar, click **Connect**. The Connections dialog box appears and displays a list of network elements that you can connect to.



6. Click on the row with the network element name and IP address. If the network element is not in the list, click **Edit Connections** and add it. (See "Maintaining the Connection List" on page 43 for instructions).
7. Click **Connect**.

8. If the CSS asks you to provide a password, proceed as follows:
   - If the network element is new, don't enter anything; just click OK. This is because network elements are supplied with a null password. (When you make subsequent connections, the CSS does not ask for a password if it is configured to remember passwords, because it now knows that the network element password is null.)

To set a network element password, wait till you are connected, and then select Element > Change Network Element Password. You can only set the password once the CSS is connected to the network element.

   - Otherwise, supply the password for the network element that you want to connect to. (The CSS asks you to supply the password if it was configured at install time not to remember passwords or if it does not know the network element password.)

To change the CSS configuration so that it remembers network element passwords, you must re-install the CSS.

Once the connection is established, 'Connected' appears in the CSS status bar. If there is a connection icon in the system tray of the operating system, it indicates whether there is any network traffic. Hovering the mouse over it pops up information about the connection speed and the number of packets sent and received.

The network element can only have a single CSS session at any one time. If you are connected, this prevents other CSS users from connecting.

Defining Routes for a Networked PC

You may need to define routes so that the PC uses the correct IP routing path to the TaitNet P25 digital network. Without a correct entry in the network routing table, the CSS will be unable to remotely connect to the network element. To define a route, use the 'route' command. The operating system Help gives assistance on the use of this command.

To define a route

1. Select Start > Run.
2. Enter `cmd`.
3. At the command line prompt, enter `route print`.
4. If the displayed list of persistent routes at the bottom of the output does not provide a route to the TaitNet P25 digital network, add one or more persistent routes in the format:

   `route -p add` *`destination`* `mask` *`subnetmask gateway`*

   For example:

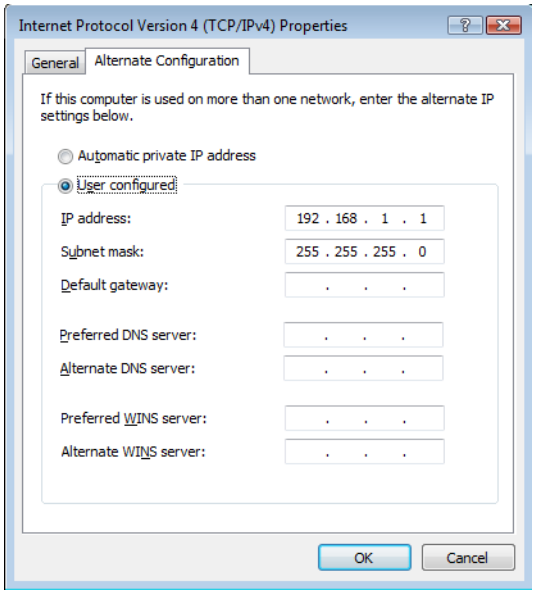
   ```
   route -p add 172.16.16.0 mask 255.255.240.0
   172.25.206.252
   ```

Connecting a Networked PC to a Network Element

You may want to temporarily disconnect a networked PC from its LAN in order to be able to establish a direct connection with the network element. A physical connection is needed as well as an alternate (Windows 7, Windows Vista, Windows XP) or temporary (Windows 2000) IP address and subnet mask.

To connect from a PC with Windows 7 or Windows Vista

1. Remove the local area Ethernet connection and connect an Ethernet patch cable between the PC and the network element. (Either a straight through or crossover Ethernet patch cable may be used with the current network element firmware.)
2. Navigate to Control Panel > Network and Internet > Network and Sharing Center.
3. Click **View status**.
4. In the Local Area Connection Status dialog box, click **Properties**.
5. In the Local Area Connection Properties dialog box, click Internet Protocol Version 4 (TCP/IPv4), and then click **Properties**.
6. Click **Alternate Configuration**.
7. Select the User configured option, and then enter a number that is on the same subnet as the network element. For example, if the TB9100 has IP 192.168.1.2, enter 192.168.1.1 for the PC.
8. Enter a suitable subnet mask, for example 255.255.255.0.

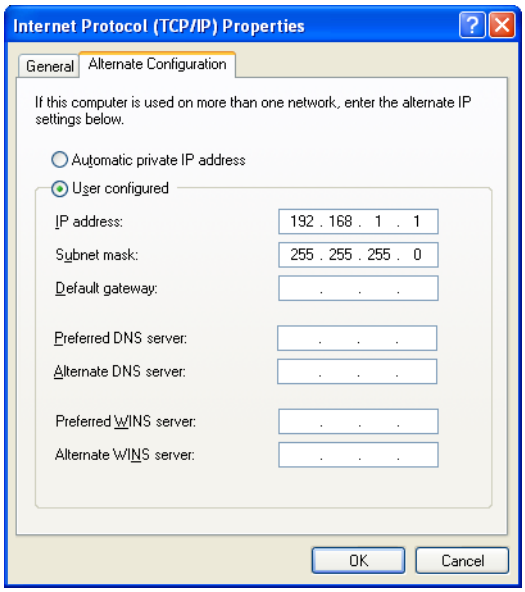


   The CSS should now be able to connect to any physically connected network element that is on the same subnet.

9. Once the CSS session is finished, re-connect the local area network cable to the PC. The PC then uses its normal TCP/IP properties.

To connect from a PC with Windows XP professional

1. Remove the local area Ethernet connection and connect an Ethernet patch cable between the PC and the network element. (Either a straight through or crossover Ethernet patch cable may be used with the current network element firmware.)
2. Click Start > Control Panel.
3. Double-click **Network Connections**.
4. Double-click the Local Area Network icon.
5. Click **Properties**.
6. Click Internet Protocol (TCP/IP), and then click **Properties**.
7. Click Alternate Configuration.
8. Select the User configured option, and then enter a number that is on the same subnet as the network element. For example, if the TB9100 has IP 192.168.1.2, enter 192.168.1.1 for the PC.
9. Enter a suitable subnet mask, for example 255.255.255.0.



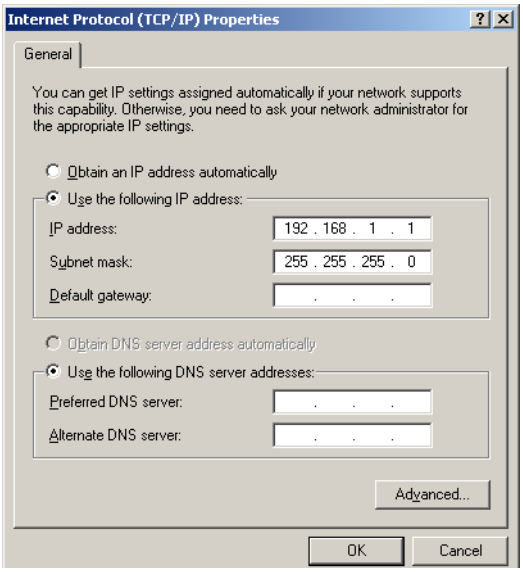
   The CSS should now be able to connect to any physically connected network element that is on the same subnet.

10. Once the CSS session is finished, re-connect the local area network cable to the PC. The PC then uses its normal TCP/IP properties.

To connect from a PC with Windows 2000

1. Remove the local area Ethernet connection and connect an Ethernet patch cable between the PC and the network element. (Either a straight through or crossover Ethernet patch cable may be used with the current network element firmware.)
2. Select Start > Settings > Network and Dialup Connections.
3. Double-click the Local Area Connection icon.
4. Click **Properties**.
5. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
6. Note the current settings so that you can restore them later.

7. Select **Use the following IP address**, and then enter a number that is on the same subnet as the network element. For example, if the base station has IP 192.168.1.2, enter 192.168.1.1 for the PC.
8. Enter a suitable subnet mask, for example 255.255.255.0.



The CSS should now be able to connect to the network element.

9. When you have finished the CSS session, re-connect the local area network cable to the PC and then restore the original PC configuration. When you close the Network connection dialog box, the restored configuration is applied.

Troubleshooting Connection Problems

If the attempt to connect to a network element failed, consider these possible causes.

1. The CSS PC is part of your organization's LAN and does not belong to the same subnet as the network element. Give the PC a suitable IP address and subnet mask as described in "Connecting a Networked PC to a Network Element" on page 31.
2. You have just switched the network element on and it is not yet ready. Try again.
3. Another CSS is connected to the same network element. A message is displayed indicating this.
4. Another CSS was connected to the same network element and the session did not complete properly. Wait one minute and try again.
5. You have just calibrated the network element. The network element is still in calibration mode and cannot respond to connection requests. Reset the network element.
6. You are attempting to connect to the wrong IP address. Check that the IP address is correct.
7. The network element is not yet using the IP address you are attempting to connect to. A previous session changed the network element's IP address. The network element configuration specifies the new address but the network element is still using the old IP address. Reset the network element.
8. The link to the network element is down. Use ping to check.

9. A router on the link uses network address translation. You need to connect using the router IP address, not the network element IP address. Also, you may need to connect using a port number other than the default.
10. The firewall is blocking access to the network element. Ask the system administrator to give you access.

Loss of Connection

The CSS can lose connection with a network element for various reasons. If the CSS receives the error message "Reciter reported that the last request had an invalid Session ID," a second CSS session originating from the same PC has superseded the original session.

If the network element already has a session with a PC, it will prevent a connection attempt by a different PC but is not able to do this if the connection attempt comes from the same PC.

Disconnecting

When you have finished working with a network element, click Disconnect on the toolbar. Alternatively, press F9 or select Element > Disconnect. You are now ready to connect to another network element.

If the network element is in Standby mode, the CSS reminds you of this and asks you to confirm that you want to proceed. This is to make sure that you do not inadvertently leave the network element out of service after a CSS session. Select No to cancel disconnecting, and then change the network element's mode back to Run before disconnecting.

Changing Mode

Normally, the network element operates in Run mode. However, some functions are only available in Standby mode.

- Run mode is used for normal operation.
- Standby mode takes the network element out of service. It is required if you want to program a configuration into the network element or carry out invasive diagnostic tests (for example to determine the lock range). In Standby mode, a TB9100 base station cannot repeat across its RF interface or send and receive on the digital line. This means that SUs cannot talk to or hear each other. Dispatchers and SUs also cannot talk to or hear each other. However, the control panel is still effective; the maintainer can talk to and hear SUs. If the base station's channel group interface is duplex, the maintainer can also talk to and hear any dispatcher connected to the analog line.

If the network element is still in Standby mode when you end a CSS session, you are asked to confirm. This is so that you do not inadvertently leave the network element out of service.

To put a network element in Standby mode

1. Connect to the network element.

2. On the toolbar, click **Standby**. You are asked for confirmation.

   Once the network element has gone into Standby mode, the status bar displays the Standby icon. Functions such as programming a configuration into the network element are now enabled.

To put a network element in Run mode

1. If necessary, connect to the network element.
2. On the toolbar, click **Run**.

   After a few moments, the status bar displays Run mode. The network element is now in service, although it may take a further ten seconds before it can handle calls over the Ethernet interface.

   If the network element cannot go into Run mode, the CSS displays an error code.

   Error codes 1 and 2: Check to see which alarms are displayed and take appropriate action.

   Error code 4: return the channel module to Tait.

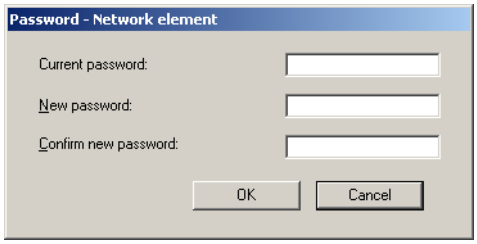
   Error code 10: The network element does not have the licenses that enable it to operate in Run mode. Obtain one or more licenses and use the Software Feature Enabler to let the network element operate in analog FM and/or digital P25 modes.

Assigning a Network Element Password

Each network element can be given a password to safeguard access to it. A CSS must know the password before it is able to connect to the network element. If you do not give the network element a password, any CSS can connect to it. If you assign or change a password, users of other CSS PCs will need it before they can connect to the network element.

To assign or change a network element password

1. Connect to the network element.
2. Select Element > Change Network Element Password.
3. If requested, provide the Administrator access code. The Password - Network Element dialog box appears.



4. If you are changing an existing password, enter that password. Otherwise leave the **Current password** box empty.

If the network element password is lost, contact your Tait dealer.

5. Enter the new password.
6. Re-enter the password in the next box.
7. Write down the new password and do not lose it; there is no other way to find out what a password is.

8. Click **OK** to change the password and close the dialog box. The CSS sends the password to the network element and stores it in an encrypted form. It will use this password to authenticate itself when establishing a connection to the network element.
9. Inform any other CSS users of the password.

Resetting the Network Element

The CSS can remotely reset the network element. This may become necessary if the network element stops functioning properly.

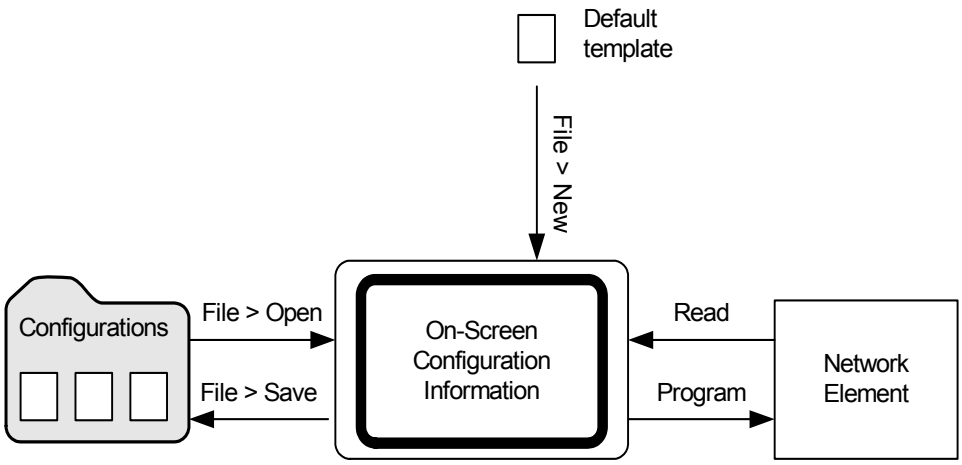
1. Select Element > Reset Network Element.
2. Wait for the network element to restart, and then connect to it again. Attempts to connect before the control panel LEDs have been turned off for at least 10 seconds will fail.

Working with Configurations

Network elements are programmed with many configuration settings. Using the CSS, you can view these settings, change them, and then program them into the network element.

- Configuration works differently from other CSS functions. Once you are connected to a network element, you can monitor it but you can't yet view its configuration. First you must click the Read icon, which instructs the network element to supply its configuration information.
- Programming the network element with a new configuration can only be done when the network element is in Standby mode.
- It is a good idea to always save a configuration to file immediately before programming it into a network element.
- Before reading or programming, connect to a complete channel, not just to the reciter or gateway module. Alarm thresholds, power configuration, and PA fan control settings are stored in the PA or PMU. If these are not connected, default values are read and your settings are not programmed.
- The CSS can obtain configuration information from a network element, from a configuration file on disk, or from the default configuration template.

Figure 2: Obtaining and storing configuration information



Creating a New Configuration

You can create a new network element configuration from scratch, modify it, and save it as a new configuration. This means that you can define a configuration without being connected to a network element. This is a good way to learn how to use the configuration part of the CSS program. It also means that you can do all the work of configuring before a network element is delivered. When the network element arrives, you just open the configuration file and program it in. (This method completely overwrites the network element's current settings.)

To create a new configuration

1. Select File > New.
2. Click **Configure** in the toolbar and make the desired configuration changes.
3. Select File > Save As, give the configuration a name, and save it.

Reading a Network Element Configuration

Before you can view a network element's configuration settings, the CSS must read them.

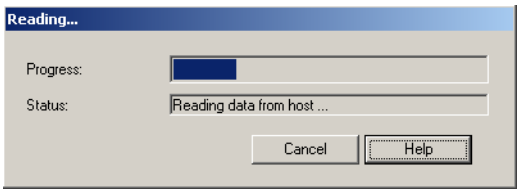
If the CSS has an open configuration file, save it first; reading a configuration overwrites any configuration that the CSS has in memory.

To read a configuration

1. Connect to the network element.
2. Click **Read**.

   The CSS reads the network element's configuration information.

   The **Reading** dialog box displays progress and gives you the option of canceling the process.



Once reading the configuration is complete, click **Configure.** You can now view the current configuration settings, make any configuration changes, and save the configuration settings to a file. You can also put the network element into Standby mode and program it with the new settings.

Saving a Configuration

It is a good idea to regularly save your current configuration settings as you work on them. Save them just before you program them into a network element. This gives you a backup, in case the network element fails or the configuration is corrupted.

To save configuration settings

1. After making any changes to configuration settings, click **OK** to confirm them.
2. Click **Save** on the toolbar.

   If the configuration settings are already named, they are saved. If not, the Save File As dialog box appears. Continue as follows:
3. Enter a name for the configuration file into the **File name** box.
4. To save the configuration file somewhere other than in the Configurations folder, navigate to another folder.
5. Click **Save**. The file name appears on the CSS title bar.

Programming a Configuration into a Network Element

Any configuration changes made using the CSS only take effect once they have been programmed into the network element. Programming only affects the settings that you can view after clicking **Configure**.

To program a configuration into a network element

1. If you have made any changes to the current form, click **OK** to confirm them.
2. Make sure that the current configuration settings displayed in the CSS are what you want.
3. Connect to the network element (if you aren't already).
4. Put the network element into Standby mode.
5. Select File > Save to create a copy of the configuration settings as a file in the Configurations folder.
6. Click **Program**.
7. If the error message "Reciter reported that the last request had an invalid Session ID" appears, the CSS session has been superseded. See "Loss of Connection" on page 34 for more information.
8. If the configuration in the CSS has a different IP address or subnet mask to that of the network element, you are asked for confirmation. Click **Overwrite** to change the network element's IP address or subnet mask. Click **Keep Existing** to program the configuration into the network element but keep the network element's existing IP address and network mask.

   The Program dialog box appears and indicates the download progress. When the network element has successfully received all the configuration settings and programmed them in, the dialog box closes.

   If the download is not completely successful, programming is aborted and a message appears. Later, you can open the file you saved and try again.
9. If you changed the network element's IP address or subnet mask, reset the network element so that the new parameters take effect.
10. Return the network element to Run mode.

Synchronizing a Configuration File

Synchronizing a configuration file with the configuration on a network element makes sure that the file has the same settings as are in the network element itself.

Tip: Synchronizing a configuration file is the quickest way to make a network element's configuration available to the CSS.

To synchronize a configuration file

1. Select File > Open and open the configuration file for the network element.
2. Connect to the network element and click **Read** on the toolbar.
3. Save the file.

Handling Older Configuration Versions

If you read a network element configuration (or open a configuration file) and its version is older than the CSS, a warning appears. This is because the CSS and the network element communicate configuration and monitoring data based on a database with a defined structure. If the network element and the CSS have the same version, they share the same database structure.

Generally speaking, it is best to use a CSS with the same version as the network element that you intend connecting to. Use an older CSS whose version matches the network element, or upgrade the network element firmware to match the CSS.

If you continue to work with an older configuration, the following occurs.

Reading an older configuration

If you read a configuration from an older network element:

- The CSS displays new data items and gives them default values.
- The CSS cannot display data items that have been removed from the newer database. You cannot view or change them.

Programming

If you program this configuration back into the network element, the following occurs.

- The network element cannot store or use new items. They are ignored.
- Data items that are no longer supported by the new CSS remain unchanged.

If you save the configuration, the CSS saves it in the new configuration version.

Handling Newer Configuration Versions

If you read a network element configuration (or open a configuration file) and its version is newer than the CSS, a warning appears. This is because the CSS and the network element communicate configuration and monitoring data based on a database with a defined structure. If the network element and the CSS have the same version, they share the same database structure.

Generally speaking, it is best to use a CSS with the same version as the network element that you intend connecting to. Install the new CSS and use it; you can have many different CSS versions on your PC at the same time.

If you continue to work with a newer configuration, the following occurs.

Reading a newer configuration

If you read a configuration from a newer network element:

- The CSS cannot display new data items.
- The CSS displays data items that the network element no longer supports and gives them default values.

Programming

If you program this configuration back into the network element, the following occurs.

- The network element cannot store or use the data items that it no longer supports. They are ignored.
- New data items remain unchanged.

If you save the configuration, the CSS saves it in the old configuration version.

Working With Different Network Elements

The CSS can monitor, configure, and carry out diagnostic tests on different TaitNet P25 network elements. Network elements include various types of TB9100 base station, P25 console gateway, and trunked analog gateway. These in turn consist of various module combinations. The following gives some guidance on how to use the CSS with different module combinations.

Single-channel base station

For a subrack with a PMU and a single reciter and PA, there are no special considerations.

Gateways

The P25 console gateway and the trunked analog gateway have a channel table and profiles, just like a TB9100 base station. However, there is no RF interface and no PA. When you select a gateway product, forms that configure or diagnose the RF interface are disabled but the other forms are unchanged, even if many parameters within them do not apply. Like a TB9100, the gateways operate on a channel selected by Task Manager action. The trunked analog gateway is not a member of a channel group. For both gateways, the selected channel specifies the default calling profile.

PMU

If present, the PMU is associated with channel module 1 (the right-most reciter or gateway module in the subrack, looking from the front). When the CSS is connected to another channel module, it cannot monitor, configure, or diagnose the PMU. The Alarm Status form will report 'No PMU detected' and other PMU alarm LEDs will be gray. Power configuration settings (Configure > Network Element > Miscellaneous) are editable, but have no effect. PMU control tests also have no effect.

- Disable the 'No PMU detected' alarm for channel modules other than channel module 1.
- Make sure that any Task Manager actions involving the PMU are programmed into channel module 1.
- If there is no PMU, disable the 'No PMU detected' alarm on all channel modules.

PA

Gateways and base stations that are receive-only have no PA. The Alarm Status form will report 'No PA detected' and other PA alarms will be gray. PA control tests have no effect.

- Disable the 'No PA detected alarm (Configure > Alarms > Control). This stops the control panel alarm LED flashing because of this alarm.

Fan alarms

Fan alarms are passed from the fan via the control panel to the channel module that is currently selected on the control panel. The CSS cannot monitor fan alarms if it is connected to a different channel module. The display of fan states in Diagnostic forms will only be correct for the currently selected channel module.

- Make sure that any Task Manager actions involving the fans are programmed into channel module 1.
- Disable the Fan failed' alarm for any fan that is not fitted.
- Disable the PA 'Fan failed' alarm for all channel modules, except (if it has a PA) reciter 1.

- Disable the PMU 'Fan failed' alarm for all channel modules, except (if there is a PMU) channel module 1.
- We recommend that you select channel 1 on the network element's control panel, so that fans can be remotely monitored by connecting a CSS to channel module 1. (Other channel modules can be selected during on-site monitoring and diagnostics.)

CSS Tools

The Tools menu gathers together less commonly used operations.

Maintaining the Connection List

Select Tools > Connections to open the Connections List dialog box. This is a simple text editor for maintaining the list of network elements that the CSS can connect to. This list is stored in the host information file (conncfg2.dat).

To add a network element to the list

1. Select Tools > Connections.
2. In the Connection List, enter the name of the network element and its IP address. The entry should have the following format:

   Network element name = 172.25.206.26
3. If the path to the network element uses port forwarding, you may need to specify a port number as well, for example:

   Network element name = 172.25.206.26:27200

   (If no port number is specified, the CSS uses the default of 27100. Tait network elements always listen for CSS communications on that port.)
4. To avoid confusion, make sure that the name you enter into the connection list is the same as the one programmed into the network element (Configure > Channel Group > Network Identity).
5. If desired, copy the file containing the connection list to other PCs that run CSS.

Alternatively, use any text editor to edit the conncfg2.dat file. You can find this file in C:\ProgramData\Tait Applications\TB9100 CSS (Windows 7), C:\Users*username*\AppData\Tait Applications\TB9100 CSS (Windows Vista) or C:\Documents and Settings\All Users\Application Data\Tait Applications\TB9100 CSS (Windows XP and Windows 2000). The connection list file for earlier CSS versions is conncfg.dat.

> You may need to configure the operating system to "Show hidden files, folders, and drives" to access this file.

Firmware Download

You can use the CSS to update the firmware of network element modules. This is a two-stage process. First the CSS downloads the firmware to the network element (this can be done in Run mode and does not affect network element operation). Then the network element takes itself out of service and activates the downloaded firmware. After activation, the network element resets itself.

> The CSS cannot update the network board's operating system kernel and some of its firmware. These items must be updated using TFTP, see TN-977b.

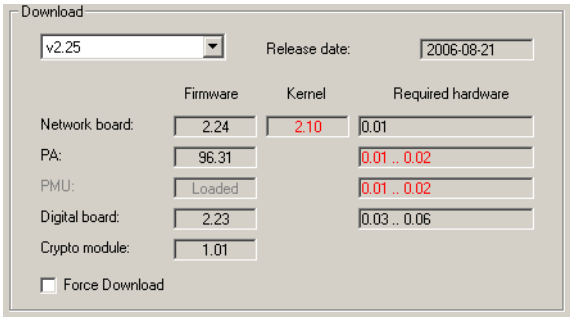
The network element is supplied with all necessary firmware, but it may become desirable to upgrade to a newer version. It is also possible to downgrade a module to an older firmware version to ensure compatibility with other network element modules. The release notes contain a compatibility table indicating the hardware versions that are compatible with any particular firmware version. The CSS also prevents the downloading of firmware that would lead to incompatibility between firmware and hardware or between modules.

Firmware Download Form

The Firmware Download form (Tools > Firmware Download) displays information about the versions installed on the network elements and in the set of firmware that you select. You can initiate a download and monitor its progress.

Download

Use the Download area to select a set of firmware for downloading. The area displays information about the firmware in the selected set and the hardware that it is compatible with.



In the list box, select a set of firmware. The drop-down list displays the available firmware sets. (The CSS looks for firmware files in the folder specified by Options > File Folders.)

The rest of the Download area displays version numbers of the individual items of firmware in the selected set: Network board, power amplifier, power management unit, digital board, and crypto module (gateways only). It also shows the versions of hardware that the firmware can work with.

When you install the CSS, firmware for the different network element modules is copied into a folder that different CSS versions can access. A compatibility file is also copied over. Firmware versions are also available from the Tait support website.

Firmware

The version of the firmware in the set of firmware that you selected. 'Loaded' instead of a version number means that the firmware version in the selected set is the same as the firmware version already installed in the connected network element.

Kernel

The version of the network board's operating system kernel that is required for working with the network board firmware. A '-' means that there is no particular kernel version required. 'Loaded' means that the kernel version required is present on the connected network element. A red version number means that the kernel version installed on the connected network element is incompatible with the network board firmware in the firmware set you selected. To upgrade the kernel, follow the instructions in TN-977b. This also upgrades the network board firmware.

Required hardware

The range of version numbers of hardware that is compatible with the corresponding firmware. Version numbers below the minimum or above the maximum displayed are not compatible.

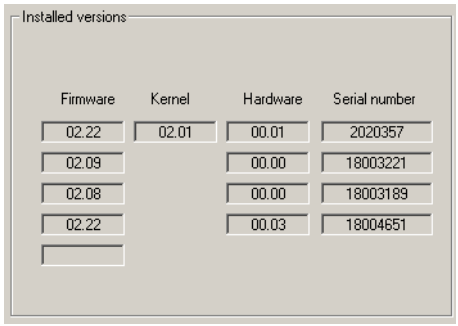
If the version numbers are displayed in red, the firmware version in the selected set is incompatible with the hardware or kernel version of the connected network element. You are unable to download.

Force download

Enable the Force download check box to repeat the download of a firmware version. When the Force download check box is selected and you click Download, all firmware files in the set are downloaded. When the check box is cleared, firmware files that display 'loaded' are not downloaded.

Installed Versions

The Installed Versions area displays the version numbers for firmware, kernel, and hardware that are currently installed in the connected network element. It also displays the serial numbers of each module, so that you can check that you are connected to the correct modules.



Downloading Firmware

A set of firmware files is copied into the CSS's Firmware Files folder at installation. More recent firmware can be obtained from the Tait support website. Copy the file containing the set of firmware (firmware.exe) to the Firmware Files folder (the default location is C:\Program Files\Common Files\Tait Programming Applications\TB9100 CSS\Firmware Files) and run it to extract the individual firmware files.

Save a backup copy of the network element configuration before downloading firmware. This is a precautionary measure; the backup may be needed if the firmware download does not successfully complete on the first attempt.

In dual base stations, downloading firmware to one base station can cause the second base station to temporarily go out of service. If the PMU firmware is part of the download package, loading this into PMUs with serial numbers prior to 18153132 causes the supply voltage to PAs to drop to around 26 V, causing the other base station's PA to raise a Supply voltage low alarm and to cease transmitting. Normal operation resumes automatically once the firmware is downloaded and activated.

If the PMU is older (shipped as part of a base station earlier than version 3.30), a firmware upgrade will cause a brief interruption of the auxiliary power output. This occurs even if the PMU firmware itself is not upgraded.

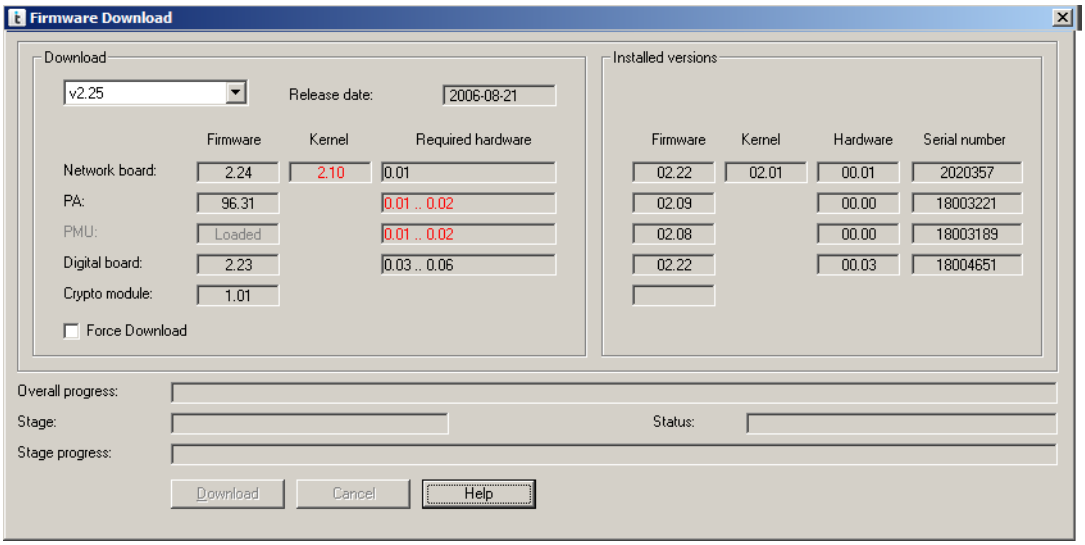
The output is interrupted from the beginning of the firmware download until Run mode is entered after the reset (PMU firmware is upgraded), or from the beginning of the reset until Run mode is re-entered (PMU firmware is not upgraded).

This interruption can cause equipment that relies on the auxiliary power output, such as an external reference, to also reset. Resetting the external reference can even cause all the other base stations that use the same external reference to reset.

You can prevent the interruption of power to other equipment by connecting auxiliary outputs from more than one PMU in parallel and upgrading firmware one base station at a time.

To download new network element firmware

1. Run the CSS software and connect to the network element.
2. Read the network element's configuration and save it to a file, so that if necessary, you can restore it manually (see "Manually Updating the Configuration" on page 48).
3. Select Tools > Firmware Download. The Firmware Download dialog box appears.



The CSS obtains information about the network element's modules and displays it in the Current versions area.

4. Under **Download**, select the firmware file set you want to download. The version numbers of each firmware item in the set appear in the Download area. If the firmware item is already downloaded and activated, its display is disabled and shows 'Loaded.'
5. If version numbers in the Required Hardware column appear in red, the selected firmware is incompatible with the network element's current hardware. You cannot download the firmware.
6. If the Kernel version appears in red, you must first update the kernel. For instructions, see TN-977b.
7. Click **Download**.

   The CSS downloads firmware for the modules you selected. This is a background activity and can proceed while the network element is in Run mode. The bottom of the dialog box indicates progress.

   The network element sends its configuration to the CSS, which temporarily stores it. The network element then goes into Standby mode and activates the downloaded firmware by programming it into flash memory. The network element resets itself. The CSS waits 30 seconds for the network element to get up and running, and then re-establishes the connection and loads the stored configuration back into the network element, adding any new data items used by the new firmware.
8. When the CSS asks you whether to overwrite the network identity or keep the existing network identity, choose overwrite, otherwise the network element will have a default identity instead of its identity in your network.

   Once the stored configuration is loaded, the network element begins operating with the new firmware and returns to Run mode.

If the activation of a module fails, an alert informs you of this. If you have no backup of the current configuration, contact your Tait dealer. If you do have a backup, repeat the download procedure. When that is completed, you must manually restore the configuration, see "Manually Updating the Configuration" on page 48.

9. Re-open the Firmware Download form and verify that the network element has the new firmware versions.
10. Check the Release Notes for new data items added by the firmware upgrade. New data items are given default values designed to give safe, expected behavior, but in particular systems they may have undesirable effects. Check that they are appropriate and change them if necessary.
11. Save the configuration (do not overwrite the old configuration file) and program it back into the network element.
12. If you upgraded the network board firmware or kernel, re-load any encryption keys. (A firmware upgrade zeroizes any stored encryption keys.)

Manually Updating the Configuration

If you needed to repeat the download procedure, the network element's configuration is probably unusable and must be restored from backup. After repeating the download, follow these steps.

1. Using the new CSS, open the backed-up configuration file. The CSS adds any new data items to the configuration, so that its database structure matches that of the new network element firmware.
2. Check the default settings of any new data items (information in the Release Notes) and change any that do not suit the system.
3. Save the configuration (do not overwrite the old configuration file) so that you have a backup.
4. Program the configuration back into the network element.

Working with the Software Feature Enabler

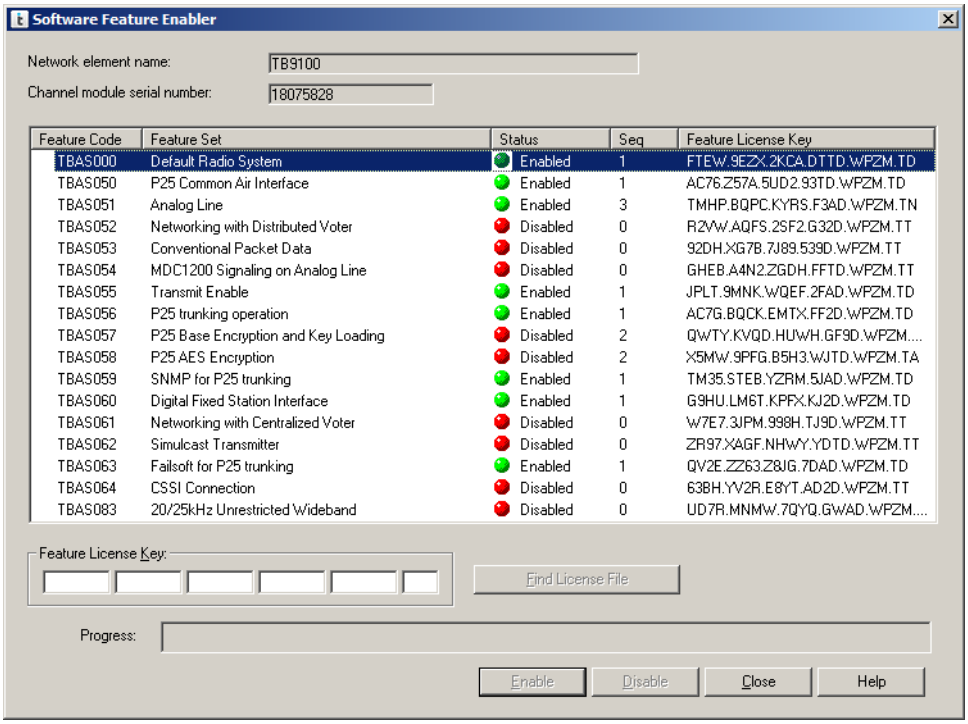
Use the software feature enabler (Tools > Software Feature Enabler) to enable additional features in the network element you are connected to. For a description of these features, see "Software Feature Licensing" on page 16. The network element already has these features but it needs license keys to enable them. Each network element requires a unique license key for each feature. A license key for one network element cannot be used in another.

Viewing Current Feature Licenses

You can see what feature licenses a network element already has.

To view a network element's feature licenses

1. Connect to the network element.
2. Select Tools > Software Feature Enabler. The Software Feature Enabler form appears.



The form displays the name of the network element you are connected to and its channel module serial number. Each row in the table displays information about a feature: the Feature code used to order a feature, its name, and whether it is enabled or disabled. The **Seq** column indicates how many times it has been enabled or disabled.

To add or remove a license, you must first put the network element in Standby mode.

Determining the Feature Licenses Required

To determine which feature licenses you need, apply the following rules (see "Licensing Requirements" on page 51 for full details).

To determine feature licenses for a TB9100 base station

The default radio system license is always included. The transmit enable license is also included, unless the base station is a fill-in receiver.

1. If the base station will handle digital P25 speech calls, you need the P25 common air interface license.
2. If the base station will be part of a channel group, you need a Transceiver networking license.
3. If the base station will use its analog line and carry digital P25 speech, you need an analog line license. If the console system uses MDC1200 signaling, you need an MDC1200 signaling on analog line license as well.
4. If the base station will be the channel group's interface to a digital dispatch system, you need a digital fixed station interface license.
5. If the base station will interface the channel group to a trunking site controller, you need a P25 trunking operation license. In addition, all channel group members will require the SNMP license.

6. If the base station will be part of a simulcast channel group, you need the simulcast transmitter license.
7. If the base station will operate as the central voter or the standby central voter, you need a Central Voter license.

We recommend that all base stations in a centrally voted channel group have the Central Voter license, as this makes configuration, spares management, and network expansion easier.

8. If the base station will operate as the central voter and the failsoft repeater (in the event of losing contact with the site controller), it needs a Failsoft for P25 trunking license. (The other members of the channel group do not need this license in order to join the repeater in Failsoft mode operation.)

To determine feature licenses for a P25 console gateway

The default radio system, analog line, transceiver networking, and P25 base encryption and key loading licenses are always included.

1. If the console system uses MDC1200 signaling, you need an MDC1200 signaling on analog line license.
2. If the network uses AES encryption, you need a P25 AES encryption license.
3. If the console gateway will be connected to a digital dispatch system, you need a digital fixed station interface license.

To determine feature licenses for a trunked analog gateway

The default radio system, analog line, and CSSI Interface licenses are always included.

1. If the console system uses MDC1200 signaling, you need an MDC1200 signaling on analog line license.
2. If the console will be involved in calls encrypted using AES, you need a P25 AES encryption license.

Licensing Requirements

Feature License	Affected Interfaces	License Required for the Service?			
		Analog FM	Digital P25	TSBK	Channel control[1]
Default radio system[2]	All	Y	Y	Y	Y
P25 common air interface	RF	N	Y	N	n/a
Analog line[3]	Analog line	N	Y	N	N
MDC1200 signaling on analog line[4]	Analog line	n/a	n/a	Y	n/a
Transmit enable	RF	Y	Y	Y	n/a
P25 trunking operation[5]	TCCP		Y	Y	Y
P25 base encryption and key loading[6]	Analog line	n/a	Y	N	n/a
P25 AES encryption[7]	Analog line	n/a	Y	N	n/a
SNMP	SNMP	n/a	n/a	n/a	n/a
Digital fixed station interface	DFSI	n/a	Y	Y	Y
Transceiver networking	Channel group	n/a	n/a	n/a	Y
Central voter	Channel group	Y	Y	Y	n/a
Simulcast transmitter	RF transmit	n/a	Y	Y	n/a
Failsoft for P25 trunking	Failsoft	n/a	Y	Y	n/a
CSSI connection	CSSI	n/a	Y	Y	Y

1.Channel control includes the ability to carry out the following: Repeat enable/disable, channel change, encryption defeat, monitor
2.The base station or gateway cannot go into Run mode unless it has a default radio system license or a P25 common air interface license.
3.Applies to digital P25 speech only.
4.Determines whether ANI and the conversion between MDC1200 and TSBKs is supported.
5.Only available for operation with external trunking equipment.
6.Required for encryption at the analog line interface. Enables DES encryption and decryption. Channel module must be crypto-capable.
7.Enables AES encryption in conjunction with the Base encryption feature license.

Enabling Additional Features

If you want a feature, obtain a license key from Tait for that feature, and then use the CSS to enable it.

To license a feature

1. Connect to the network element.
2. If you received the license key in a license file, copy that file (and any others that you received for other features or other network elements) to the license file folder (select Options > File Folders to see which folder the CSS uses).
3. Go into Standby mode, and then select Tools > Software Feature Enabler.
4. Click the feature to select it.

5. If you received a license file, click **Find License File**. This searches the license file folder for a license file for the current network element and the selected feature. If the CSS finds one, it displays the license key (in the feature's row and in the Feature License Key boxes), and increments the Seq column by 1.
6. If you don't have a license file, enter the license key into the Feature License Key boxes.
7. Click **Enable**. A 'Feature enabled' message appears. The license key appears in the feature's row and the Seq column is incremented by 1.

Many features also have a configuration setting that enables or disables them. Often, the default setting is 'enabled.'

Disabling a Feature

Features are not normally disabled. However, disabling may be desirable in special circumstances, for example, if you are trying out the feature and decide not to purchase it.

A disabled feature can only be re-enabled by purchasing a new license key. The original feature license key cannot be re-used.

Before disabling a feature, make sure that the network element configuration does not use it. Once a feature is disabled it does not work, even if the CSS configuration enables it.

If the network element configuration requires a function but the software feature enabler has disabled it, a syslog message will be generated when the network element attempts to implement the function. For example, if you disable the P25 common air interface, but use a calling profile that tells the network element to handle dispatcher calls as digital P25 calls, the dispatcher will be unable to make calls. Each attempt produces a syslog message.

To disable a feature

1. Connect to the network element.
2. Go into Standby mode, and then select Tools > Software Feature Enabler.
3. Check the **Channel module serial number** box to make sure that the CSS is connected to the correct network element.
4. Click the feature's row.
5. Click **Disable**.

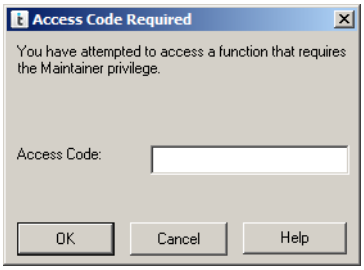
   The progress bar indicates how far the disabling has progressed. On completion, a new number appears in the **Feature License Key** column. Communicate this new number to Tait if you are entitled to a refund or if you want to re-enable the feature.

Working with Privileges

If access codes have been set, you must enter an access code to obtain the Maintainer or the Administrator privilege before you can carry out some functions. From the toolbar you can change privileges. Only the Administrator can change access codes.

Obtaining a Privilege

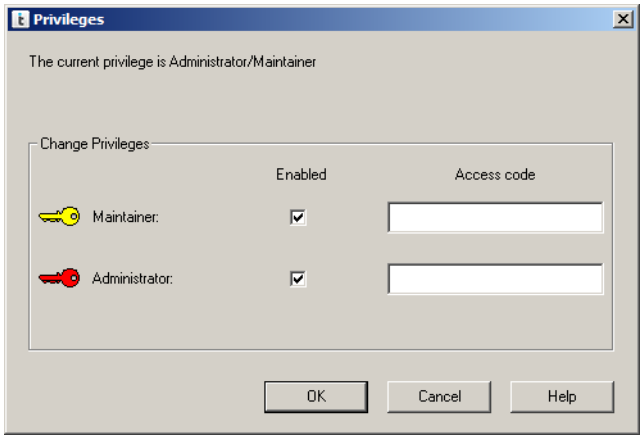
If you request a function that you don't currently have the privilege for, the Access Code Required dialog box appears, asking for an access code.



1. Enter the access code for the required privilege.
2. Click OK. The Privileges icon on the toolbar indicates the privileges you now have. A yellow key indicates Maintainer privilege. A red key indicates Administrator privilege.

Changing Privileges

The Privileges dialog box indicates which privileges are currently active. You can enable or disable privileges. You may, for example, have enabled Administrator privilege in order to change a network element password, but now you want to return the CSS to Guest privilege, because a number of people have access to the CSS. The Guest privilege is always enabled and cannot be disabled.



If a row is disabled, the privilege has no access code and you automatically have this privilege. If you want the privilege to be controlled by an access code, select Tools > Change Privilege Access Codes.

To enable a privilege

1. On the toolbar, click **Privileges**.
2. Select the check box of the privilege you want to enable.
3. Alongside the check box, enter the corresponding access code.
4. Click OK.

To disable a privilege

1. On the toolbar, click **Privileges**.

2. Clear the check box of the privilege you want to disable.
3. Click OK.

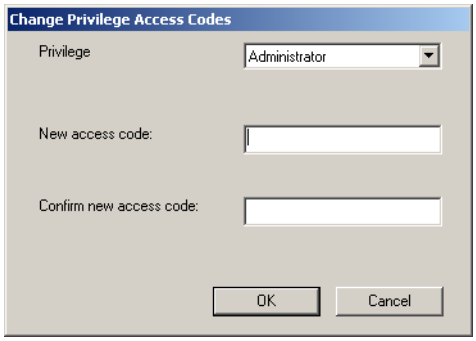
Setting up and Changing Privilege Access Codes

If access codes have not been set up, CSS users automatically have all privileges and they are not asked for access codes. If you want to increase security, set up access codes by entering them as described below.

If access codes have been set up (for example during installation), you can change them with Administrator privilege.

To set up or change an access code

1. Select Tools > Change Privilege Access Codes.
2. If the Access Code Required dialog box appears, supply the current Administrator access code. The Change Privilege Access Codes dialog box appears.



3. In the **Privilege** box, select the privilege for which you want to set up or change an access code.
4. In the **New access code** box, enter the new access code.
5. In the **Confirm new access code** box, enter the same code again.
6. Click OK.

CSS Options

Using the Options menu you can configure aspects of the CSS software.

CSS Settings

Select Options > Settings to modify any CSS settings.

Temperature Display	The CSS can display temperature in degrees Fahrenheit or Celsius. Select the option you prefer.
Quality of service	By default, the CSS does not attach a DSCP value to IP packets that it sends to the network. If you want the CSS to attach a DSCP value, enter a number other than 0 into the DSCP box. The new value does not come into effect until the current connection is closed and a new one is established. You must make sure that the PC's operating system has a QoS packet scheduler installed, otherwise the CSS will be unable to connect to network elements. See your Windows operating system documentation for instructions. For more information on DSCP, see "Quality of Service" on page 163.

File Folder Locations

The Default file locations area (Options > File Folders) specifies folders for configuration files, log files, license files, and firmware files. To modify a default location, click the button to the right of the box and select a folder. To find out where the CSS log is stored, see "Viewing the CSS Application Log" on page 114.

Configuration files	Specifies the default location that the CSS looks in when opening configuration files and saves to when saving them. (This may have been chosen during installation.)
Firmware files	Specifies where the CSS will look for firmware files when you ask it to download new firmware into a network element. If you receive new firmware for a network element upgrade, copy it to this folder.
License files	Specifies where the CSS will look for license files when you ask it to enable additional features in a network element. If you receive a license file, copy it to this folder.

Part D Monitoring

The CSS can monitor Tait P25 network elements. It can provide operational information about the various interfaces and modules. The CSS can also display data logs and module details.

For information about monitoring alarms, see "Alarms" on page 198. For information about monitoring Task Manager, see "Monitoring Task Manager" on page 279.

To monitor a TB9100 base station or gateway, connect to it, click **Monitor**, and select an item from the navigation pane.

Interfaces

- Monitoring the RF Interface
- Monitoring the Channel Group Interface
- Monitoring the Analog Line
- Monitoring the Trunking Interface
- Monitoring Failsoft Mode
- Monitoring the DFSI Interface
- Monitoring the CSSI Interface
- Monitoring Conventional Packet Data
- Monitoring Encryption

Channel Group

- Monitoring Channel Group Status
- Monitoring the Channel Coordinator

Synchronization

- Monitoring Simulcast

Modules

- Monitoring the Reciter or Gateway Module
- Monitoring the Power Amplifier
- Monitoring the Power Management Unit

Data Logs

- Viewing Call Records
- Viewing the System Log
- Viewing the Trace Log
- Viewing Call Statistics
- Viewing the CSS Application Log

Module Details

- Viewing Reciter or Gateway Module Information
- Viewing Power Amplifier Information
- Viewing Power Management Unit Information

Interfaces

The CSS can monitor the network element's interfaces. You must be connected to that network element.

Monitoring the RF Interface

The RF Interface form (Monitor > Interfaces > RF Interface) shows what the receiver and transmitter is currently doing. It displays:

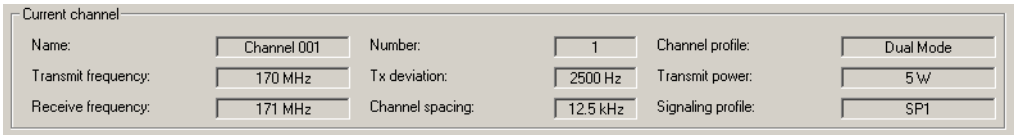
- Details about the channel that the base station is currently operating on
- Operational information about the receiver
- Operational information about the transmitter

Most information in this form is not relevant to gateways.

Current Channel

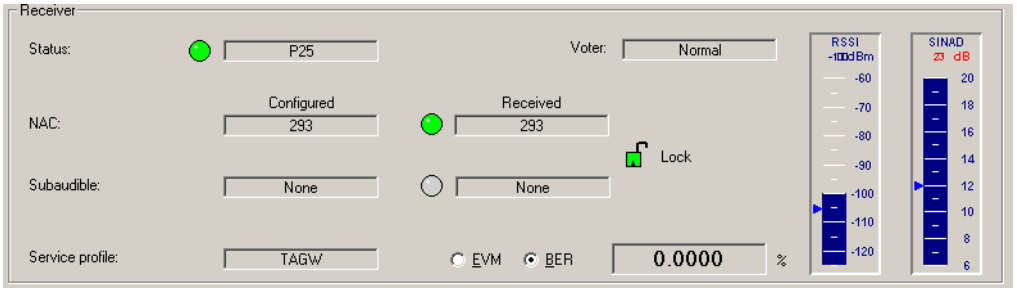
The Current channel area shows you which channel the base station is operating on and displays its main configuration settings. The choice of channel is the result of Task Manager action. If the channel name is Invalid channel, Task Manager has told the base station to operate on a channel that does not exist.

To view additional settings defined by the channel, look in the channel table (Configuration > Network Element > Channel Table) and in the profiles assigned to the channel.



Receiver

In the Receiver area, you can check that the receiver is enabled, see whether it is gated, and view information about the NAC or subaudible signaling. You can also view the RSSI, SINAD, and the digital P25 signal quality (EVM or BER).



Status

The Status LED provides an overview of the status of the receiver.

Color	Meaning
Red	The receiver is not operational.
Green	The receiver is receiving a valid signal.
Gray	The receiver is able to receive but not currently receiving anything. No fault has been detected.

The Status box alongside provides more detail about the receiver status.

Status	Meaning
Invalid channel	The currently selected channel does not exist or is corrupted.
No synth lock	The receiver synthesizer(s) are out of lock. The receiver is unable to operate on the configured frequency.
Configuration disabled	Configuration has disabled the receiver. The current channel profile allows the receiver to receive neither analog FM nor digital P25 signals.
Task Manager lock	Task Manager has 'locked' (disabled) the receiver.
P25	The receiver has unmuted to a digital P25 signal.
Analog	The receiver has unmuted to an analog FM signal.
Enabled P25	The current channel profile enables the receiver to receive digital P25 signals but not analog FM signals.
Enabled analog	The current channel profile enables the receiver to receive analog FM signals but not digital P25 signals.
Enabled dual	The current channel profile enables the receiver to receiver digital P25 or analog FM signals.

Voter

The Voter box indicates whether commands received over the DFSI interface have affected voter operation.

Display	Meaning
Normal	Voter operation has not been altered by DFSI command.
Selected	The DFSI has instructed the channel group to declare any voice streams from the connected member as the vote winner.
Disabled	The DFSI has instructed the current member not to participate in voting. Any streams from the RF interface will not be voted on and therefore will not be repeated or made available to the channel group.

NAC

The two NAC boxes display the NAC that the receiver is configured with and the current or most recently received NAC. Alongside the Received NAC box, an LED monitors NAC detection.

LED Color	Meaning
Green	The receiver has detected a matching NAC.
Red	The receiver has detected a NAC that is different from the one it is configured to receive.
Gray	The receiver is not currently detecting a NAC.

If the **Lock** padlock is locked, the receiver will unmute irrespective of the received signal's NAC. Task Manager has locked the decoding of subaudible signaling and the NAC.

Subaudible

The two Subaudible boxes display the configured and the received CTCSS tone or DCS code. The configured tone or code is specified in the signaling profile for the current channel. The receiver can only detect a CTCSS tone if it is the same as the configured one, but it can detect any DCS code. The form displays what the receiver is currently receiving (or has just received).

Alongside the **Received** box, an LED monitors the detection of subaudible signaling.

LED Color	Meaning
Green	The receiver has detected a valid DCS code or the particular CTCSS tone that it is configured to recognize.
Gray	The receiver is not currently detecting any subaudible signaling.

If the **Lock** padlock is locked, the receiver will unmute irrespective of the received signal's CTCSS tone, DCS code, or NAC. Task Manager has locked the decoding of subaudible signaling and the NAC.

Service profile

The name of the service profile that the current channel specifies. This profile controls the behavior of the inbound RF channel. Note that a different service profile can be selected for the inbound analog line.

EVM

Click **EVM** and the box to the right displays the error vector magnitude of the received signal. The EVM can range between 200 (high quality) and 1000 (low quality).

BER

Click **BER** and the box to the right displays the estimated bit error rate of the received signal, expressed as a percentage.

RSSI

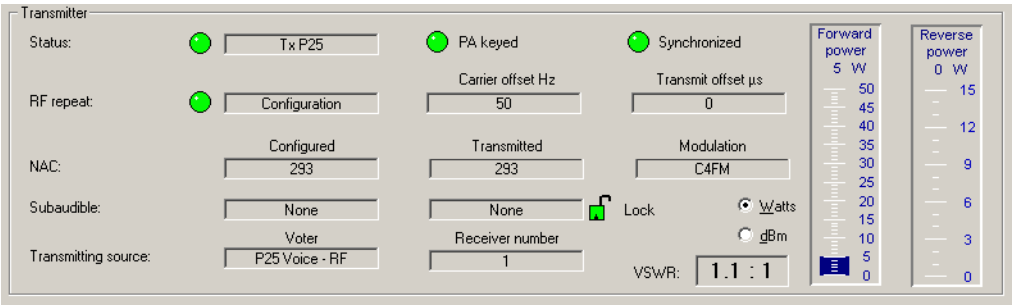
The RSSI gauge displays the current strength of the received signal in dBm. The equivalent numeric value appears under the gauge heading. If this value is red, it exceeds the maximum or has fallen below the minimum that the gauge can display. A pointer indicates the configured threshold for opening the receiver gate.

SINAD

The SINAD gauge displays the signal-to-noise ratio of the received signal in dB. The equivalent numeric value appears under the gauge heading. If this value is red, it exceeds the maximum or has fallen below the minimum that the gauge can display. A pointer indicates the configured threshold for opening the receiver gate.

Transmitter

In the Transmitter area, you can check that the transmitter is enabled, see whether it is keyed, view information about the NAC and the subaudible signaling, and see the source of what is being transmitted. You can also monitor the forward and reverse power.



Status

The Status LED provides an overview of the status of the transmitter.

Color	Meaning
Red	The transmitter is not operational.
Green	The transmitter is transmitting
Gray	The transmitter is idle. No fault has been detected.

The Status box alongside provides more detail about the transmitter status.

Status	Meaning
No license	The network element does not have the Transmit enable feature license. It cannot transmit. Alternatively, it does not have the Unrestricted Wideband feature license and the channel table has channel configurations for mid-band or wideband in the 150-174 MHz or 421-470 MHz frequency bands. If this is the reason, the Receiver status displays "Invalid channel."
Invalid channel	The currently selected channel does not exist or is corrupted.
No synth/FCL lock	The receiver synthesizer or FCL is out of lock. The receiver is unable to operate on the configured frequency.
Configuration disabled	Configuration has disabled the transmitter. The Transmitter check box in the Edit Channel Profile dialog box is cleared.
Task Manager lock	Task Manager has 'locked' (disabled) the transmitter.
Tx P25	The transmitter is transmitting a digital P25 signal.
Tx analog	The transmitter is transmitting an analog FM signal.
Tx CWID	The transmitter is transmitting its CWID.
Idle	The transmitter is not transmitting.

PA keyed

When the PA keyed LED is green, the transmitter is transmitting; carrier is present. This is caused by one of the following:

- A call (the **Transmitting source** LED is green and the Voter box indicates the origin of the call)
- A CWID transmission
- A transmit tail
- The Carrier button on the control panel has been pressed

Synchronized

If the LED is red, the transmitter is unsynchronized. The Simulcast form displays the reason in the Status box under Transmit timing (Monitor > Synchronization > Simulcast). Non-simulcast transmitters are always unsynchronized. To prevent the LED from displaying red and giving the misleading impression that something is wrong, disable the Unsynchronized alarm (Configure > Alarms > Control). This turns the LED gray.

If the LED is green, the transmitter is able to synchronize its transmissions with the other transmitters in the channel group (simulcast operation).

The LED should be gray if the transmitter is non-simulcast. The synchronization status is not relevant.

RF repeat

When the RF repeat LED is green, RF repeat is enabled and the transmitter will repeat any vote-winning RF signal that the base station or channel group receives. When the RF repeat LED is gray, RF repeat is currently disabled.

The box alongside indicates the cause of the current RF repeat setting.

Cause	Description
Configuration	The RF repeat setting was selected by configuration (the channel table has enabled or disabled it).
Task Manager	A Task Manager action has enabled or disabled RF repeat. This can only happen if the channel table has put RF repeat under dispatcher control. The action was probably triggered by locally connected dispatch equipment via function tones. Other triggers of the Task Manager action could include function codes and changes to digital inputs.
DFSI	A dispatch command from digital dispatch equipment using the DFSI interface enabled or disabled RF repeat. This can only happen if the channel table has put RF repeat under dispatcher control.
Power up	The previous RF repeat setting was restored from flash memory after a reset. Other actions may have subsequently defined the RF repeat setting without altering it. For example, the network element may have started up with RF repeat enabled. If a Task Manager action subsequently selected channel 1 on going to Run mode and channel 1 specifies that RF repeat is enabled, the display would still be 'Power up.'
IP	The RF repeat setting resulted from a command sent over IP from another network element. Generally, this appears when another network element's channel coordinator changes the RF repeat setting. This can only happen if the channel table has put RF repeat under dispatcher control and the channel group configuration enables collective control of RF repeat. If the change originated from digital dispatch equipment, 'IP' appears briefly and is updated by 'DFSI.' If the change originated from analog dispatch equipment, 'IP' appears briefly and is updated by 'Task Manager.'
TCCP	The RF repeat setting was provided by TCCP signaling. The setting has been defined by the trunking site controller, overriding the configuration and any Task Manager actions. RF repeat is off, as control channels do not repeat their signals.

Carrier offset Hz — (Simulcast operation only) Displays the configured offset in Hertz. The actual carrier frequency will differ from the configured transmit frequency by the configured offset. Note that the monitored transmit frequency does not include the carrier offset.

Transmit offset µs — (Simulcast operation only) Displays the configured local transmit offset in microseconds. This delays the launch time from the nominal time requested by the central voter.

NAC — The two NAC boxes display the NAC that the transmitter is configured with and the NAC that the transmitter is currently transmitting or has most recently transmitted. The configured NAC is specified in the signaling profile for the current channel.

Modulation

Displays the modulation scheme that the transmitter is configured to use.

Display	Description
C4FM	The modulation scheme mandated by P25 Phase 1.
CSM	Constant-envelope Simulcast Modulation. This is a modulation scheme designed to improve on the performance of C4FM in simulcast systems. It can currently be used with Tait SUs that are configured for CSM.
Wide	Wide (also known as Wide Pulse) is a modulation scheme designed for simulcast systems. It is similar to C4FM but uses wide-band (25kHz) channels. SUs must be configured to receive on a Wide channel.

Subaudible

The two Subaudible boxes display the CTCSS tone or DCS code that the transmitter is configured with and the CTCSS tone or DCS code that the transmitter is currently transmitting or has most recently transmitted. The configured tone or code is specified in the signaling profile for the current channel.

If the **Lock** padlock is locked, the transmitter does not send any subaudible signaling. Task Manager has locked the encoding of subaudible signaling.

Transmitting source

The Transmitting source box shows where the signal being transmitted came from.

Display	Description
None	There is no source. The transmitter is independently providing control channel signaling.
FM - Line	An analog FM call received over the analog line or DFSI
FM - IP	An analog FM call received over the digital line from another channel group member.
FM - RF	An analog FM call received over the air interface
FM - Panel	An analog FM call received from the control panel microphone
P25 Voice - Line	A digital P25 call received over the analog line or DFSI
P25 Voice - IP	An digital P25 call received over the digital line from another channel group member.
P25 Voice - RF	An digital P25 call received over the air interface
P25 Voice - Panel	An digital P25 call received from the control panel microphone
P25 Data	A digital P25 data call.

Receiver number

The receiver number of the network element that provided the signal being transmitted. This supplements the information in the Transmitting source box.

Forward power

Displays the measured forward power of the PA output. Click **Watts** or **dBm** to select the units used.

Reverse power	Displays the measured reverse power of the PA output. Click **Watts** or **dBm** to select the units used.
VSWR	Displays the Voltage Standing Wave Ratio of the PA's RF output.

Monitoring the Channel Group Interface

To help in troubleshooting, the Channel Group form (Monitor > Interfaces > Channel Group) monitors the network element's operation as part of a channel group. Use the form for the following:

- Checking that the channel group interface is operational and seeing what the member's voting role is
- Checking channel group settings when installing the system
- Monitoring network link operation and measuring network jitter
- Checking for transmit buffer underflows

Checking Channel Group Interface Status

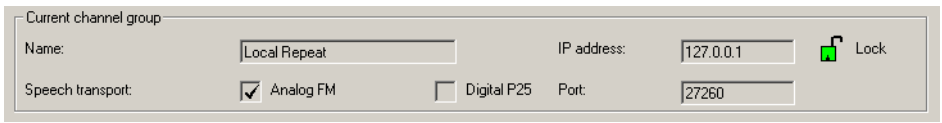
1. Select Monitor > Interfaces > Channel Group.
2. Check the Status LED and box to see whether the channel group interface is operational and what voting role the member is carrying out.

LED	Box text	Description
Red	No license	The member does not have a networking feature license. It cannot send or receive voice data streams on its channel group interface.
	Task Manager lock	Task Manager has locked the channel group. The channel group interface is disabled.
	Standby	The member is in Standby mode, which takes it out of service, disabling the channel group interface.
Gray	Switched voter	The member is functioning as a switched voter within the channel group. Voting is disabled.
	Satellite voter	The member is functioning as a satellite voter within the channel group.
	Central voter	The member is functioning as a central voter within the channel group.

Checking Channel Group Settings

If the system is not behaving as expected, check the channel group settings.

1. Select Monitor > Interfaces > Channel Group.
2. Under **Current channel group**, check the settings displayed. These are a subset of the settings in the Channel Groups dialog box (Configure > Channel Group > Channel Groups and click Edit).

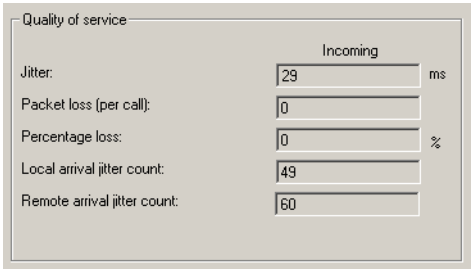


- Confirm that the expected channel group is in use. The network element uses the channel group that is assigned to the current channel.

- Check that the required types of voice stream can be sent to the channel group. If **Analog FM** is selected, the digital line can send analog FM voice streams to other channel group members. If **Digital P25** is selected, the digital line can send digital P25 voice streams.
- Check that the **IP address** is correct. This is the (normally multicast) address of the current channel group. The network element sends voice streams to this address and (if the address is multicast) receives voice streams that have this destination address.
- The **Port** is not normally changed from the default.

Monitoring the Network Link

To monitor the network element's network link to other channel group members, select Monitor > Interfaces > Channel Group and view the Quality of Service area. This area displays quality of service values for the incoming voice stream belonging to the current over. If an over is long, its values reset every 20s.



Jitter (ms)

The peak delay variation of RTP packets arriving at the connected network element for the current over. A high jitter is a sign that the network is congested.

This value does not accurately measure the jitter of the linking infrastructure. It includes delay variation in the sending of packets and is measured after processing in the network element.

Packet loss (per call)

The number of packets lost in the current voice over. Packet loss should be rare. Users will not notice a loss of up to 10 packets. Packet losses may be caused by inadequate linking bandwidth, cable faults, or power cycling of the switch or router.

Percentage loss

The percentage of packets lost in the current over. Packet losses should be rare. Frequent packet loss indicates that there is something wrong with the linking infrastructure.

Local arrival jitter count

The number of times in the current over that a local voice stream packet had excessive jitter. Jitter is excessive if a packet arrives too late. The network element knows the arrival time of the start of the stream that the packet belongs to and can determine when the next packet is expected. If the packet has not arrived at the expected time plus the configured max interarrival jitter (Configure > Alarms > Network Thresholds), the count is incremented. Whenever the counter is incrementing, the QoS jitter alarm is active.

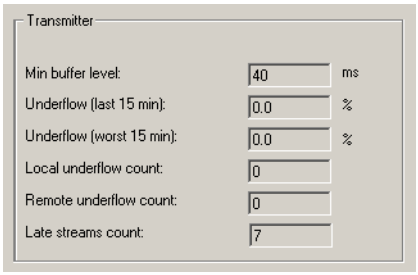
This parameter applies only to voice streams that are local to the channel group. It does not include voice streams provided to the channel group by an external interface.

Remote arrival jitter count

The number of times in the current over that a remote voice stream packet had excessive jitter (see above). A voice stream is remote if an interface external to the channel group provided it. External interfaces include the trunking, failsoft and DFSI voice services.

Monitoring the Transmit Buffer

If the jitter on the incoming voice stream is high, the base station's transmit buffer may not be able to cope. To check the buffer, select Monitor > Interfaces > Channel Group and view the Transmitter area.



Min buffer level

The lowest level of the transmit buffer, measured over a 5-second period. A negative value indicates an underflow. The measured level is affected by the relevant configuration setting in the Edit Channel Group dialog box:

- Preamble (unsynchronized operation)
- Buffer min (synchronized (self-regulating marshalling) operation)
- Marshalling duration (synchronized (fixed marshalling duration) operation)

When the base station transmits TSBKs, it uses a minimum buffer level of 100 ms and the display updates to reflect this.

Underflow (last 15 minutes)

The percentage of packets during the last 15 minutes that arrived late enough to cause a buffer underflow. If too many buffer underflows occur, this indicates a problem with the transmit timing or the bandwidth of network links (see the System Manual).

Underflow (worst 15 minutes)

The highest percentage of packets during any 15 minute period in the last 24 hours that arrived late enough to cause a buffer underflow. If too many buffer underflows occur, this indicates a problem with the transmit timing (see the System Manual).

Local underflow count

The number of packets from local streams that did not arrive in time to be transmitted. A stream is local if it originates from within the channel group. Streams in a control channel are always regarded as local. The counter increments each time a packet arrives so late that the transmit buffer underflows (becomes empty). Voice packets are discarded on arrival (after a fill-in packet was created and supplied to the transmitter). Signaling packets on control channels are placed in the transmit buffer at the proper position as if the packet hadn't been late.

Remote underflow count

The number of packets from remote voice streams that did not arrive in time to be transmitted. A voice stream is remote if an interface external to the channel group provided it. External interfaces include the trunking, failsoft and DFSI voice services.

Late streams count

The number of times that a stream arrives later than the required transmit time. In control channels, the counter increments once for every message that was after the required transmit time. Otherwise, the counter increments once per late voice over. A stream arriving at an unsynchronized transmitter is always late, but this is not an issue if the transmitter is not configured for simulcast operation.

Monitoring the Analog Line

The Analog Line form (Monitor > Interfaces > Analog Line) indicates what is happening on the analog line. You can check its status, view information about the current calling profile, look at line levels, and view the current state of line signaling.

Status

If the Status LED displays red, the analog line is unable to function. The Status box alongside indicates the reason.

Status	Description
No license	The network element does not have an analog line feature license. This is needed for passing digital P25 calls over the analog line but not for analog FM calls, tone remote signaling, or for TSBKs.
Invalid channel	Configuration information is missing or corrupted.
Configuration disabled	The configuration disables the current calling profile. The analog line cannot operate.
Task Manager lock	Task Manager has locked (disabled) the analog line.
Enabled	The analog line is operational.

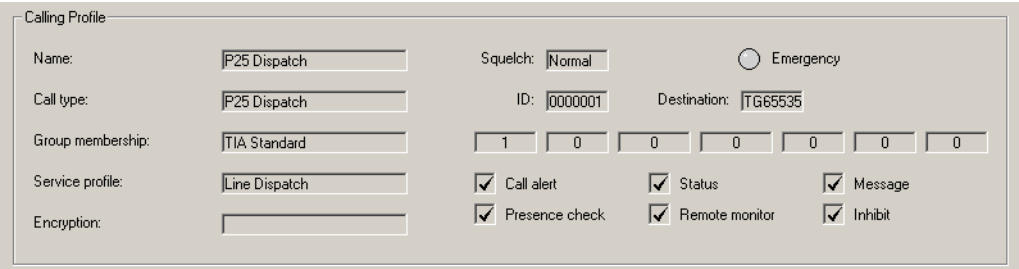
RF repeat

The RF repeat LED only has meaning if the CSS is connected to a TB9100 base station. When the RF repeat LED is green, the base station repeats the signal it receives, unless another signal with a higher priority is present at one of its interfaces. If the base station is part of a channel group, the signal it repeats may have been received by any of the channel group's base stations.

When the RF repeat LED is gray, the base station's repeat function is currently disabled. Signals from a receiver (at this base station or at any other base station in the channel group) can be sent to the analog line but not to the transmitter.

Calling profile

The Calling profile area displays details about the current calling profile. The calling profile is selected by the channel table or by function tone from an analog console system.



Name — The name of the calling profile.

Squelch — Specifies what the analog line unmutes to. If the squelch is Normal, the network element switches any vote winner onto the analog line. If the squelch is Selective, the network element only switches the vote winner onto the analog line if it is addressed to the current calling profile's line ID or to a group listed in the current calling profile's group membership.

Emergency — When the Emergency LED is green, any calls that the analog line makes will be emergency calls. This is because the current calling profile configures them that way. It does **not** mean that the base station is currently receiving an emergency call.

Call type — Defines the type of call that the channel group makes when the dispatcher initiates a call. (The analog line can always forward incoming calls of any type.) If the call type is P25 group or P25 individual, the following boxes provide further information.

Item	Meaning
ID	The identity of the caller.
Destination	The individual or group ID that the call is made to.

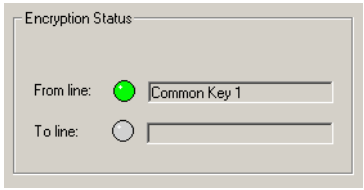
Group membership — The name of the collection of groups assigned to the calling profile. Alongside are displayed the group IDs belonging to the collection. If trunked analog gateway is the selected product, the Group membership box is disabled and the first of the boxes alongside displays the gateway's current group ID. This is because the trunked analog gateway can only belong to a single group at any one time.

Service profile — The service profile assigned to the calling profile. The check boxes alongside indicate which services are enabled at the analog line input. (The receiver input can have a different service profile, assigned to the channel.) For details about these services, see "Working with Service Profiles" on page 126.

Encryption — Displays the encryption key that is assigned to the current calling profile.

Encryption Status

The Encryption status area monitors the encryption of the input on the analog line input and the decryption of signals destined for the analog line output.



From line

The **From line** LED indicates whether encryption is proceeding normally. The box alongside indicates whether the call is clear, what key is being used, or what the encryption problem is.

LED	Box text	Encryption status
Grey		There is currently no speech.
Green	Clear	The input speech is not being encrypted.
	Key name	The speech is being encrypted using the named key.
Red	Key empty	There is no secure key data for the CKR that the key name is mapped to. The speech cannot be encrypted so it is not transmitted. Check that the key name is mapped to the correct CKR and that the secure key data for that CKR has been loaded.
	No license	The calling profile specifies an encryption key but the required encryption feature license is not present. Speech is transmitted clear.

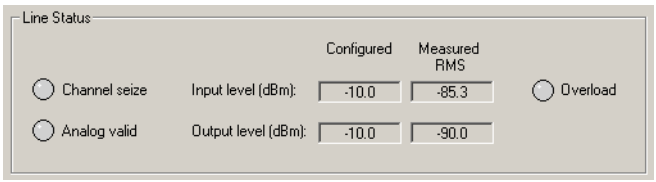
To line

The **To line** LED indicates whether there are any problems with decryption. The box alongside indicates whether the call is clear, what key is used for decryption, or what the decryption problem is.

LED	Box text	Encryption status
Grey		There is no speech output.
Green	Clear	The speech was not encrypted.
Green	Key name	The speech has been decrypted using the named key. If the key has no name, the CKR number is displayed.
Red	Clear	The speech is clear but should not be; the calling profile specifies an encryption key.
Red	Key name	The key used by the caller is not the key specified by the calling profile. The speech has been decrypted using the displayed key. If the key has no name, its CKR number is displayed.
Red	Key empty	The key that the calling profile selects has not been loaded or has been zeroized. No other key fits, so the speech cannot be decrypted.
Red	No key	The gateway does not have the key that was used to encrypt the speech. The call cannot be decrypted.
Red	No license	The encryption feature license is not present. If the speech is clear, it is provided to the analog line. If the speech is encrypted, it cannot be decrypted.

Line Status

The Line status area shows the status of line signaling and the levels of the line input and output.



The first row of controls displays information about the analog line input.

If the **Channel seize** LED is green, the analog line is receiving a signal that an analog input is present.

The **Input level** boxes display the configured input level (the expected level of the line input) and the RMS level currently being measured.

If the **Overload** LED is red, the level is too high and is about to cause distortion in the DSP. It is acceptable for occasional speech peaks to trigger this LED, but if this happens regularly and often, too much gain is being applied and tone detection will not work properly. Enter a higher line level (Configure > Analog Line > General). If the **Overload** LED goes red at the beginning of the voice over, the HLGT is too high. Configure the console system to reduce the level of its HLGT output.

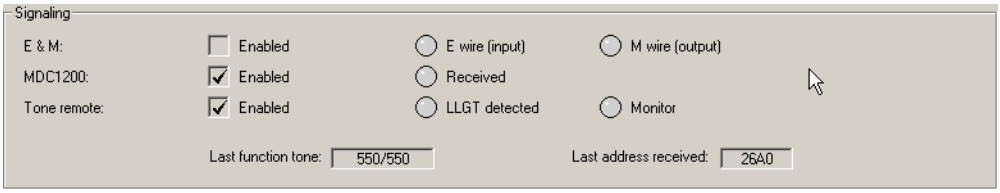
The second row of controls displays information about the analog line output.

If the **Analog valid** LED is green, the analog line is sending a signal that there is a valid output on the analog line.

The **Output level** boxes display the configured analog line output level and the RMS level currently being measured.

Signaling

The Signaling area shows the status of line signaling on the analog line. Check boxes indicate what is enabled in configuration and LEDs show what signaling is currently happening.



E & M

If the **Enabled** box is checked, the analog line is configured to recognize and use E & M signaling. If the **E Wire (input)** LED is green, the network element has detected that the E wire has been asserted. If the **M Wire (output)** LED is green, the network element has asserted the M wire.

MDC1200

If the **Enabled** box is checked, the analog line is configured to recognize MDC1200 signaling. If the **Received** LED is green, the analog line has detected incoming MDC1200.

Tone remote

If the **Enabled** box is checked, the analog line is configured to recognize tone remote signaling. If the **LLGT detected** LED is green, the analog line is receiving low level guard tone. If the green **Monitor** LED lights briefly, the analog line received a dispatcher command to monitor the channel.

Last function tone

Displays the frequency pair of the last function tone that was received. If a dual function tone was received, the two frequencies in the pair are different. If a single frequency tone was received, this is still displayed as a pair, but both frequencies are the same.

Last address received

Displays the last MDC1200 address that was received. This is the destination address of a call initiated from the dispatcher.

Monitoring the Trunking Interface

Using the Trunking Interface form (Monitor > Interfaces > Trunking) you can monitor the operation of the interface between the trunking site controller and the network element you are connected to. The master base station has a control connection and other members have a status connection. The form displays more information when you are connected to the master.

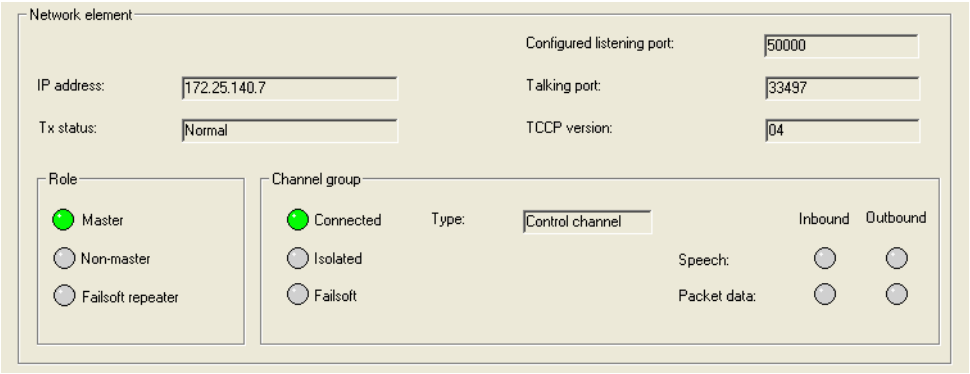
Status

A red Status LED indicates that the trunking interface is not operational. A green LED means that there is a trunking connection. A gray LED indicates that there is no trunking connection, but that there are no problems with the network element. The Status box alongside provides more detail.

Status	Description
No license	The network element does not have an external trunking interface license. It cannot be a channel group master.
Configuration disabled	The current channel is configured in the channel table as a conventional channel. It cannot have a trunking interface.
Connected	The network element has a trunking status or control connection.
Not connected	The network element does not have a connection to a trunking site controller.

Network element

The network element area displays information relevant to the current role of the network element within the trunking system.



IP address

The IP address of the trunking site controller.

Tx status

Displays the current transmit status of the member. This is the status information that the member will provide to the trunking site controller when requested.

Display	Description
Normal	Member is operating normally. If it is part of a simulcast channel group, it is synchronized and will transmit when requested.
Unsync – Tx	Member is unsynchronized. The channel group is simulcast and the member is configured to transmit when unsynchronized.
Unsync- Silent	Member is unsynchronized and will not transmit.
Fault – Silent	Member has a fault that prevents it from transmitting or that has caused the PA to fold back its power output. Select Monitor > Alarms > Status to find out what the fault is.

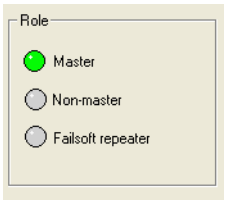
Configured listening port
: The port that the base station is listening to for TCCP communications. This port is defined by configuration.

Talking port
: The port that the base station sends its control service communications to. The base station obtains this port number from the site controller's requesting packet.

TCCP version
: The version of the Trunking Channel Control Protocol that the member supports. This protocol is used for communications between a trunking site controller and network elements.

Role

The Role area indicates the role that the network element is currently playing within the channel group.



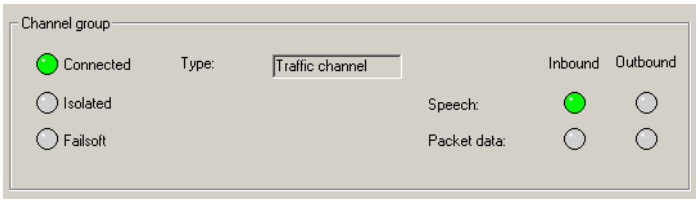
Master
: A green LED indicates that the network element is the channel group master. It has a control connection to the trunking site controller. The Master area below provides further details.

Non-master
: A green LED indicates that the network element is a non-master. Another member is the master.

Failsoft repeater
: A green LED indicates that the network element is currently operating as a failsoft repeater. It can only do this if there is no TCCP connection to any channel group member. Select Monitor > Interfaces > Failsoft to monitor failsoft operation.

Channel group

The Channel group area indicates the state and mode of the channel group as a whole.



Connected

The channel group has a control connection to a trunking site controller. The box alongside indicates whether the channel group is operating as a traffic channel, a control channel, or is 'down' (has been told to stop transmitting and receiving).

Isolated

The channel group has no master (no TCCP control connection to a trunking site controller). There could still be TCCP status connections to channel group members. The channel group functions as a simple voice-repeat wide area channel.

Failsoft

The channel group is in failsoft mode. A member has taken over as failsoft repeater following the loss of all connections to the trunking site controller.

Type

Indicates what type of channel group the network element is part of. When the channel group has a control connection to a trunking site controller, the controller tells it what type to be.

Display	Description
Control channel	The channel group is a trunking control channel.
Traffic channel	The channel group is a traffic channel.
Down	The base station is down. The trunking controller has taken the channel group out of service, instructing it not to transmit or receive.
Conventional	The channel group has no trunking control connection, and is operating in conventional mode.
Standby	The network element is in Standby mode.

Speech

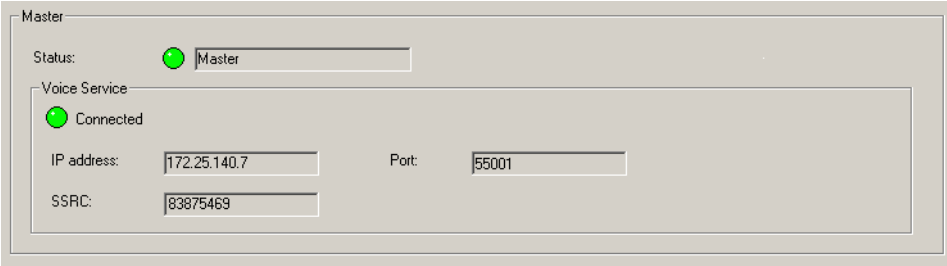
A green LED indicates that the channel group is handling speech. Inbound speech is from a SU to the trunking controller, outbound speech is from the trunking controller to one or more SUs.

Packet data

A green LED indicates that the voice service is carrying packet data.

Master

If you are connected to the channel group master, the Status LED in the Master area is green and the Master area provides information about master operation.



Status — The Status LED and box indicate the network element's master status.

LED	Display	Description
Red	Configuration disabled	The configuration does not permit the channel group member to be a master. The Allow control connection check box is cleared in the Trunking form (Configure > Network Interfaces > Trunking).
Gray	Enabled	The channel group member is able to be a master but is not currently operating as one.
Green	Master	The channel group member is currently operating as the master.

Voice service

The Voice service area monitors the voice service that the master provides between the channel group and the trunking site controller.

If the channel group is in failsoft mode and the network element is the failsoft repeater, it sends the voice service to a different IP address and port. These are configured in Configure > Network Interfaces > Failsoft.

Connected — A green LED indicates that there is a voice service connection.

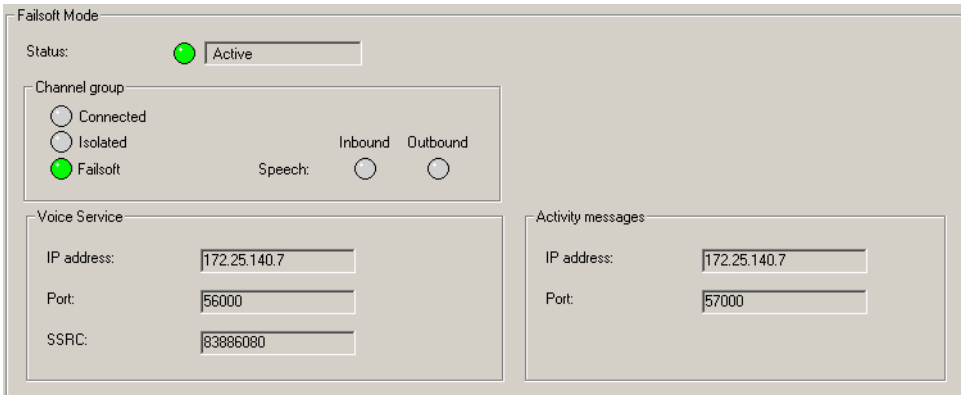
IP address — The IP address that the base station is configured to send voice streams to. This can be the trunking controller or another device.

Port — The UDP port that the base station sends voice streams to. The base station obtains the port number from the trunking controller's connection message.

SSRC — The SSRC (synchronization source) currently being used. The SSRC is a large number specified by the trunking controller in its connection message. It uniquely identifies voice streams sent from the master base station.

Monitoring Failsoft Mode

Using the Failsoft Mode form (Monitor > Interfaces > Failsoft), you can monitor failsoft operation. Connect to the network element operating as the failsoft repeater or failsoft gateway to view full details. If you are connected to another channel group member, the form only indicates whether the channel group is in failsoft mode.



Status

The Status LED and box indicate the network element's failsoft status.

LED	Display	Description
Red	No license	The network element does not have a Failsoft feature license. It cannot become a failsoft repeater or failsoft gateway.
	Configuration disabled	Configuration does not allow the network element to become a failsoft repeater or failsoft gateway (Configure > Network Interfaces > Failsoft).
Gray	Enabled	The network element is able to be a failsoft repeater or failsoft gateway but is not currently operating as one.
Green	Active	The network element is currently operating as a failsoft gateway or as a failsoft repeater.

Channel group

The Channel group area indicates the current state of the channel group that the connected element is part of. Failsoft gateways do not belong to a channel group.

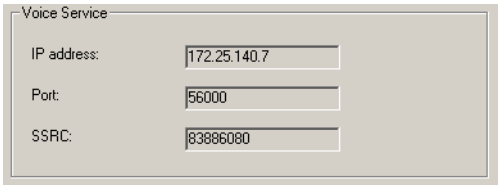
Display	Description
Connected	The channel group is connected to a trunking site controller. It has a master.
Isolated	The channel group has no connection to a trunking site controller.
Failsoft	The channel group has lost its connection to the trunking site controller and is now in Failsoft mode. If the member you are connected to is not the failsoft repeater, another member must be.

Speech

A green LED indicates that the channel group is passing speech via the failsoft repeater. Inbound speech is from a SU to dispatch equipment. Outbound speech is from the dispatch equipment to one or more SUs.

Voice service

The Voice service area in the Failsoft Mode form displays information about the voice service that the failsoft gateway or failsoft repeater is providing.



IP address

The IP address to which the failsoft gateway or failsoft repeater will send voice streams.

Port

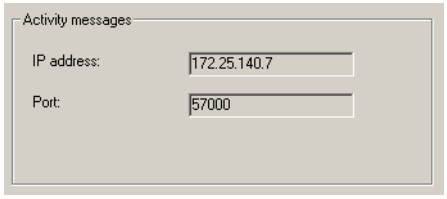
The UDP port to which the failsoft gateway or failsoft repeater will send voice streams.

SSRC

The decimal value of the SSRC (synchronization source) currently being used. It uniquely identifies voice streams sent from the failsoft gateway or failsoft repeater.

Activity messages

When the network element is active as a failsoft repeater or failsoft gateway, it sends activity messages to the trunked network's group control tree.



IP address

The IP address that activity messages are being sent to. This address is specified by the failsoft configuration (Configure > Network Interfaces > Failsoft).

Port

The port that activity messages are being sent to. This address is specified by the failsoft configuration (Configure > Network Interfaces > Failsoft).

Monitoring the DFSI Interface

Using the DFSI form (Monitor > Interfaces > DFSI), you can monitor the operation of the interface between digital dispatch equipment and a channel group. The CSS must be connected to the channel group member with the DFSI (digital fixed station interface).

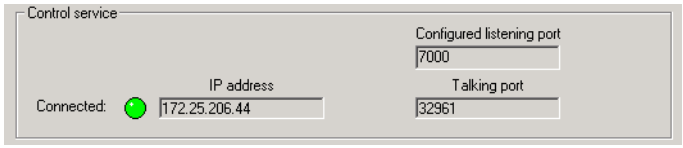
Status

The Status LED and box indicate the status of the network element's digital fixed station interface (DFSI).

LED	Display	Description
Red	No license	The member does not have a DFSI feature license. It cannot provide a DFSI interface.
	Configuration disabled	Configuration has not enabled the member to provide a DFSI interface (Configure > Network Interfaces > DFSI).
Gray	Enabled	The member is able to provide a DFSI interface but the interface is not currently active.
Green	Active	The member is currently providing a DFSI interface.

Control service

The Control service area monitors the control service provided by the DFSI.



Connected

A green LED indicates that the DFSI is active. The network element has received a connect message and has responded to it. It is able to receive and action control commands from the FSH.

IP address

The IP address of the FSH control service.

Configured listening port

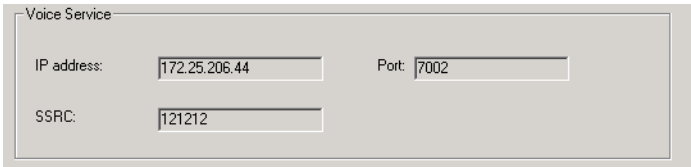
The port on which the network element is listening for DFSI communications. This port is defined by configuration.

Talking port

The port that the network element sends its control service communications to. The network element obtains this port number from the FSH.

Voice service

The Voice service area monitors the voice service provided by the DFSI. (If the network element has a TCCP connection, the Voice service and Traffic areas will display voice service information, but this should not be relied upon. Use the TCCP form instead.)



IP address

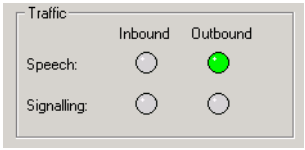
The IP address that the network element sends voice streams to. Depending on the configuration, this could be the control service IP address or a different unicast or multicast address.

Port — The UDP port that the network element sends voice streams to. It obtains this port number from the connection message.

SSRC — The SSRC (synchronization source) currently being used. The SSRC is a large number specified by the FSH in its connection message. It uniquely identifies voice streams sent from the channel group master to the FSH.

Traffic

The Traffic area indicates the types of communication that the DFSI is carrying.



Speech — A green LED indicates that the DFSI is carrying speech. Inbound speech is from a SU to the FSH, outbound speech is from the FSH to one or more SUs.

Signaling — The LED lights green briefly to indicate that a TSBK was sent or received.

Monitoring the CSSI Interface

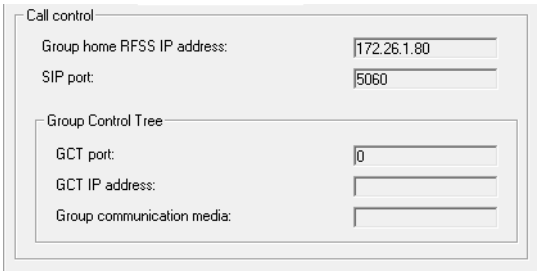
Using the CSSI form (Monitor > Interfaces > CSSI), you can monitor the operation of the trunked analog gateway's console subsystem interface (CSSI) to the RFSS controller. This form is not used with base stations or P25 console gateways.

Status — The Status LED and box indicate the status of the trunked analog gateway's CSSI interface.

LED	Display	Description
Gray	No license	The network element does not have a CSSI feature license. It cannot provide a CSSI interface. Make sure that it is a trunked analog gateway.
Red	Configuration disabled	Configuration has not enabled the gateway to provide a CSSI interface (Configure > Network Interfaces > CSSI).
	Not connected	The gateway is not connected to an RFSS controller.
	Standby	The network element is in Standby mode.
Green	Connected	The gateway is connected to its RFSS controller.

Call control

The Call control area displays the configured gateway settings used for call control. For information about configuring these items, see "CSSI Interface" on page 168.



Group home RFSS IP address
: The IP address of the RFSS controller application that the trunked analog gateway is currently connected to. This is the home RFSS controller of the gateway's talk group. The trunked analog gateway can only connect to an RFSS controller if it is defined in the list of RFSS controllers (Configure > Analog Line > RFSS) and selected for the group that the trunked analog gateway belongs to (Configure > Analog Line > MDC1200 Addresses).

SIP port
: UDP port number that the gateway uses for sending and receiving SIP messages. The trunked analog gateway uses the SIP protocol for registration with its home RFSS and for call control.

Group control tree

The Group control tree area displays the following configuration settings if the gateway is configured for operation with a privileged RFSS.

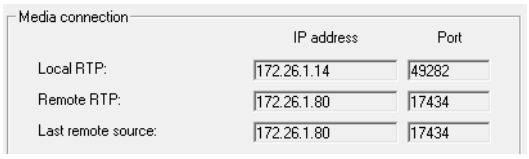
GCT port
: UDP port number that the gateway uses for sending and receiving control messages relating to the setup and clearing down of group calls. These messages use the proprietary group control tree protocol.

GCT IP address
: IP address that the gateway uses for group control tree protocol messages as described above.

Media base IP address
: The base multicast IP address that the gateway uses to compute the multicast address to use with a group call voice stream.

Media connection

The Media connection area displays information about the voice stream. Fixed information is always displayed. Variable information is displayed when the call is active.



Local RTP
: The destination IP address and port being used by inbound RTP packets.

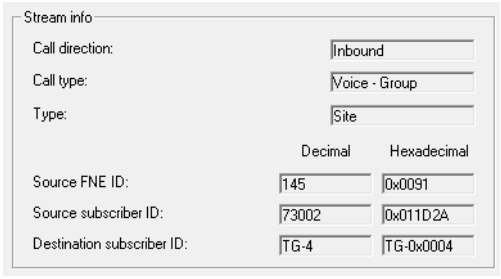
Remote RTP
: The destination IP address and port that the gateway uses for RTP packets it sends.

Last remote source

The source IP address and port in the RTP packets that the gateway is currently receiving or last received. If the gateway is connected to a standard RFSS, this information will be the same as the Remote RTP field above. If the gateway is connected to a privileged RFSS, the Remote RTP field will give the multicast address and port used by the RVP, while the Last remote source field will give the IP address and port of the site controller or IMG supplying the voice stream.

Stream info

The Stream info area provides detailed information about the voice stream that is currently passing through the gateway.



Call direction

Indicates whether the call is inbound (from the infrastructure to the console) or outbound (from the console to the infrastructure).

Call type

Indicates whether the call is voice, group voice or data.

Source type

Indicates whether the voice stream originated from a dispatch console or from a site (ultimately from an SU).

Source FNE ID

The identification number of the site or RFSS controller that is providing the inbound stream.

Source subscriber ID

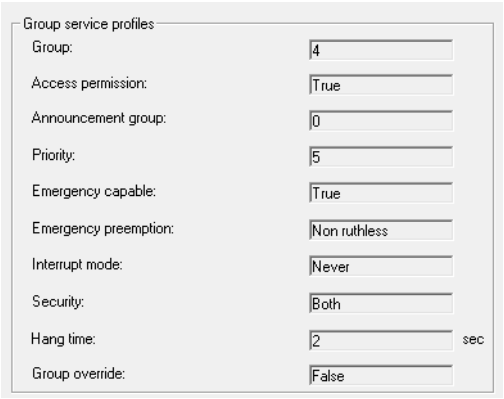
The SUID of the calling party.

Destination subscriber ID

The SUID or SGID of the called party. If this is a group, the number is prefaced by 'TG.'

Group Service Profiles

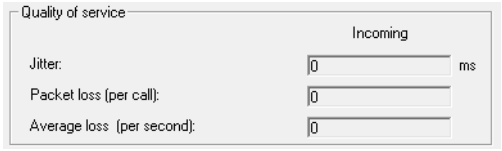
The Group Service Profiles area displays information about the service that the trunked network will provide for calls to the group that the trunked analog gateway belongs to. The RFSS controller provides this information to the gateway when it registers with the controller.



Group	The ID of the group that the trunked analog gateway currently belongs to.
Access permission	Indicates whether non-emergency calls can be made to the group.
Announcement group	Displays the ID of the announcement group that the group belongs to. 0 means that no announcement group is defined.
Priority	Indicates the priority level that the RFSS controller will assign to calls to the group.
Emergency capable	Indicates whether emergency calls can be made to the group.
Emergency preemption	Indicates whether ruthless or non-ruthless (smooth) preemption is used by emergency calls to the group.
Interrupt mode	Defines the conditions under which one member of the group can interrupt another during a group call.
Security	Indicates what kind of security is allowed in calls to the group. This can be clear calls only, secure calls only, or both types of call.
Hang time	The duration in seconds for which the system waits after voice ends before canceling the assignment of the traffic channel to the call. This duration is configured in the core network for the particular group and communicated to the gateway.
Group override	Indicates the associated group override setting for the group that the gateway is registered with on the trunked network. When this setting is enabled, call setup time for outgoing announcement calls is increased to give radios time to leave an existing group call. The gateway does this by applying the System call additional transmission delay.

Quality of Service

This area displays quality of service values for the current over's incoming voice stream on the CSSI interface. If an over is long, its values reset every 20 s.



Jitter (ms)

The peak delay variation of RTP packets arriving at the gateway. A high jitter is a sign that the network is congested.

This value does not accurately measure the jitter of the linking infrastructure. It includes delay variation in the sending of packets and is measured after processing in the network element.

Packet loss (per call)

The number of packets lost in the current voice over. Packet loss should be rare. Users will not notice a loss of up to 10 packets. Packet losses may be caused by inadequate linking bandwidth, cable faults, or power cycling of the switch or router.

Average loss (per second)

The average number of packets lost per second during the current over. Packet losses should be rare. Frequent packet loss indicates that there is something wrong with the linking infrastructure.

Group call diagnostics

This area displays diagnostic information about group calls. It is useful for determining whether faults in the routed multicast network are causing group calls to fail. The counters indicate the number of occurrences since the last reset.

No GCT payload

The number of times that voice for a group call has arrived at the gateway when a GCT payload message has not been received. This message should arrive before voice, to set up the call. Significant numbers mean that there are too many call control packet losses on the routed multicast network.

PTT request timeout

The number of times that a PTT request timed out without the originator receiving a grant or a deny. The dispatcher (outbound direction) or an SU user (inbound direction) has pressed PTT, causing a PTT request to be sent. The cause is either packet loss across the network or failure of the IMG.

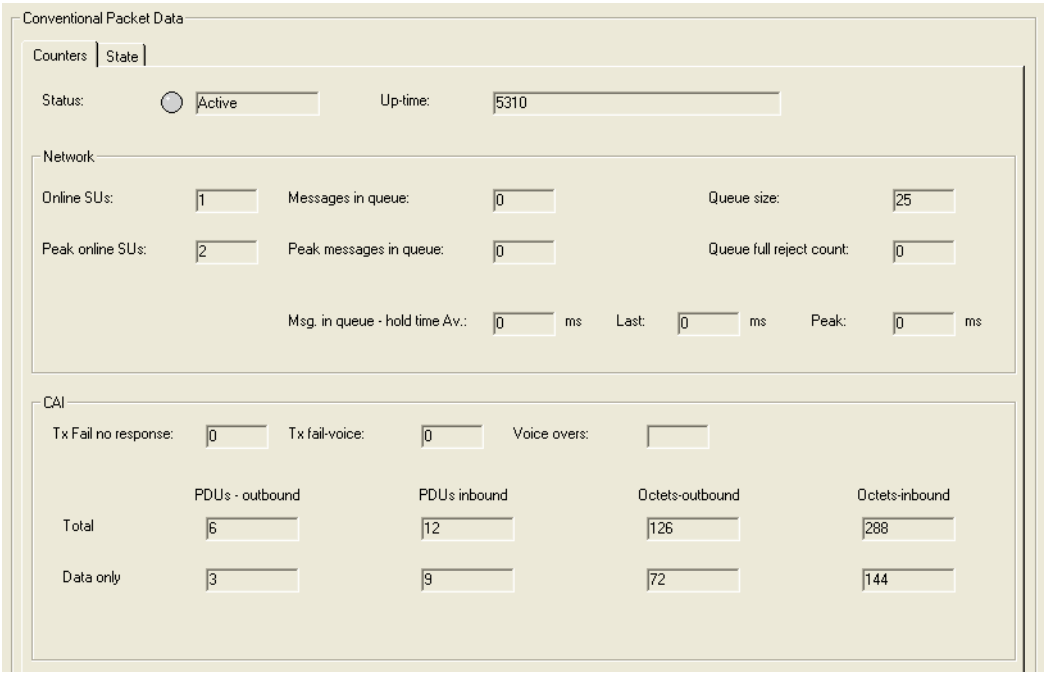
PTT denied

The number of times that the dispatcher's PTT request was denied. High numbers indicate that there are not enough traffic channel resources in the system or that the dispatcher is attempting to preempt a talkgroup member with higher priority.

Monitoring Conventional Packet Data

You can monitor network elements that are functioning as a data gateway. Data gateways are not used in trunked networks.

If the connected network element is functioning as a data gateway, select Monitor > Interfaces > Conventional Packet Data to monitor the data gateway and the flow of packet data across it. You can check that the data gateway is operating correctly and ascertain whether its channel is overloaded.



Two tabs provide information about the data and about the state of the data gateway and its interfaces. Quantities in these tabs often indicate a total for the up-time of the data gateway. If they exceed the maximum that the gateway can store, they begin again from 0.

Counters

The Counters tab displays quantitative information about the data passing through the data gateway.

Status

The current status of the data gateway.

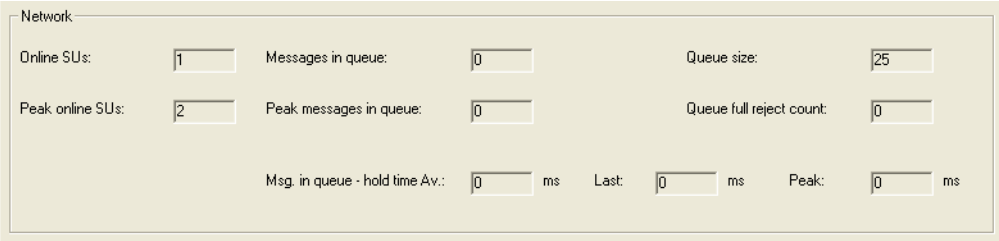
Display	Description
Active	The data gateway is active. It will respond to data packets that it receives.
No license	The network element does not have a data gateway license. It cannot function as a data gateway.
Not enabled	Configuration has not enabled the data gateway function.
Down trunked channel	The network element cannot be a data gateway as it is currently a trunked channel.

Up-time

The length of time since the network element began operating as a data gateway. The format is days-hours-minutes. The up-time began when the network element last entered Run mode, took over as central voter, was enabled as a data gateway, or was powered up.

Network

The Network area displays information about the radios registered with the home agent and the queue of data waiting for transmission.



Online SUs

The number of radios currently registered with the home agent via the gateway.

Peak online SUs

The highest number of radios that have been simulaneously online.

Messages in queue

The number of messages currently in the gateway's queue, waiting to be transmitted.

Peak messages in queue

The highest number of messages that have ever been in the queue.

Queue size

The configured maximum number of messages that the gateway can queue.

Queue full reject count

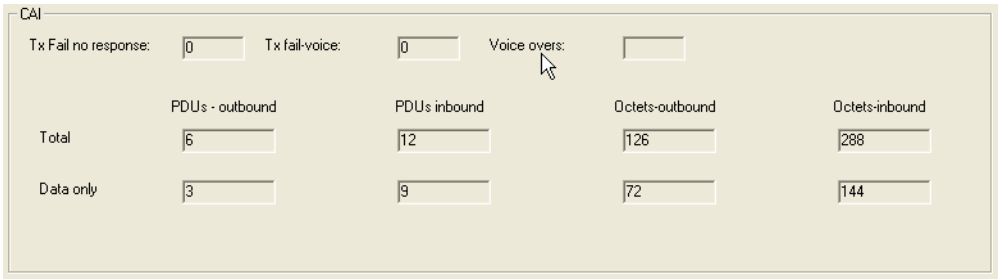
The number of messages that have been rejected because the queue was full.

Msg in queue - hold time

Three boxes display information in milliseconds about the length of time that messages were held in the queue before being transmitted. **Av** displays the average length of time, **Last** displays the length of time for the most recent queued message, and **Peak** displays the longest length of time.

CAI

The CAI area displays information about the data that has passed over the common air interface to and from SUs.



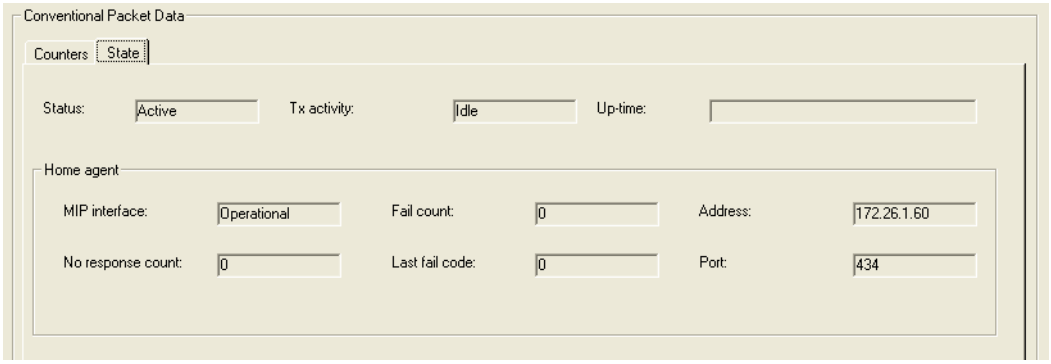
Tx fail - no response

The number of messages that failed to reach the SU; no response was received from the SU.

Tx fail - voice	The number of messages that failed to reach the SU because voice pre-empted the channel. The configured number of retries were carried out but were not successful.
Voice overs	The number of voice overs that occurred on the packet data gateway's channel. The more voice traffic there is, the less bandwidth is available for packet data.
Total	The Total row displays information about the total amount of data that was transferred over the CAI. You can compare this with the equivalent Data only amount shown underneath, to get an indication of the amount of overhead that the CAI is adding to the data, and hence the number of retries.
Data only	The Data only row displays information about the net amount of data (actual data payload) that has been transferred over the CAI.
PDUs - outbound	The number of packet data units that have been sent from the data gateway to SUs.
PDUs - inbound	The number of packet data units that the data gateway has received from SUs.
Octets - outbound	The number of octets that the data gateway has sent to SUs.
Octets - inbound	The number of octets that the data gateway has received from SUs.

State

The State tab displays information about the status of the packet data gateway and its interfaces.



Status	The current status of the data gateway.

Display	Description
Active	The data gateway is active. It will respond to data packets that it receives.
No license	The network element does not have a data gateway license. It cannot function as a data gateway.
Not enabled	Configuration has not enabled the data gateway function.
Down trunked channel	The network element cannot be a data gateway as it is currently a trunked channel.

Tx activity

The type of transmit activity that is currently occurring over the CAI on the data gateway's channel.

Display	Description
Data	The gateway is sending packet data
Idle	The gateway is not sending anything
Voice	The network element is sending voice. Voice has pre-empted any packet data in the queue.
Voice hang	The network element is currently not sending anything. It must wait for the voice hang timer to expire before sending packet data.
LCW	The network element is currently sending link control words to give information about the status of the uplink.

Up time

The length of time since the network element began operating as a data gateway. The format is days-hours-minutes. The up-time began when the network element last entered Run mode, took over as central voter, was enabled as a data gateway, or was powered up.

Home agent

The Home agent area displays information about the data gateway's interface to the home agent.

MIP interface

The state of the mobile IP interface between the data gateway and the home agent.

Display	Description
Operational	The gateway has recently received data or acknowledgements from the home agent.
Idle	The gateway is not sending anything to the home agent.
HA no response	The gateway has sent data to the home agent but received no response.
Failure	The gateway did not successfully complete the startup procedures for setting up its mobile IP interface. Double-check the gateway's configuration settings for the home agent, especially its authentication (SPI and Key). If this does not solve the problem, send the network element to an authorized Tait service center.

No-response count

The number of times that the data gateway sent a message to the home agent and received no response. This number is counted from the last response received.

Fail count

The number of times that the gateway received a failure code from the home agent. This number is counted from gateway power up.

Last fail code

The hexadecimal value of the last failure code received from the home agent.

Address

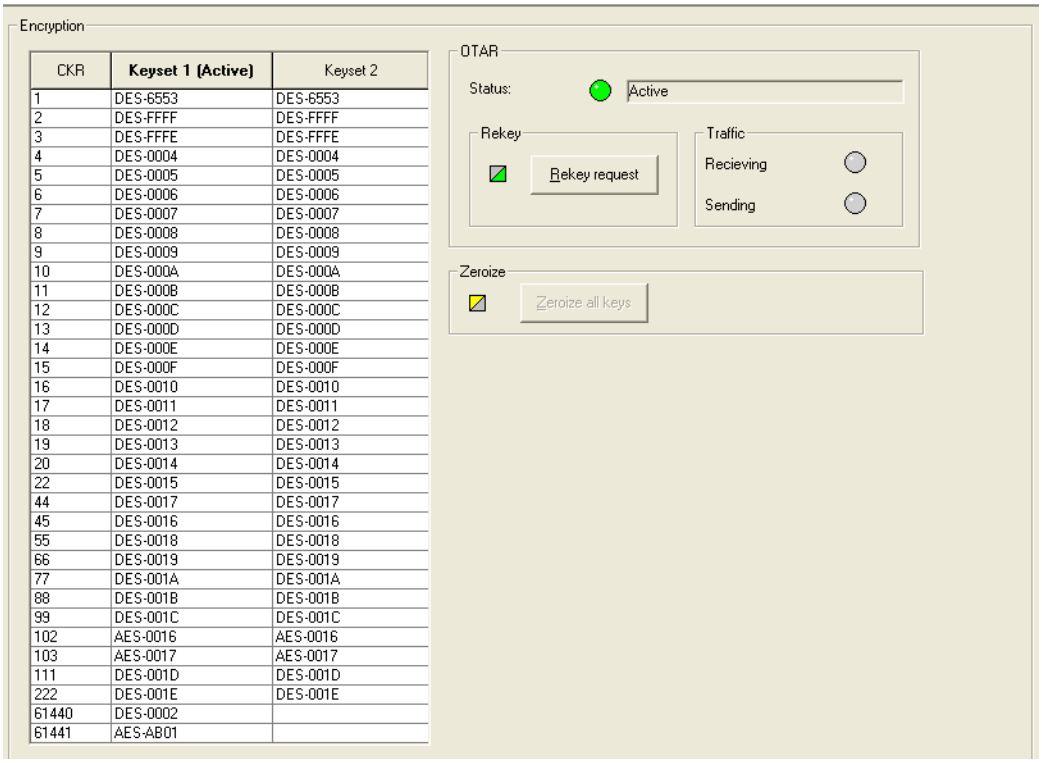
The IP address that the gateway is configured to use when communicating with the home agent.

Port

The port number that the gateway is configured to use when communicating with the home agent.

Monitoring Encryption

The Encryption screen (Monitor > Interfaces > Encryption) displays the keys that are currently in the gateway and monitors the status of OTAR communications.



CKR	Keyset 1 (Active)	Keyset 2
1	DES-6553	DES-6553
2	DES-FFFF	DES-FFFF
3	DES-FFFE	DES-FFFE
4	DES-0004	DES-0004
5	DES-0005	DES-0005
6	DES-0006	DES-0006
7	DES-0007	DES-0007
8	DES-0008	DES-0008
9	DES-0009	DES-0009
10	DES-000A	DES-000A
11	DES-000B	DES-000B
12	DES-000C	DES-000C
13	DES-000D	DES-000D
14	DES-000E	DES-000E
15	DES-000F	DES-000F
16	DES-0010	DES-0010
17	DES-0011	DES-0011
18	DES-0012	DES-0012
19	DES-0013	DES-0013
20	DES-0014	DES-0014
22	DES-0015	DES-0015
44	DES-0017	DES-0017
45	DES-0016	DES-0016
55	DES-0018	DES-0018
66	DES-0019	DES-0019
77	DES-001A	DES-001A
88	DES-001B	DES-001B
99	DES-001C	DES-001C
102	AES-0016	AES-0016
103	AES-0017	AES-0017
111	DES-001D	DES-001D
222	DES-001E	DES-001E
61440	DES-0002	
61441	AES-AB01	

You can click on a column header to sort the table by that column.

CKR

The common key reference for a set of key material. Each key has a CKR. When the key is updated, the CKR stays the same. To see the key name that has been assigned to this CKR, select Configure > Analog Line > Encryption.

CKRs with the default numbers 61440 and 61441 are for the UKEKs used for communicating keys securely from the KMF to the network element.

Keyset 1and Keyset 2

The Keyset 1 and Keyset 2 columns display the keys that are in each keyset. Each column shows the encryption algorithm followed by the key ID, for example:

AES-011A

(Active) in the column name, together with bold formatting, indicates that the keyset is active. The gateway uses the keys in the active keyset to encrypt and decrypt calls. It only uses keys in the inactive keyset for decrypting incoming calls that were encrypted using non-current keys.

OTAR

The OTAR area lets you monitor the operation of OTAR communications with the KMF. You can also rekey the network element or zeroize its keys.

LED	Display	Description
Gray	No license	The network element does not have the feature licenses needed to support OTAR.
	No crypto	The network element has no crypto-module. It is not crypto-capable.
Red	Standby	The network element is in Standby mode.
	Not enabled	OTAR is not enabled in configuration (Configure > Analog Line > Encryption).
	Bad configuration	The OTAR configuration is corrupt.
	KMF not responding	The network element has communicated with the KMF but not received a response.
Green	Active	OTAR communications are operative.

Rekey request

Click Rekey request to instruct the network element to ask the KMF to send the complete set of keys.

Under normal circumstances, the KMF will automatically update the network element's keys, so that the use of this command is not necessary. If there is reason to suspect that the network element's keys are not current, you can use this command to have the KMF re-send the current keys.

Flashing LEDs in the Traffic area indicate that the KMF has responded to the request.

Zeroize

Click Zeroize all keys to remove all the secure key data that has been loaded by a key fill device.

To maintain security, we recommend zeroizing all key data before sending a gateway module for repair. It is also possible to zeroize all keys before loading new key data, to make sure that all obsolete key data is removed.

After zeroizing, in order to restore encryption keys in a network element you need to load provisioning keys using a KFD. Once this is done, the KMF can supply all the current keys automatically using OTAR.

Traffic

The LEDs in the Traffic area display green when the network element is receiving or sending OTAR messages.

Channel Group

The CSS can monitor information about the whole channel group. Status information is provided by the channel group member that the CSS is connected to and is displayed in tables, with one row of information for each channel group member. The CSS also displays status information about the channel coordinator of the member that the CSS is connected to.

Monitoring Channel Group Status

The Group Status form (Monitor > Channel Group > Status) provides two different views of the channel group. The Dynamic view tab displays information on channel group members that are currently receiving an RF stream. The base station you are connected to must be aware of these streams to provide the information. If the base station you are connected to is the central voter then all (up to 14) receiving channel group members are shown. A satellite receiver may only show itself.

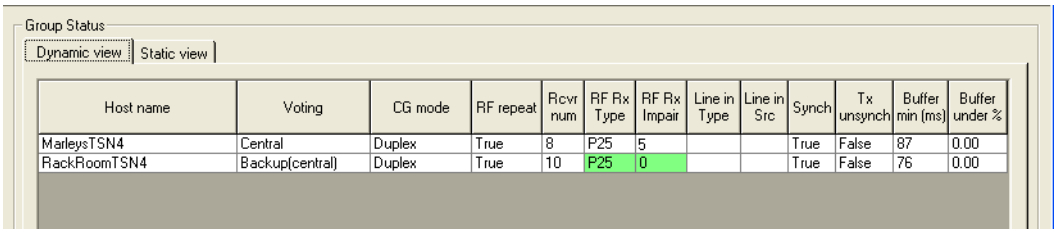
The information displayed is passed from other channel group members to the connected member using the RTCP protocol. The connected member supplies the information to the CSS.

Channel Group Dynamic View

The Dynamic view tab (Monitor > Channel Group > Status) monitors the operation of the channel group in real time. It consists of two tables. The first displays the dynamically changing information, in particular that relating to voting and simulcast, while the second displays relatively unchanging information. The display can handle up to 14 simultaneously receiving members.

Connect the CSS to the central voter; satellite voters do not indicate who is winning the vote.

First Table



Green cells indicate the voice stream that has won the vote or been selected. If the channel group is duplex, there can be a winning inbound (subscriber) stream and an outbound (dispatcher) stream.

A red cell indicates that digital dispatch equipment has de-selected the member using a DFSI interface so that the member does not participate in the vote.

Host name — The name of the channel group member.

Voting — The type of voting taking place at each channel group member.

Display	Description
Distributed	Voting is distributed among all channel group members. The central voter has failed and no other member is capable of acting as a replacement.
Central	Voting is centralized at this channel group member. All other channel group members should display 'satellite' or 'Backup (central).' Only one member should display 'central voter' at any one time.
Satellite	This channel group member has acknowledged that another channel group member is the central voter. This member plays a supporting role to the central voter.
Distr(central)	This channel group member is currently operating as a distributed voter but is configured for central voting. It is therefore a candidate central voter but something is preventing central voting.
Backup (central)	This channel group member is currently operating as a satellite voter but is configured for central voting. Another channel group member is acting as the central voter.
Standby	The member is in Standby mode. Normal voting and switching does not operate. However, the control panel can still receive and make calls. These calls will only be visible in the table if the CSS is connected to this member or to the central voter.

A cell with a colored background indicates that a dispatcher command has modified the member's voting behavior.

Display	Description
green	The dispatcher has selected the member's receiver. This receiver's signal will always win the vote. If this receiver has no signal, the channel group votes as it is configured to do.
red	The dispatcher has disabled the member's receiver. The receiver's signal cannot win the vote.

CG Mode

Displays the mode of the channel group.

Display	Description
duplex	The channel group can simultaneously handle an inbound (subscriber to dispatcher) and an outbound (dispatcher to subscriber) voice stream.
simplex	The channel group provides a single voted or selected stream at any one time. If the dispatcher is talking, subscribers cannot be heard.

RF repeat

Indicates whether the member currently repeats the vote-winning output or not. This can be set by configuration, by dispatcher command, by Task Manager action, or by a trunking site controller instruction to be a control channel.

Rcvr num

Displays the receiver number of the channel group member. This number is used by digital dispatch equipment, when the dispatcher selects or disables a receiver. It is also used in voting. Voice streams from members with a lower receiver number win the vote (or are selected) when other things are equal.

RF Rx Type

Displays whether the call is digital P25 or analog FM. A 'U' indicates that the call is ungated; the network element is in monitor mode.

If this and the adjacent cell has a green background, the RF stream is winning the vote.

RF Rx Impair

Displays the impairment value of the received signal. Impairment is a number between 0 and 15. It is the inverse of signal quality. For digital P25 calls, the impairment is based on the EMV value of the received signal. For analog FM calls, it is based on an internal measure similar to SINAD.

The central voter determines which signal wins the vote, based on the number of errors reported by the receiver's vocoder.

Line In Type

Displays the type of call coming from the line in. This can be digital P25 or analog FM.

Line In Src

Displays the source of the call coming from the 'line in.'

Display	Description
Dig	A digital voice service (DFSI, trunking, or failsoft)
Ana	Analog line
CP	Control panel microphone

Synch

Indicates the synchronization status of the transmitter. True means that the transmitter is synchronized, False that the transmitter is not synchronized. A simulcast transmitter should display True. If it displays False, connect to it and select Monitor > Synchronization > Simulcast to see the reason why it is not synchronized. Non-simulcast transmitters are always unsynchronized.

Tx unsynch

Indicates whether the base station is configured to transmit when it or the central voter is unsynchronized or the voice stream arrives late.

Buffer min (ms)

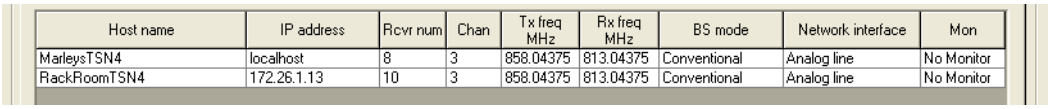
Displays the lowest buffer size over the current or most recent voice over. If the central voter in a simulcast channel group uses fixed marshalling, the marshalling duration needs to be large enough to ensure that the smallest buffer size exceeds the desired minimum. If the central voter uses self-regulating marshalling, it will regulate the size of the furthest member's buffer around the configured buffer minimum.

Buffer under %

The percentage of packets during the last 15 minutes that arrived late enough to cause a buffer underflow. If this value is too high, lengthen the preamble (unsynchronized channel groups), increase the Buffer min value (synchronized channel groups with self-regulating marshalling), or increase the fixed marshalling duration at the central voter (synchronized channel groups with fixed marshalling duration).

Second Table

The second table in the Dynamic view tab (Monitor > Channel Group > Status) displays additional, more unchanging information about all channel group members.



Host name	IP address	Rcvr num	Chan	Tx freq MHz	Rx freq MHz	BS mode	Network interface	Mon
MarleysTSN4	localhost	8	3	858.04375	813.04375	Conventional	Analog line	No Monitor
RackRoomTSN4	172.26.1.13	10	3	858.04375	813.04375	Conventional	Analog line	No Monitor

Most of this information is common to the Static view tab. The following are unique to the Dynamic view tab.

Network interface

Indicates whether the member is providing the channel group with an external network interface.

Display	Description
None	There is no channel group interface other than the RF interface and the control panel.
Analog line	The member has an active analog line interface, for example to analog dispatch equipment. (By default, all analog lines are active. To 'deactivate' an an unused analog line so that it does not appear in this column, select Configure > Analog Line > Calling Profiles and disable its calling profiles.)
DFSI	The member has an active digital fixed station interface, for example to digital dispatch equipment.
TCCP ctrl	The member has an active TCCP control interface to a trunking site controller. It is the channel group master.
TCCP status	The member has an active TCCP status interface to a trunking site controller. It is not the master.
FS reptr	The member is acting as a failsoft repeater.

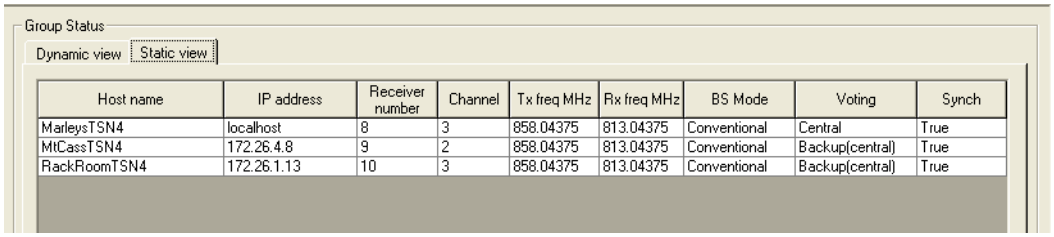
Mon

When Monitor appears in this column, the base station is in monitor mode. Monitor mode overrides any selective squelch at the analog line and disables the receiver's filters for NAC, CTCSS and DCS. The receiver will unmute irrespective of the signal's NAC or analog subaudible signaling. However, the receiver still applies gating to analog FM calls based on RSSI and/or SINAD.

The DFSI supports dispatcher commands that enable or disable monitor mode. The analog line can also control monitor mode, via suitable Task Manager tasks. Monitor commands can control the monitor mode of the whole channel group, if that control is set to collective in each member's channel group configuration.

Channel Group Static View

The static view of the channel group helps you check that all members of the channel group have a consistent configuration. This is particularly useful during network installation. Many settings need to be the same for all channel group members.



Host name — The name of the channel group member. Check that each name is unique.

IP address — The IP address of the channel group member.

Rcvr num — The receiver number of the channel group member. This number is used by digital dispatch equipment, when the dispatcher selects or disables a receiver. It is also used in voting. Voice streams from members with a lower receiver number win the vote (or are selected) when other things are equal. Make sure that each channel group member has a unique number.

Chan — The member's current operating channel. Normally, all members are set up to operate on the same channel number. If the channel group is set up to handle channel change commands from the dispatcher, monitor this column when testing these commands.

Tx freq MHz — The transmit frequency of the member's current channel.

Rx freq MHz — The receive frequency of the member's current channel.

BS Mode — The current mode of the channel group member.

Display	Description
Control channel	The base station is functioning as part of a trunking control channel.
Traffic channel	The base station is functioning as part of a traffic channel.
Conventional	The base station is operating in conventional mode. The configuration of the current channel specifies Conventional, not Trunking (Configure > Network Element > Channel Table).
Down	The trunking controller has taken the channel group out of service. The base station will not receive or transmit.
Isolated	The channel group has lost its control connection to the trunking controller. There is no master.
Failsoft	The channel group is in failsoft mode.
Standby	The base station is in Standby mode. A CSS has taken it out of service.

Voting — The type of voting taking place at each channel group member.

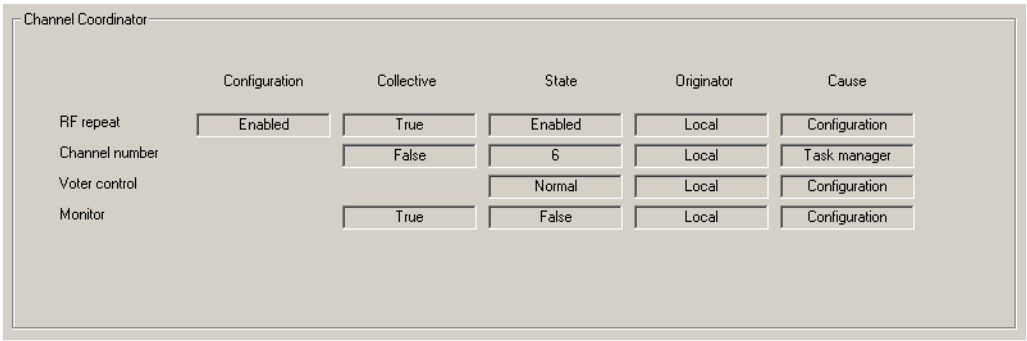
Display	Description
Distributed	Voting is distributed among all channel group members. If one member has this voting type, all others should have the same type.
Central	Voting is centralized at this channel group member. All other channel group members should display 'satellite' or 'Backup (central).' Only one member should display 'central voter' at any one time.
Satellite	This channel group member has acknowledged that another channel group member is the central voter. This member plays a supporting role to the central voter.
Distr(central)	This channel group member is currently operating as a distributed voter but is configured for central voting. It is therefore a candidate central voter but something is preventing central voting.
Backup (central)	This channel group member is currently operating as a satellite voter but is configured for central voting. Another channel group member is acting as the central voter.
Switched	There is no RF voting, but the channel group member still selects or prioritizes voice streams. This setting is appropriate if the channel group receivers do not have a common uplink frequency.
Standby	The member is in Standby mode. Normal voting and switching does not operate. However, the control panel can still receive and make calls. These calls will only be visible in the table if the CSS is connected to this member or to the central voter.

Synch

Indicates the synchronization status of the transmitter. True means that the transmitter is synchronized, False that the transmitter is not synchronized. A simulcast transmitter should display True. If it displays False, connect to it and select Monitor > Synchronization > Simulcast to see the reason why it is not synchronized. Non-simulcast transmitters are always unsynchronized.

Monitoring the Channel Coordinator

The Channel Coordinator form (Monitor > Channel Group > Channel Coordinator) monitors the operation of the channel coordinator in the channel group member that the CSS is connected to. The form displays the current state of the variables that are coordinated (RF repeat, Channel number, Voter control and Monitor—the dispatcher command) and indicates who is responsible for that state and what caused it. For more information about the channel coordinator, see the TaitNet P25 Conventional System Manual.



In some situations, this form may display incorrect information. For example, in a centrally voted channel group, the originator of a channel change command can be incorrectly displayed as the central voter. When connected to a member with a high receiver number that has requested a channel change, the CSS indicates that the channel change came from another member via IP, when in fact it was local from Task Manager.

Configuration

Displays the configured setting for RF repeat.

Display	Description
Enabled	The entry in the channel table for the current channel enables RF repeat. RF repeat is enabled and cannot be disabled by collective control or by dispatcher command.
Disabled	The entry in the channel table for the current channel disables RF repeat. RF repeat is disabled and cannot be enabled by collective control or by dispatcher command.
DispatchControlled	The entry in the channel table for the current channel places RF repeat under dispatcher control. Dispatcher commands and collective control can determine the RF repeat state.

Collective

'True' means that the variable is under collective control; the coordinator will send channel control commands to and respond to commands from other channel group members. 'False' means that the variable is solely determined by the individual member; the channel coordinator does not affect the variable.

State

The current state of the variables under the control of the channel coordinator.

Variable	State	Description
RF repeat	Enabled	Repeat is enabled. The base station transmits streams from SUs over the RF interface.
	Disabled	Repeat is disabled. The base station does not transmits streams from SUs over the RF interface.
Channel number	nnn (for example 3)	The number of the channel that the member is currently operating on.
Voter control	Normal	Normal voter operation.
	Selected	A dispatcher command has selected this network element's receiver as the vote winner.
	Disabled	A dispatcher command has prevented this network element's receiver from winning the vote.
Monitor	False	A dispatcher Monitor command has not affected the base station's squelch behavior.
	True	A dispatcher Monitor command has overridden the channel profile's squelch setting and instructed the network element to use Normal squelch (see "Squelch" on page 184)

Originator

The network element responsible for the present state of the variable.

Display	Description
Local	The channel group member that the CSS is connected to is responsible for the present variable state.
nnn (for example 3)	The channel group member with receiver number *nnn* is responsible for the present variable state.

Cause

The cause of the present state of the variable.

Display	Description
Configuration	The present state of the variable is due to the local configuration.
Task Manager	The present state of the variable is due to Task Manager action, triggered for example by an analog dispatch console command.
DFSI	The present state of the variable is due to a command from a digital dispatch command, received over the local DFSI interface.
power up	The present state of the variable resulted from power up.
IP	The present state of the variable resulted from a command sent over IP from another network element

Synchronization

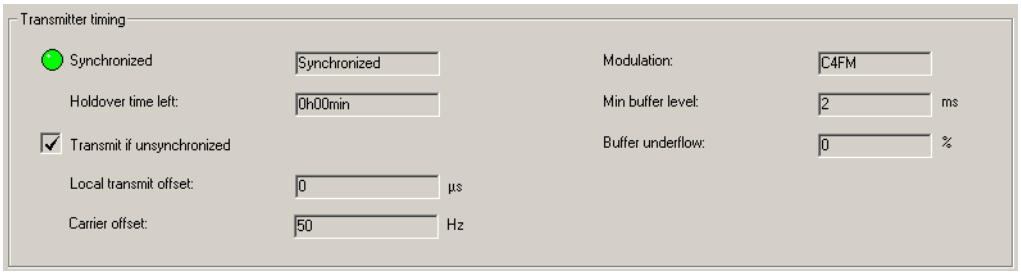
The CSS can monitor the synchronization of the transmitter, the central voter, and the streams that the network element is receiving.

Monitoring Simulcast

Using the Simulcast form (Monitor > Synchronization > Simulcast), you can monitor the simulcast timing of the transmitter and of the voice stream. If the CSS is connected to the central voter, you can monitor its timing.

Transmitter Timing

The Transmitter timing area provides information on synchronization at the transmitter.



Status

If the Status LED is green, the transmitter is synchronized. If the LED is red, the transmitter is unsynchronized. The box alongside provides details.

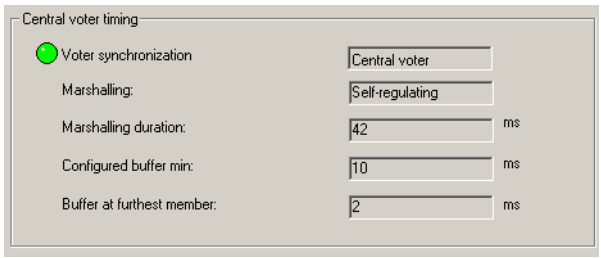
Display	Description
Synchronized	The transmitter is synchronized. It is able to synchronize its transmissions with the channel group.
No license	The member does not have a Simulcast Transmitter feature license.
Not configured	The current channel profile does not enable Simulcast.
Holdover	The member is in holdover mode. It has lost its 1 PPS signal but has not yet become unsynchronized.
1 PPS absent	The member has lost its 1 PPS signal and is unsynchronized.
Extref absent	The member has lost its external reference.
Extref invalid	The member has an external reference frequency but cannot lock onto its channel frequency using that reference. Either the reference source is faulty, or the member is configured to expect the wrong frequency (Configure > Network Element > Miscellaneous).
No H/W support	The member's hardware does not support synchronization. The digital board hardware must be version 00.07 or higher. Version 00.06 digital boards can be upgraded to 00.07.

Holdover time left	The time remaining before the configurable holdover time elapses. If this time elapses and the 1PPS source has not been restored, the transmitter becomes unsynchronized.
Transmit if unsynchronized	Indicates whether the member is configured to transmit when it, the central voter, or the arriving voice stream is unsynchronized.
Local transmit offset	Displays the configured local transmit offset in microseconds. This delays the launch time from the nominal time requested by the central voter.
Carrier offset	Displays the configured carrier offset in Hertz. The actual carrier frequency will differ from the configured transmit frequency by the configured amount.
Modulation	The modulation scheme that the transmitter is currently using. This is selected by the current channel profile.
Min buffer level	The lowest level of the transmit buffer, measured over a 5-second period.
Buffer underflow	The percentage of packets that did not arrive in time for synchronized transmission.

Central Voter Timing

If you are connected to the central voter, this area indicates whether the central voter is synchronized and displays the parameters that the central voter is using. Check that the Voter synchronization box displays Central voter, to confirm that you are connected to the central voter.

- If the Voter synchronization LED is red, the central voter is unsynchronized.
- If the Voter synchronization LED is green, the central voter is synchronized.



Voter synchronization

The LED monitors the synchronization state of the central voter. It is disabled if you are not connected to the central voter. The text box indicates whether the member is the central voter. The following can be displayed.

Display	Description
No license	The member does not have a networking feature license. It cannot send or receive voice data streams on its channel group interface.
Task Manager lock	Task Manager has locked the channel group. The member's channel group interface is disabled.
Standby	The member is in Standby mode, which takes it out of service, disabling the channel group interface.
Distributed voter	The member is functioning as a distributed voter within the channel group. The channel group lacks a functioning central voter.
Satellite voter	The member is functioning as a satellite voter within the channel group.
Central voter	The member is functioning as a central voter within the channel group.

Marshalling

Indicates the marshalling method set in configuration.

Display	Description
Fixed	The central voter uses a fixed marshalling duration when telling members when to transmit
Self-regulating	The central voter automatically adjusts the marshalling duration based on feedback from the furthest member

Marshalling duration

The current marshalling duration. This is fixed in configuration or regulated by the central voter, depending on the marshalling method used.

Configured buffer min

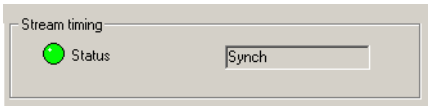
If marshalling is self-regulating, the central voter regulates around this as the minimum buffer level. It will adjust the marshalling duration to fill the buffer at the furthest member to this minimum level.

Buffer at furthest member

The level of the transmit buffer at the member that is furthest away from the central voter. It is the smallest transmit buffer of any channel group member. If marshalling is self-regulating, the central voter is responsible for ensuring that there are no buffer underruns. If marshalling is fixed, you must ensure that the marshalling duration is long enough to prevent buffer underruns.

Stream Timing

The LED and the box alongside provide information about the stream arriving at the channel group member.



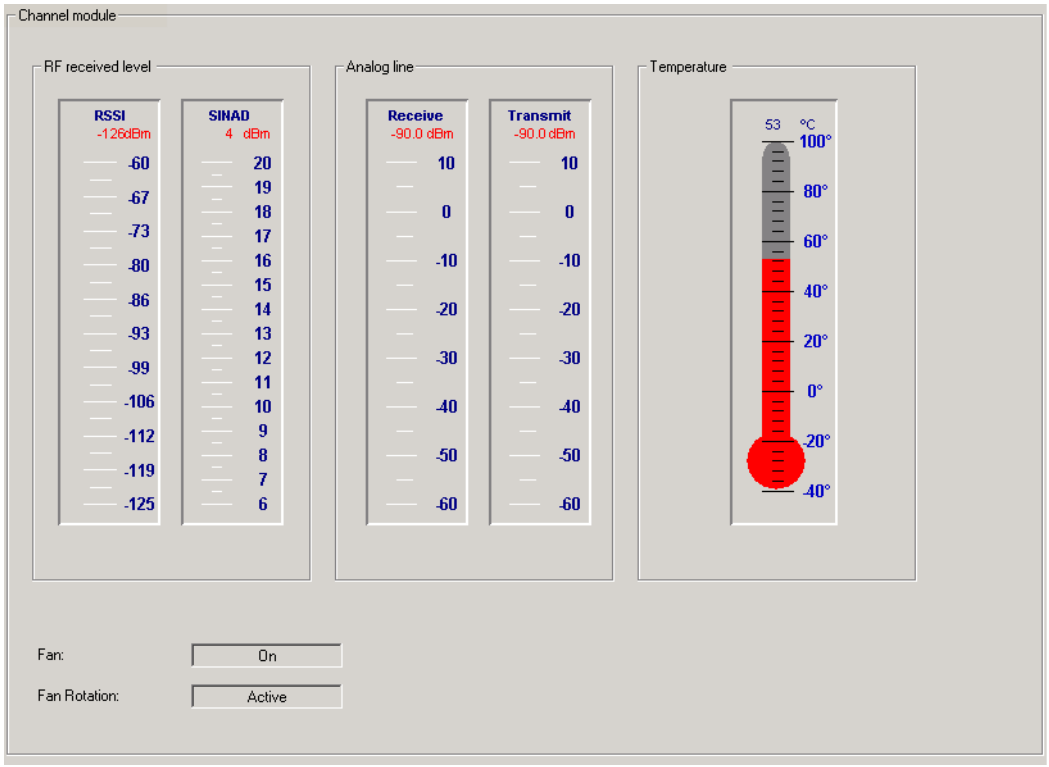
LED	Box	Description
Green	Synch	The stream is synchronized
Red	Unsync	The stream is unsynchronized (the central voter is unsynchronized)
	Late	The stream is synchronized but it is arriving too late for synchronized transmission
Gray		There is currently no stream

Modules

The CSS can monitor operational details about individual modules. These details include temperatures, currents, voltages, and other levels.

Monitoring the Reciter or Gateway Module

The Channel Module form (Monitor > Modules > Channel Module) monitors the RSSI and SINAD of the received RF signal and audio levels on the analog line. Each level is displayed graphically as a gauge. The equivalent numeric value appears under the gauge heading. If the value is red, it has exceeded the maximum or fallen below the minimum that the gauge can display.



RF received level — The RF received level area displays the RSSI and SINAD levels of the inbound RF signal. (For the equivalent RSSI in microvolts, see "Converting Between Microvolts and dBm" on page 141). The SINAD is only an estimation, obtained by measuring the out-of-band noise.

Analog line — The Analog line area displays the audio levels for the receive (line in) and transmit (line out) paths of the analog line.

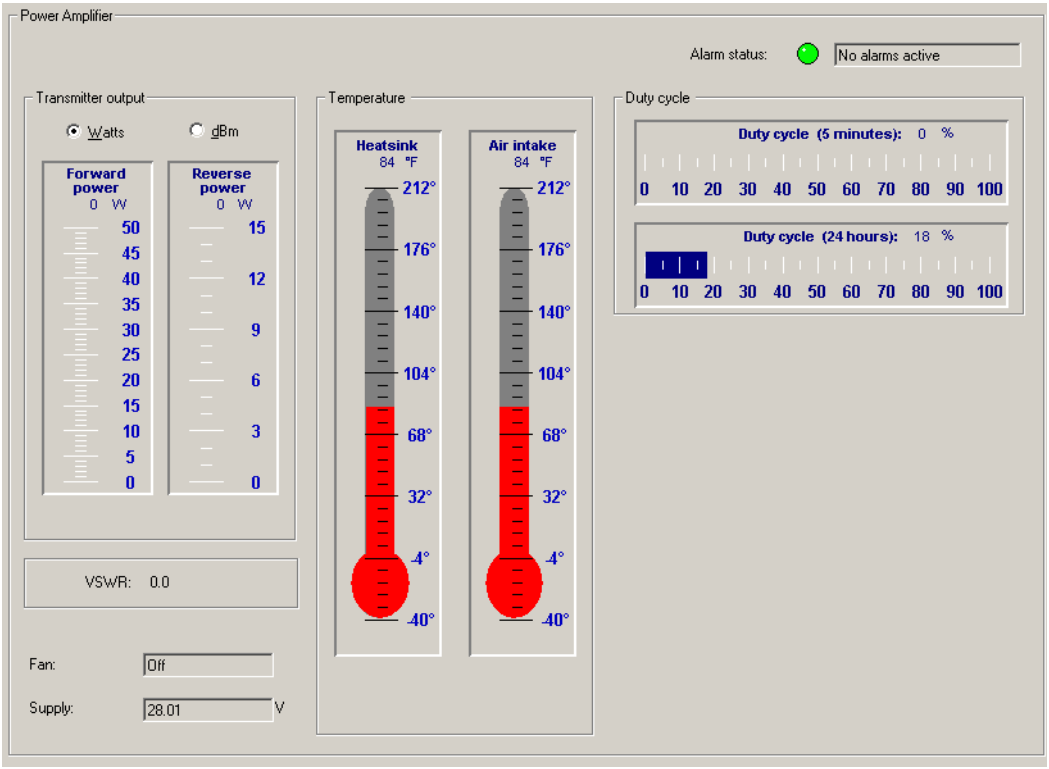
Temperature — The Temperature area displays a thermometer that shows the temperature measured at the channel module heatsink.

Fan — Displays whether the channel module has turned the fan on or off.

Fan rotation — Active means that the channel module has detected fan rotation. Inactive means that the fan has failed, if the **Fan** box displays On. This box does not apply if the channel module is fitted with a 2-wire fan.

Monitoring the Power Amplifier

The Power Amplifier form (Monitor > Modules > Power Amplifier) monitors the levels of various PA parameters. Some levels are displayed graphically as a gauge or thermometer. The equivalent numeric value appears in or under the heading. If a value goes off the scale, it turns red.



To switch the temperature display between Celsius and Fahrenheit, select Options > Settings.

Alarm status

The Alarm status box indicates whether the PA has an alarm. If the LED is red, select Monitor > Alarms > Status to see which alarm is active.

Transmitter output

The Transmitter output area displays the forward and reverse power. Click the Watts or dBm option to change the units of the display.

> The base station reports power values in 1 W increments. With a 5 W PA this can mean that the forward power gauge displays a power of 0 W when in fact the PA is operating at 0.99 W.

Heatsink temperature

Displays the highest of the three temperatures measured at the PA driver, Final 1, and Final 2 transistors. (The 5 W PA has no final transistors and the 50 W PA has no Final 2 transistor.)

Air intake temperature

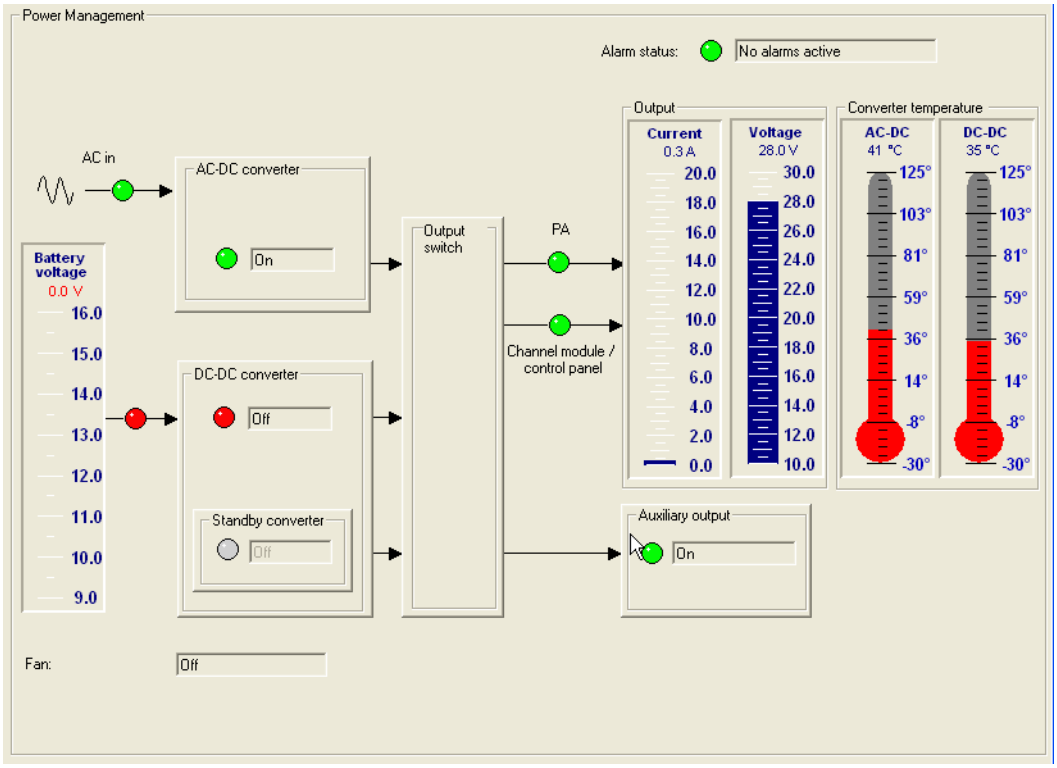
This thermometer displays the temperature measured at the air intake to the PA heatsink. If the PA is a 100 W PA, the value displayed will be approximately 10 to 15 degrees Celsius higher than the actual ambient temperature. In addition, the display can be misleading if the PA has been transmitting without the fan turned on: the displayed temperature will be much hotter than the actual air intake temperature. If the fan has been running for 30 seconds, the reading will be accurate.

Duty cycle	The Duty cycle area has two gauges. The first gauge indicates the average duty cycle over the past 5 minutes. 50% means that the PA was transmitting for 2.5 of the last 5 minutes. The display is updated once every minute. The second gauge indicates the average duty cycle over the past 24 hours. 25% means that the PA was transmitting for 6 of the last 24 hours. The display is updated once every hour. If the PA has been on for less than 24 hours but for more than 1 hour, the gauge displays the average duty cycle for the time that the base station has been operating.
VSWR	The VSWR displays the voltage standing wave ratio. If this is greater than 10:1, an alarm is triggered and the PA folds its output back to 10% of its capability. Only when the VSWR falls below 5:1 will the power output begin to recover.
Fan	Indicates whether the fan is on.
Supply	Displays the voltage of the power that the PMU is supplying to the PA.

Monitoring the Power Management Unit

The Power Management form (Monitor > Modules > Power Management) monitors the operation of the PMU. You can:

- Check the voltage of the battery and the current that the PMU outputs to the PA.
- Check the status of the PMU's inputs and outputs.



This form has gauges displaying the battery voltage, the output current, and the output voltage. Boxes represent different PMU submodules and LEDs indicate the status of power inputs and outputs. If a submodule is not fitted, the box alongside the LED is disabled.

Alarm status

The Alarm status box indicates whether there is a current alarm. If the LED is red and the box displays 'Alarms active', one or more PMU alarms have been triggered. Select Monitor > Alarms > Status to see which alarms are active.

Battery voltage

The battery voltage gauge indicates the voltage of the DC power supply to the PMU. The LED alongside indicates the state of the power supply.

LED	Description
Green	DC power input is usable
Red	DC power input is off (or too low or too high)
Gray	No battery power supply is fitted

AC-DC converter

The LED in the AC-DC Converter box indicates the state of AC power.

LED	Text	Description
Green	On	AC power input is usable
Red	Off	AC power input is off (or too low or too high)
Gray	Off	Mains Failure test is running

DC-DC converter

The LED in the DC-DC converter box indicates the state of the battery input.

LED	Text	Description
Green	On	Battery input is usable. The PMU can provide up to 500W (or up to 40W of power in low power mode).
Red	Off	Battery voltage is off (or too low or too high).
Gray	Off (disabled)	A DC-DC converter is not fitted.

Standby converter

The LED in the Standby converter box indicates the state of the DC supply to the standby converter.

LED	Text	Description
Green	On	The standby DC supply is on.
Red	Off	Battery voltage is off (or too low or too high.
Gray	Off (disabled)	No standby battery power supply is fitted. (AC-only PMUs do not have standby converters.)

PA

The PA LED displays green if the PMU is supplying power to the PA.

Channel module/ control panel

The Channel module/control panel LED indicates the status of the power supply to the receiver and the control panel. Green means that it is supplying power. Gray means that it is not, because the PMU is in battery protect mode.

Auxiliary output

The Auxiliary output box has an LED that indicates the status of the auxiliary power output.

LED	Text	Description
Green	On	The auxiliary output power supply has been turned on.
Red	Off	There is a fault. This could be because there has been a current overdraw and the fuse is blown. On cooling, the fuse will automatically reset.
Gray	Off	The PMU has turned the output off.
Gray	Off (disabled)	An auxiliary power output submodule is not fitted.

Output current gauge

The Output current gauge shows how much current the PMU is supplying to the subrack.

Output voltage gauge

The Output voltage gauge shows the voltage of the power that the PMU is supplying to the subrack.

Converter temperature

Two thermometers show the respective temperatures of the AC-DC converter and the DC-DC converter. The PMU fan should operate to keep this temperature within limits. The following actions occur as the temperature increases.

Temperature (°C)	Temperature (°F)	Action
65	149	PMU fan turns on
75	167	PMU fan stays on always
87	188	High temperature alarm raised

As the temperature decreases, the following actions occur.

Temperature (°C)	Temperature (°F)	Action
80	176	High temperature alarm clears
60	140	PMU fan turns off

Fan

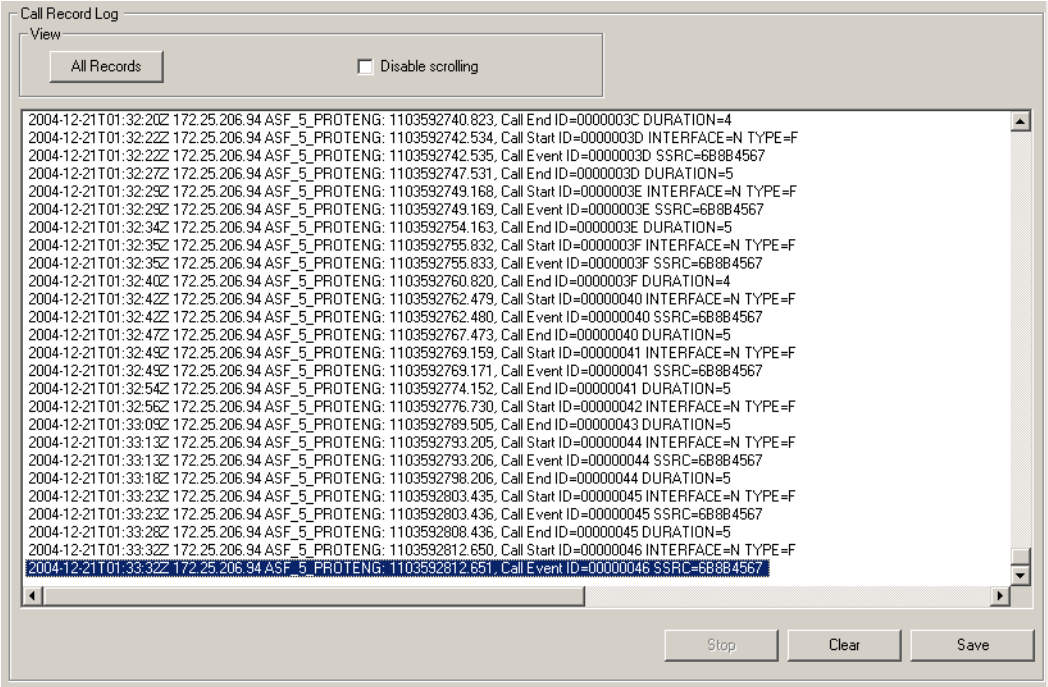
The Fan box indicates whether the PMU fan is off or on.

Data Logs

The CSS can ask the connected network element to provide records of various types of logged events. You can view them and save them to a file. In addition, the CSS has its own log.

Viewing Call Records

The CSS can display records of digital P25 calls that the connected network element has participated in.



Viewing call records can cause voice drop-outs. When you click **All Records**, the network element sends all the entries in its log to the CSS. This may flood switched networks, which cannot prioritize voice packets. The result is that voice traffic does not arrive in time. To avoid this problem, configure the network element to send call records to a syslog collector. For details, see "Logging to a Syslog Collector" on page 213.

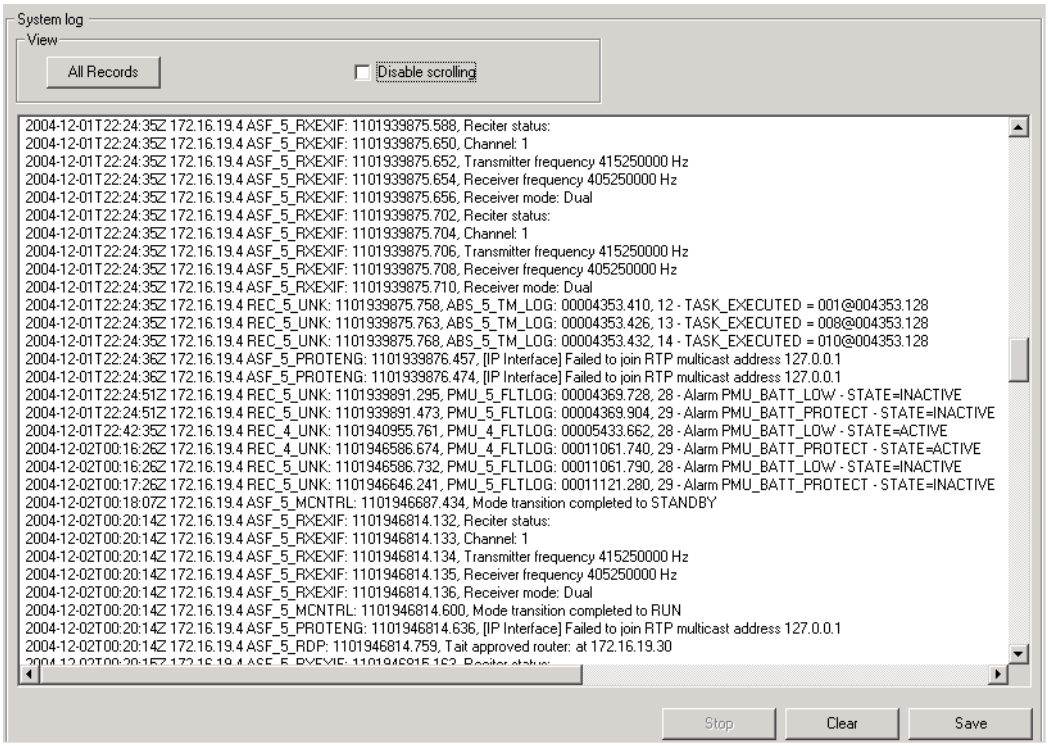
To view the call record log

1. Select Monitor > Data Logging > Call Record Log. The appropriate form appears, but displays no data.
2. Click **All Records**. The CSS asks the connected network element to supply all call records it has stored.
3. To stop the records from scrolling on the screen as the CSS receives them, select the **Disable scrolling** check box.
4. To update the display with new call records, click **All Records** again. The network element only sends call records that have not already been supplied. To view only new call records, click **Clear** before clicking **All Records**.

Using the buttons on the bottom of the form, you can tell the network element to stop supplying records, clear the display, or save the records to a file.

Viewing the System Log

The CSS can ask the connected network element to provide records of events that lie above the level of Notice. The network element can store up to 1000 such events.



Viewing the system log can cause voice drop-outs. When you click **All Records**, the network element sends all the entries in its log to the CSS. This may flood switched networks, which cannot prioritize voice packets. The result is that voice traffic does not arrive in time. To avoid this problem, configure the network element to send the data to a syslog collector. For details, see "Logging to a Syslog Collector" on page 213.

To view the system log

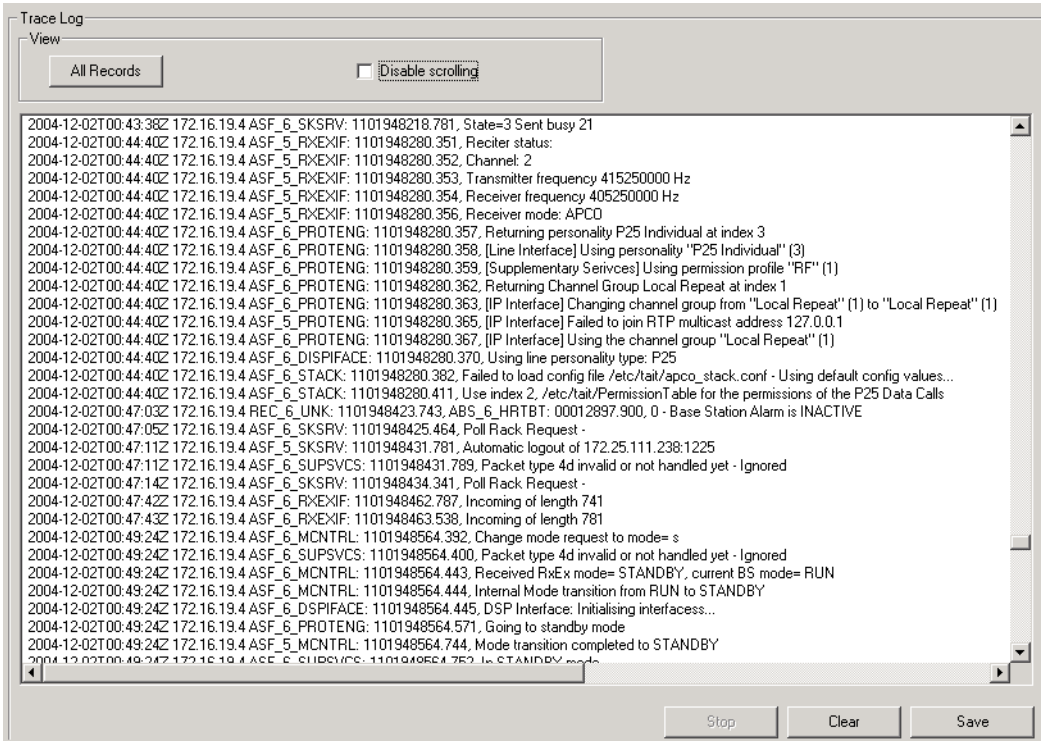
1. Select Monitor > Data Logging > System Log. The appropriate form appears, but displays no data.
2. Click **All Records**. The CSS asks the connected network element to supply records, beginning with the oldest.
3. To stop the records from scrolling on the screen as the CSS receives them, select the **Disable scrolling** check box.
4. To update the display with new records, click **All Records** again. The network element only sends records that have not already been supplied.

   Using the buttons on the bottom of the form, you can tell the network element to stop supplying records, clear the display, or save the records to a file.

Viewing the Trace Log

The trace log provides information about the operation of the network element. Normally, you would look in the system log for such information. However, Tait may request that you look in the trace log for particular items or save the trace log to a file and send it to them.

The trace log contains system log messages, call records, and additional messages with a severity level of Information. Information messages are Tait-internal and very detailed. The network element's trace log can store up to 1000 messages.



Viewing the trace log can cause voice drop-outs. When you click **All Records**, the network element sends all the entries in its log to the CSS. This may flood switched networks, which cannot prioritize voice packets. The result is that voice traffic does not arrive in time. To avoid this problem, configure the network element to send the data to a syslog collector. For details, see "Logging to a Syslog Collector" on page 213.

To view the trace log

1. Select Monitor > Data Logging > Trace Log. The appropriate form appears, but displays no data.
2. Click **All Records**. The CSS asks the connected network element to supply records, beginning with the oldest.
3. To stop the records from scrolling on the screen as the CSS receives them, select the **Disable scrolling** check box.
4. To update the display with new records, click **All Records** again. The network element only sends records that have not already been supplied.

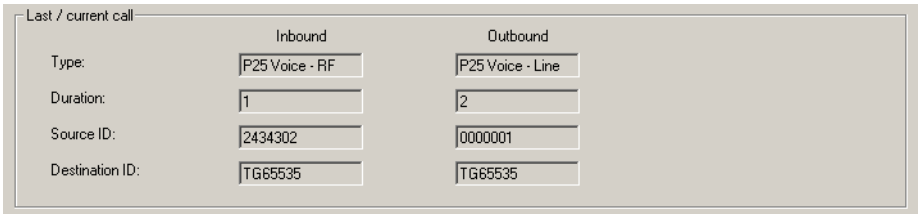
   Using the buttons on the bottom of the form, you can tell the network element to stop supplying records, clear the display, or save the records to a file.

Viewing Call Statistics

The Call Statistics form (Monitor > Data Logging > Call Statistics) displays information about the current or most recent call(s) and statistics about recent calls.

Last / current Call

The Last / current call area can simultaneously show details about an inbound and an outbound call. These may be the same call.



Type

The Type boxes provide information about the type and origin of the call.

Call Type	Description
FM	Call is analog FM
P25 Voice	Call is digital P25
P25 Sig.	'Call' is digital P25 signaling (one or more TSBKs)

Call Origin	Description
RF	Call originated from the local RF interface
Line	Call originated from the local analog line or DFSI interface
IP	Call originated from another channel group member and was received on the channel group interface
Panel	Call originated from the control panel microphone

Duration

How long (in seconds) the call has been in progress.

Source ID

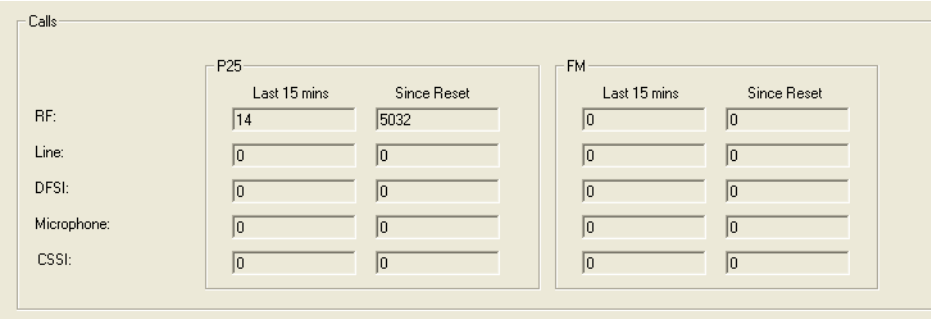
The P25 ID of the sender (P25 calls only).

Destination ID

The ID of the intended receiver of the call (P25 calls only).

Calls

The Calls area displays statistics on the number of voice calls separately for analog FM and for digital P25 calls.



Some activities, which might appear to be a single call, actually result in the counters increasing by more than one. For example, a status query received on the DFSI increases the counter by two. There is a "call" to the SU requesting its status and a "call" consisting of the SU's response.

Last 15 minutes	The Last 15 minutes columns display call totals for the last completed 15-minute period. When the next 15 minute period completes, the displays reset to zero.
Since reset	A column of totals that have accumulated since the network element was last reset.
RF	Calls that were initiated from the RF interface.
Line	Calls that were initiated from the analog line.
DFSI	Calls that were initiated from dispatch equipment over the DFSI interface.
Microphone	Calls that were initiated from the control panel microphone.
CSSI	Calls to the dispatcher that were received over the trunked analog gateway's CSSI interface.

Viewing the CSS Application Log

The CSS maintains a log of events in a file. This log may provide useful information if there are problems with the CSS or in the communications between the CSS and a network element.

To view the Application log

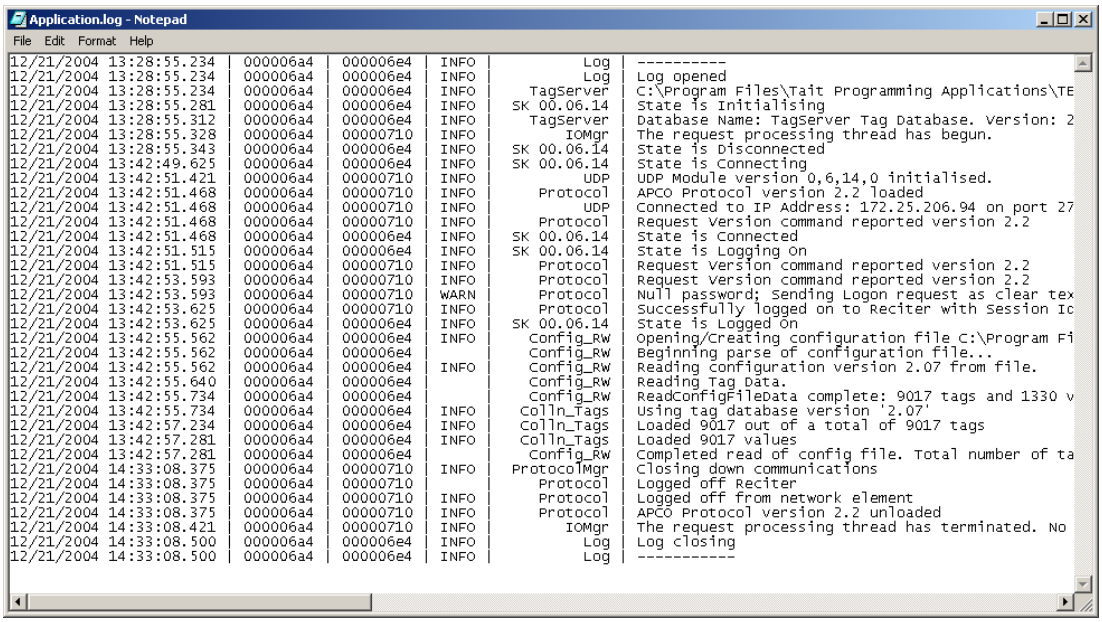
1. Navigate to the Log Files folder.

   For the Microsoft Windows 7 or Windows Vista operating system, the path is:
   C:\Users\Public\Public Documents\Tait Applications\TB9100 CSS *n.nn.nn*\Log Files.

   For the Windows XP and Windows 2000 operating systems, the path is: C:\Documents and Settings\All Users\Documents\Tait Applications\TB9100 CSS *n.nn.nn*\Log Files.

2. Open Application.log in any text editor.

   A display similar to the following appears.

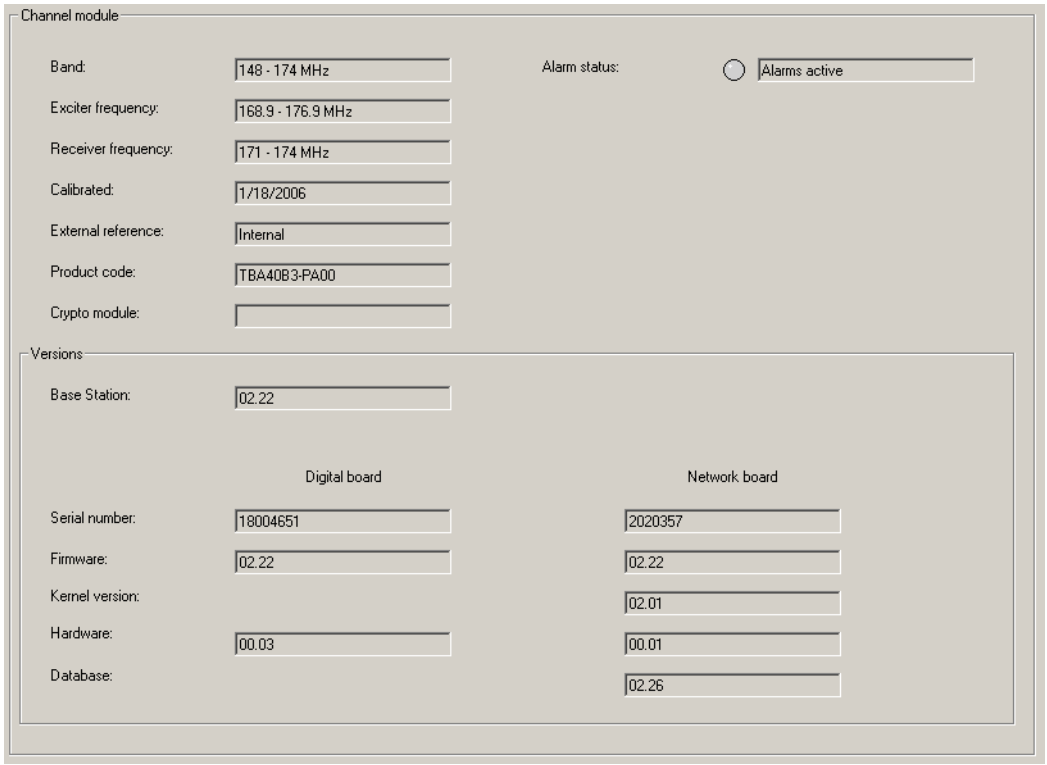


Module Details

The CSS can display details about the channel module, PA, and PMU of the network element it is connected to. Items under the heading Module Details display information about the module such as its frequency range and firmware version. To monitor the way the modules are operating, see "Modules" on page 104.

Viewing Reciter or Gateway Module Information

The Channel Module form (Monitor > Module Details > Channel Module) displays information about the channel module of the network element you are connected to. Use it to confirm exactly what it is that you are dealing with.



Band

The RF frequency band of the reciter. This is the frequency range that the reciter is type-approved to operate in.

Alarm status

Indicates whether the channel module currently has any alarm conditions. If the LED is green, there are no active channel module alarms. If the LED is red, the text box displays 'Alarms active,' and there is at least one active alarm. To see which alarm is active, select Monitor > Alarms > Status.

Exciter frequency

The current switching range of the exciter, as recorded by the network element when it was last tuned using the Calibration Software. You can confirm the actual switching range using a diagnostic test (Diagnose > RF Interface > Synthesizers). K4 band exciters have two sub-bands but the CSS can only display the switching range of one sub-band. However, the exciter can always operate in either sub-band. To have the CSS display the other sub-band, select it using the calibration software.

Receiver frequency

The current switching range of the receiver, as recorded by the network element when it was last tuned using the Calibration Software. You can confirm the actual switching range using a diagnostic test (Diagnose > RF Interface > Synthesizers).

Calibrated

The date when the reciter was last modified using the Calibration Software. (This includes adjusting the switching range and tuning the frequency response.)

External reference

Indicates whether the reference frequency is currently being provided by an external or an internal source.

Product code

The product code and name for the type of channel module.

Crypto module

The status of the firmware crypto module in the channel module. Gateway modules usually need a crypto module so that they can be an encryption and decryption point for dispatcher communications. TB9100 base stations cannot normally have a crypto module; they are crypto-denied.

.

Display	Description
Not fitted	A firmware crypto module is not present and cannot be loaded, as the reciter is crypto-denied.
(blank)	A firmware crypto module is not present, but can be loaded by a CSS firmware download. The channel module is crypto-capable.
1.01	The version number of the firmware crypto module.

Versions

The Versions area (Monitor > Module Details > Channel Module) displays version information for the channel module's digital and network boards.

Network element

Displays the full version number of the channel module. This is mainly for Tait internal use.

Serial number

A unique identifier assigned to the board in the factory.

Firmware

The version number of the firmware currently installed on each board.

Kernel

The version number of the network board's operating system kernel.

Hardware

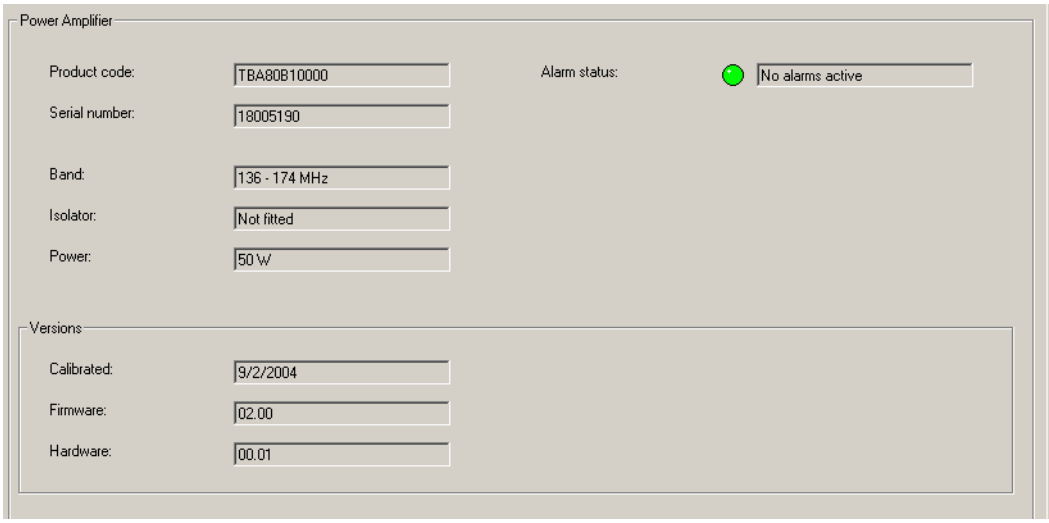
The version number of the hardware for each board. This version number is used to establish compatibility with firmware versions.

Database

The version number of the network element's database. The CSS communicates primarily with the channel module's network board. The CSS and the network board must use the same database version.

Viewing Power Amplifier Information

The Power Amplifier form (Monitor > Module Details > Power Amplifier) displays information about the PA module of the base station you are connected to. Use it if you need to confirm exactly what it is that you are dealing with.



Product code	The product code and name for the type of PA.
Serial number	A unique identifier assigned to the PA in the factory.
Band	The RF frequency range that the PA is type-approved to operate in.
Isolator	Indicates whether the PA is fitted with an optional internal isolator (not currently available.)
Power	Specifies the RF power output rating of the PA. There are 5 W, 50 W, and 100 W variants.
Alarm status	Indicates whether the PA currently has any alarm conditions. If the LED is green, there are no active alarms. If the LED is red, the text box displays 'Alarms active,' and there is at least one active alarm. To see which alarm is active, select Monitor > Alarms > Status.

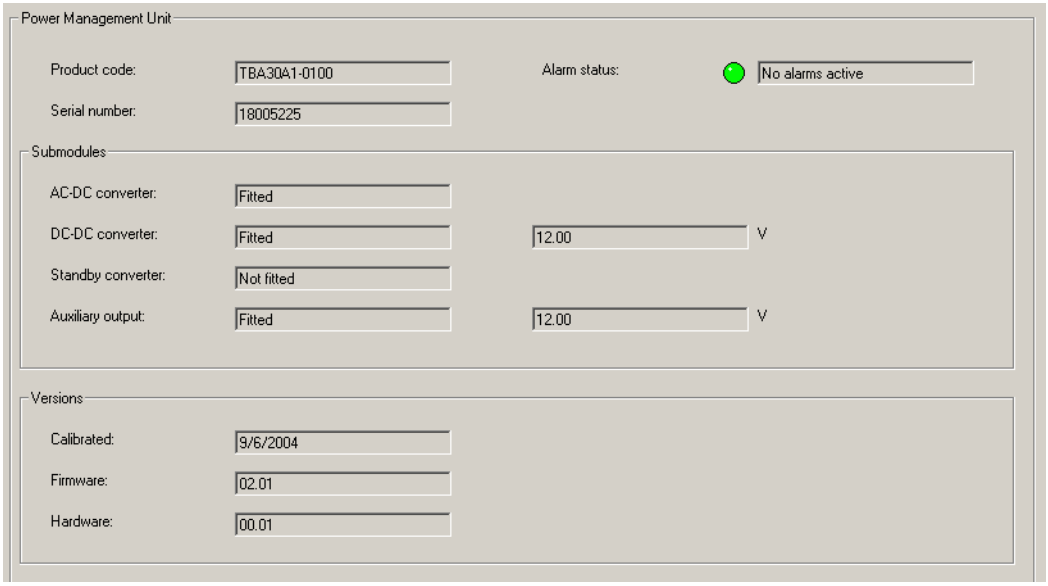
Versions

The Versions area (Monitor > Module Details > Power Amplifier) displays version numbers for aspects of the PA.

Calibrated	The date when the PA was last calibrated using the Calibration Software.
Firmware	The version number of the PA firmware.
Hardware	The version number of the PA hardware.

Viewing Power Management Unit Information

The Power Management Unit form (Monitor > Module Details > Power Management Unit) displays view information about the PMU if you are connected to the channel module in position 1 of the subrack. Use it if you need to confirm exactly what it is that you are dealing with.



Product code — The product code and name of the PMU module.

Serial number — A unique identifier assigned to the PMU in the factory.

Alarm status — Indicates whether the PMU currently has any alarm conditions. If the LED is green, there are no active alarms. If the LED is red, the text box displays 'Alarms active,' and there is at least one active alarm. To see which alarm is active, select Monitor > Alarms > Status.

Submodules

The Submodules area (Monitor > Module Details > Power Management Unit) indicates which submodules the PMU is fitted with.

AC-DC converter — Indicates whether the PMU is fitted with an AC-DC converter submodule, so that it can use mains input.

DC-DC converter — Indicates whether the PMU is fitted with a DC-DC converter submodule, so that it can use DC power as an input. The box alongside indicates whether the submodule is designed for a 12, 24, or 48 V input.

Standby converter — Indicates whether the PMU is fitted with a standby converter submodule.

Auxiliary output — Indicates whether the PMU is fitted with a submodule that provides an auxiliary power output. The box alongside indicates whether the submodule is designed for a 12, 24, or 48 V output.

Versions

The Versions area (Monitor > Module Details > Power Management Unit) displays version numbers for aspects of the PMU.

Calibrated	Indicates when the PMU was last calibrated using the Calibration Software.
Firmware	The version number of the PMU firmware.
Hardware	The version number of the PMU hardware.

Part E Configuring

You can use the CSS to configure TB9100 base stations and gateways. Click **Configure**, choose a configuration, and select an item from the navigation pane.

- Choosing a Configuration

Network Element

- Working with the Channel Table
- Working with Service Profiles
- Configuring the System Interface
- Configuring Miscellaneous Items

RF Interface

- Working with Channel Profiles
- Working with Signaling Profiles
- Configuring the CWID
- Enabling RF Linking

Channel Group

- Network Identity
- Working with Channel Groups
- Quality of Service

Network Interfaces

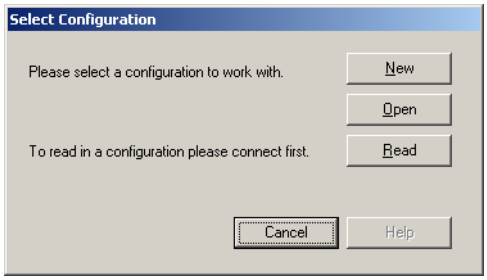
- Trunking
- Failsoft
- DFSI Interface
- CSSI Interface
- Conventional Packet Data

Analog Line

- General Analog Line Settings
- Working with Calling Profiles
- Encryption
- Defining Group Memberships
- Mapping Tone Remote Commands
- Setting Tone Remote Options
- Mapping MDC1200 Addresses
- Declaring RFSS Controllers
- ISSI Profiles

Choosing a Configuration

If you click **Configure** and the CSS doesn't already have a configuration in memory, it asks you to choose one to work with.



- Click **New** to open a new configuration based on the default template.
- Click **Open** to select an existing configuration file.
- Click **Read** to read in the configuration of the network element you are connected to.

Network Element

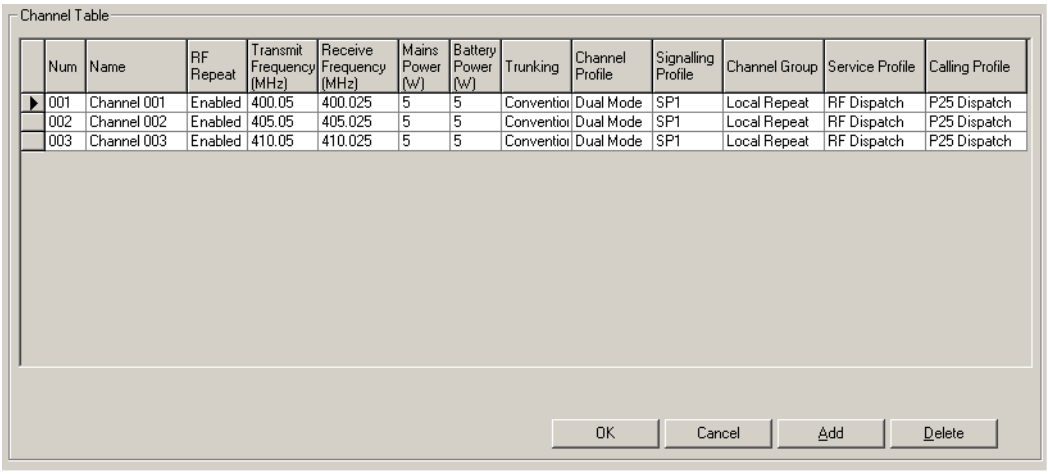
Under Network Element, the navigation pane groups items that apply to the network element as a whole and are not specific to a particular interface.

Working with the Channel Table

In the Channel Table form (Configure > Network Element > Channel Table), you can view the configured channels, edit them, and add more channels.

Channel Table Details

The Channel Table form (Configure > Network Element > Channel Table) displays the channels defined in the channel table of the configuration file that you opened or the network element database that you read.



The form contains a table that displays a row for each channel. The row indicates the channel's number and name, the configured transmitter power output for mains and battery power, and the profiles that have been assigned to the channel.

The arrow at the left of one row indicates that that row is selected; if you click **Add**, a copy of that row will be added. Use the mouse or the arrow keys to change the selection. When you make any changes to a row, the arrow changes to a pencil.

The arrow does **not** define the current channel. To find out the channel that the network element is currently operating on, select Monitor > Interfaces > RF Interface.

The first two columns indicate the number and name of each channel. The other columns define the main characteristics of each channel. Frequencies and transmit output power you can edit directly. Profiles and the channel group are selected from a list. Click a cell and a drop-down list appears, showing the items that have been defined.

Num

The number of the channel. It is not editable, so that you do not break existing Task Manager statements. To replace a deleted channel, select the previous channel and click **Add**. This adds an entry to the channel with the number of the deleted channel.

Name

The name of the channel. When you create a channel, it is given a default name of the form 'Channel nnn' where nnn is the channel number. You can edit this name to reflect the channel's purpose or users.

RF repeat

The RF repeat column specifies whether the base station operates as a repeater. For an introduction to the Repeat function, see "RF Repeat Function" on page 10.

Option	Description
Enabled	The base station operates as a repeater. It is able to transmit the signal received from its RF interface or the RF interface of other channel group members. It repeats the best RF signal received by the channel group, not necessarily the signal it receives on its own RF interface.
Disabled	The base station does not repeat received RF signals. It can only transmit what is provided by this base station's or another channel group member's dispatcher interface or control panel microphone.
DispatchControlled	The repeat function is under dispatcher control. The DFSI gateway can automatically pass dispatcher commands on to the channel group to enable or disable repeat. If the dispatch equipment is connected via the analog line, Task Manager actions are needed to implement the commands and propagate them to the channel group. For more details, see "RF repeat actions" on page 267 and the TaitNet P25 Conventional System Manual.

Transmit Frequency

The radio frequency that the channel transmits on.

Receive Frequency

The radio frequency that the channel receives on.

Mains Power

The RF power output in watts. This is the power that the channel is configured to provide when the base station is using mains power.

If you specify an RF power of 100 W and the PA is rated at 50 W, it will run at 50 W. There is therefore no need to alter this value if you temporarily substitute an amplifier with lower power, for example, if there is a fault and you don't have a fully powered module on hand.

Battery Power

The RF power output in watts. This is the power that the channel is configured to provide when the base station is using battery power.

This setting is not used by reciter 2 in a subrack, because the PMU cannot inform it when it is running on battery power.

Trunking	Select Conventional for non-trunked operation or Trunked if the channel is to be part of a trunked system. This setting specifies how the channel operates. The network element needs to behave differently, depending on whether its channel group is controlled by a trunking site controller or a dispatcher.
Channel Profile	The channel profile assigned to the channel. See "Profiles" on page 7 for an overview of the different profiles and their functions.
Signaling Profile	The signaling profile assigned to the channel.
Channel Group	The channel group that the network element is part of.
Service Profile	The set of services that the inbound channel will support.
Calling Profile	The calling profile used by the analog line.
Add	Inserts a copy of the selected channel immediately below that channel. For more information, see "Adding a Channel" on page 125.
Delete	Removes the selected row from the channel table. (To restore a row with the deleted channel number, select the row above and click **Add**).

Be careful not to delete channel 1 from the channel table. Once it has been deleted, you cannot re-create it, except by first deleting all channels in the channel table. (All other channels in the table can be re-created using the Add button.)

Editing a Channel

Editing a channel is mostly about assigning the correct profiles to it.

To edit a channel

1. In the channel table (Configure > Network Element > Channel Table), click in the row that defines the channel. An arrow appears at the left of the row indicating that it is selected.
2. If desired, click in the **Name** cell and edit the channel's name.
3. If necessary, alter the receive frequency and the transmit frequency.

Do not assign a prohibited frequency to the transmitter. For example, 406.0-406.100 MHz is reserved internationally for distress beacons.

The CSS does not check whether the base station can operate on the configured frequency pair.

For simplex applications, you can make the receive and transmit frequencies the same. The base station automatically increases the transmit frequency by 25 kHz when it is not transmitting, to avoid desensitizing the receiver.

4. In the **Mains Power** and **Battery Power** columns, specify values for the transmitter's RF output power when powered by mains and DC respectively.

5. In the **Trunking** column, specify whether the channel is part of a conventional or a trunked system.
6. In the **Channel Profile** column, select the channel profile you want the network element to belong to. (Click in the cell, then click the arrow that appears. A list of the defined channel profiles appears.) The channel profile determines a whole range of settings, including switching behavior and (for analog mode), receiver gating and channel spacing.
7. In the **Signaling Profile** column select the channel profile you want the base station to belong to. This defines the use of NAC (for digital P25 mode), subaudible signaling (for analog FM mode), and tail timers.
8. In the **Channel Group** column, select the channel group that you want the network element to belong to. This determines the multicast address on the TaitNet P25 digital network that it sends voice to and listens to.
9. In the **Service Profile** column, select a the service profile that defines the set of services that you want the channel to support.
10. In the **Calling Profile** column, select a calling profile that you want to apply to the analog line (dispatcher commands that use MDC1200 can change this selection or override some of its settings.)
11. Click **OK** to confirm the changes and close the form.

If you are editing a large number of channels, periodically click OK, and then (on the toolbar) Save. Otherwise you could lose a lot of data if there is a computer failure.

Adding a Channel

You can add a channel to the channel table.

1. Select Configure > Channels and Profiles > Channel Table.
2. Click on a channel similar to the one you want to add. A black triangle appears to the left of the row.
3. Click **Add**. This inserts a copy of the selected channel immediately below that channel. The inserted channel is given the next available number and an equivalent name, for example, if the next available channel number is 008, the name is Channel 008.
4. If desired, click the **Num** column heading to sort the new channel into numerical order.
5. Edit the values in the channel row as needed (see "Editing a Channel" on page 124).

Selecting the Operating Channel

Different methods can be used to select the channel that a network element operates on. For each method, you need to configure the network element.

Selection at Run mode

The configuration contains a Task Manager task that instructs the network element to go to a channel on the transition to Run mode, for example:

IF **Network Element in Run mode** THEN **Go to Channel Channel 001**

Normally, the network element is shipped with this channel selection method. (This Task Manager task can be deleted. Once the network element has operated on a channel, it remembers that channel even through a reset.)

Selection by digital inputs

The operating channel can be selected by an external device that is able to toggle the state of the network element's digital inputs. You must specify how many digital inputs are involved and create Task Manager tasks that instruct the network element to go to a channel when the combination of digital input states produces the required digital input value.

1. In the System Interface form (Configure > Network Element > System Interface), specify the number of bits to use in computing an input value.

2. Create Task Manager tasks that select the channel based on the digital input value, for example:

IF **Digital input value 1** THEN **Go to Channel Channel 001**

IF **Digital input value 2** THEN **Go to Channel Channel 002**

IF **Digital input value 3** THEN **Go to Channel Channel 003**

Selection by dispatcher command (Analog dispatch equipment)

Dispatcher commands can select the current channel. The dispatch equipment sends a function tone. You need to set up Task Manager statements such as the following:

IF **Tone remote detected** 550 THEN **Go to channel** 2

When the analog line receives a 550 Hz function tone, the network element switches to that channel. If the network element is part of a channel group, configure all channel group members for collective control of the channel number.

We recommend that you delete the Task Manager task that selects a channel on transition to Run mode. Then a network element will return to its previous channel after a reset. This is the channel that the dispatcher expects to be on.

Selection by dispatcher command (digital dispatch equipment)

Dispatcher commands can select the current channel. The dispatch equipment sends a channel select command over the DFSI interface. If the network element is part of a channel group, configure all channel group members for collective control of the channel number.

We recommend that you delete the Task Manager task that selects a channel on transition to Run mode. Then a network element will return to its previous channel after a reset. This is the channel that the dispatcher expects to be on.

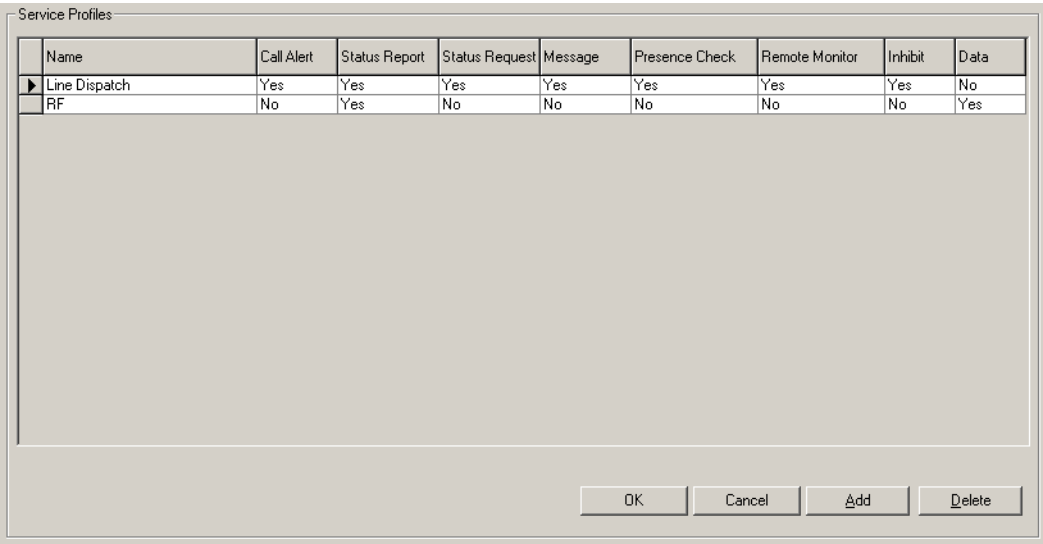
Other Methods

Any Task Manager input can be used to select a channel. A SU user could for example make a call using a special NAC to change channel.

Working with Service Profiles

The Service Profiles form (Configure > Network Element > Service Profiles) displays a list of available service profiles. A service profile indicates which additional services are permitted. Emergency alert is always permitted, so does not appear. All acknowledgements are also always permitted. Service profiles apply when the network element is operating in digital P25 mode. They do not affect MDC1200 signaling in analog FM mode. Tait recommends that all services are normally enabled. Consoles and SUs can allow or disallow services to the end user. However, services can be disabled at the base station to prevent pirate SUs from using them on the TaitNet P25 digital network.

A service profile can be selected by a channel in the channel table and/or by a calling profile. When a service profile is selected by a channel, it controls the behavior of the inbound RF channel. If a service is enabled, the inbound channel supports that service. When a service profile is selected by a calling profile, it controls the behavior of the analog line in. If a service is enabled, the analog line lets the analog console system use that service. The console system sends a MDC1200 signal, which is converted into the digital P25 equivalent.



The profiles display Yes or No for each service. Yes means that the service is enabled, No that it is disabled. The following describes briefly what each service is.

Name — The name of the service profile.

Call Alert — Call alert (also known as paging) is a message that asks the SU user to call the sender. It may for example trigger a persisting message on the target SU such as a repeating tone and flashing display.

Status Report — A status report is a message that the SU sends, perhaps in response to a status request.

Status Request — A status request is a message that requests a status report.

Message — A message is a free-form text string.

Presence Check — A presence check is a message that checks out a given SU. If the SU responds, it is within communications range and its RF circuitry is functioning. The operator is not disturbed.

Remote Monitor — A remote monitor message causes the SU to initiate a call by itself. It allows the sender to listen to what is going on at the SU location.

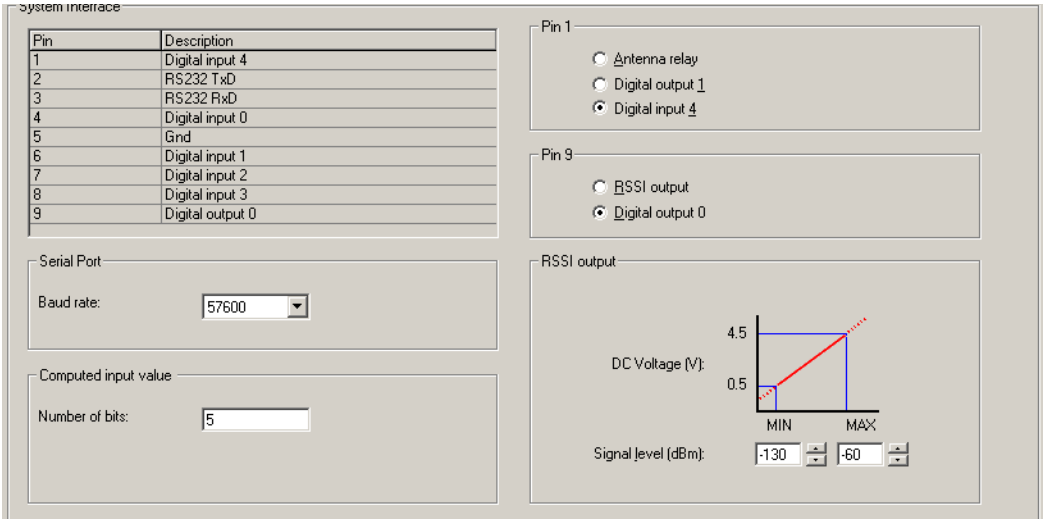
Inhibit — An inhibit message disables the destination SU, for example if it is reported stolen. When the Inhibit service is enabled, the Uninhibit service is also enabled.

Data — The data service (not currently supported) involves the sending and receiving of data rather than voice.

Configuring the System Interface

In the System Interface form (Configure > Network Element > System Interface), you can configure the operation of digital inputs and outputs and the serial port. These all connect to the DB9 labeled DIG on the rear of the channel module.

To monitor the current status of the digital inputs and outputs, or to carry out diagnostic tests on them, select Diagnose > Line Interfaces > System Interface.



Pin assignments

The unnamed table displays the functions assigned to each pin on the DIG DB9 connector at the rear of the channel module. The display reflects the choices made for Pins 1 and 9.

Serial port

Baud rate

The default baud rate setting is 57,600 bit/s and is not normally changed. For Calibration Software operation it must be at this speed. The setting is ignored when the serial port provides raw C4FM data and a baud rate of 19,200 is used instead.

Computed input value

Number of bits

Tells the network element how many bits (digital inputs) to use in calculating the digital input value. Digital input 0 provides the least significant bit. Four digital inputs are always available. To make a fifth digital input available, configure Pin 1 as Digital input 4. Inputs are assigned the value 0 when they are low and 1 when they are high. To monitor the current computed input value, select Diagnose > Line Interfaces > System Interface.

The digital input value can be used as an input in Task Manager statements (see "Digital input value" on page 257). Task Manager can for example select the channel number to use based on the computed input value.

Pin 1

The three option buttons let you specify one of three functions for Pin 1.

Function	Description
Antenna relay	Select this option in simplex applications to provide a signal that drives an antenna relay. For details, see "Antenna Relay Operation" on page 130.
Digital output 1	Configures pin 1 as a digital output. Select this option if you need a digital output.
Digital input 4	Configures pin 1 as a digital input. Select this option to make a fifth bit available for the computed input value or to make a fifth digital input available.

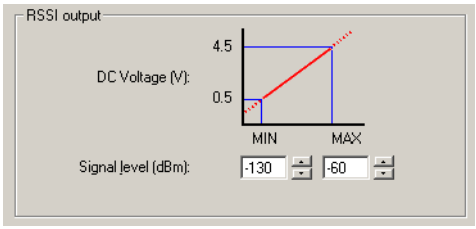
Pin 9

The two option buttons let you specify one of two functions for Pin 9.

Function	Description
RSSI output	Configures pin 9 to output a voltage proportional to the received signal strength. For more details, see "RSSI Output" on page 129.
Digital output 0	Configures pin 9 as a digital output. You can also configure pin 1 as a digital output.

RSSI Output

The TB9100 can provide an RSSI output on pin 9 of the DB9 labeled DIG. This is used for external voting or in systems with two base stations for redundancy.



To enable and configure the RSSI output

1. Select Configure > Network Element > System Interface.
2. Under **Pin 9**, click **RSSI output**.
3. Under **RSSI output**, enter into the **Signal level** boxes the minimum and the maximum signal strengths that the base station needs to deal with. The RSSI output will be 0.5V at the minimum signal strength, increasing linearly up to 4.5V at the maximum signal strength.

Antenna Relay Operation

For simplex applications, the base station can be set up with an antenna relay, so that the receiver and transmitter can share the same antenna. For details, see the installation instructions that come with the Tait TBAA03-15 Relay Coaxial Assembly kit.

To enable the operation of an antenna relay

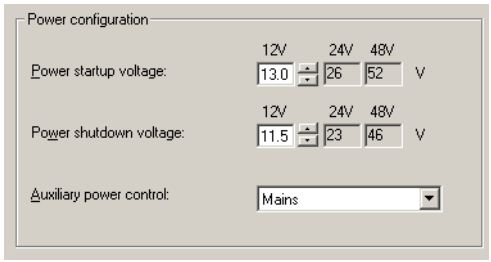
1. Select Configure > Network Element > System Interface.
2. Under **Pin 1**, click **Antenna relay**.
3. In the channel table, make sure that RF repeat is disabled in all channels. Using an antenna relay when RF repeat is enabled will result in relay chatter. When the base station receives a signal, it switches to transmit so that it can repeat it. The result is that it can no longer see the signal. As there is nothing to transmit, it switches back to receive, which causes it to switch to transmit again, and so on.
4. Program these settings into the base station.

Configuring Miscellaneous Items

The Miscellaneous form (Configure > Network Element > Miscellaneous) gathers together a number of settings.

Minimum battery voltages

Use the Power configuration area (Configure > Network Element > Miscellaneous) to adjust the minimum voltages for the DC power input to the PMU. These values are stored in the PMU. You cannot adjust them below limits fixed in hardware.



Three pairs of voltages are displayed, corresponding to the different DC-DC converter options (a nominal 12V, 24V, or 48V input). If, for example, your PMU has a 24V DC-DC converter, the voltages under 24V apply. To alter the startup or shutdown voltage, edit the voltage with the white background or click an adjacent arrow button. The voltage under 24V and 48V changes accordingly.

If the battery voltage falls below the value in the relevant **Power shutdown voltage** box and there is no AC power, the PMU shuts down. (If there is AC power, a battery protection mode alarm is raised, indicating that the loss of AC power will result in shutdown.)

If the battery voltage rises above the value in the **Power startup voltage** box, the PMU re-starts. (For full details, see the TB9100/P25 CG Installation and Operation Manual.)

Network elements with no PMU or with a PMU that has no standby converter cannot have their shutdown and startup voltages adjusted; these voltages are fixed in hardware.

Auxiliary power control

If the PMU is fitted with an auxiliary power supply unit, you need to configure it to suit the way it will be used. Generally, its output can be used to trickle charge batteries (to maintain the charge in batteries that are used as an emergency backup power supply) or to power other site equipment. If it is used to trickle charge batteries, configure it to be on when mains power is on. If it is used to power other site equipment, configure it to be under Task Manager control. If necessary, Task Manager can turn it off and back on again.

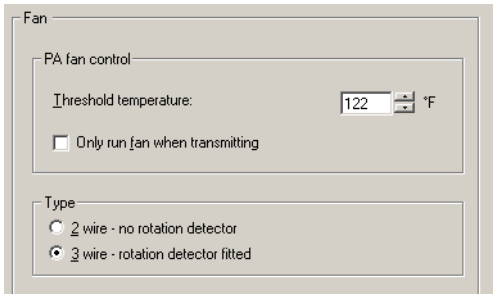
While the auxiliary power output can be used for more than one purpose at once, this is not generally recommended. It can result in a short-circuit and equipment damage. The output is floating. If it is connected to a negatively earthed battery and to positively earthed auxiliary equipment, a short-circuit will result.

In the Power configuration area (Configure > Network Element > Miscellaneous), the Auxiliary power control box specifies what controls the auxiliary output. The setting is stored in the PMU. Select one of the following options.

Option	Description
Task Manager	The auxiliary power supply will be on unless the Task Manager action **Lock auxiliary supply** turns it off. You can define Task Manager tasks that turn the auxiliary power off and back on as needed. See "Auxiliary supply lock" on page 266.
Mains	The auxiliary power supply will be on only when the PMU uses AC mains power. This option is suitable for trickle charging batteries. The Task Manager actions **Lock auxiliary supply** and **Unlock auxiliary supply** have no effect. (This option is not designed for use with a DC-only PMU. However, if the PMU is DC-only and you select this option, the auxiliary power output will always be on, contrary to what one would expect.)

Configuring Fan Settings

The Fan area (Configure > Network Element > Miscellaneous) gathers together fan-related settings. These specify how the network element monitors its PA and PMU fan and when the PA fan is turned on. The operation of the reciter fan is not configurable.



PA Fan Control

The PA Fan Control area determines when the PA fan is turned on. The settings are stored in the PA and can be adjusted to meet user requirements based on the transmit duty cycle and whether the site facility is air-conditioned. Strike a balance between lengthening fan life and reducing the PA operating temperature.The settings you choose should also help avoid extreme temperature swings. The PA is designed to run at full duty cycle at up to +60 °C ambient operating temperature into any transmit VSWR load.

While the PA fan on/off thresholds are user-configurable, the PMU fan has fixed on/off thresholds controlled by PMU firmware.

Threshold temperature

If the temperature at the driver, final 1, or final 2 stages exceeds the threshold temperature, the fan is turned on (but only when the PA is transmitting, if the check box below is selected). When the temperature at all three parts of the PA falls 5 °C below the threshold, the fan is turned off.

Tip: To monitor all PA temperature values, select Diagnose > Power Amplifier > Control Tests.

Only run fan when transmitting

When this check box is selected, the fan will only operate if the PA is transmitting and any one of the monitored PA temperatures exceeds the threshold.

Fans used in the TB9100 must have the correct wiring. Power and ground (2-wire fans) or power, ground and rotation detect (3-wire fans). Both fans in the front panel should be of the same type.

Type

Specify whether the PA and PMU fan type is 2-wire or 3-wire. If you select 3-wire, the network element will use the third wire as a rotation detector. If it has turned the fan on but does not detect rotation, it activates the 'Fan failed' alarm.

Configuring the Fan to Turn on with the PA

You can configure the PA fan to turn on when the PA begins transmitting. Follow these steps:

1. Select Configure > Network Element > Miscellaneous.
2. Set the threshold temperature to a value that is lower than the usual site ambient temperature.
3. Select the **Only run fan when transmitting** check box.

With these settings, the PA fan normally turns on with RF output and cools the PA as soon as it begins working. It turns off when the RF output stops. However, if the PA temperature is below the threshold, the fan does not turn on.

External clock reference frequency (if fitted)

Use the External clock reference frequency (if fitted) area (Configure > Network Element > Miscellaneous) to specify the frequency of an external reference frequency source. If an external source is connected to the reciter, you must select the appropriate option so that the reciter knows what the frequency is. Reset the base station so that the new setting takes effect.

Control panel

The Enable check box in the Control panel area enables the speaker and microphone. Disabling them may be desirable for security reasons. Before using them, a maintainer on site must first modify the configuration.

Revert to Run mode

You can configure the network element to automatically revert to Run mode when the CSS disconnects. This prevents loss of service when a network element is inadvertently left in Standby mode or when a communications failure disconnects the CSS. Reverting to Run mode occurs only on disconnection, not when a maintainer stops using the CSS.

In the Miscellaneous form (Configure > Network Element > Miscellaneous), select one of the following options for the Revert to Run mode box.

Option	Description
Never	The network element does not revert to Run mode. The CSS user must manually put it back into Run mode before disconnecting. You are warned if you try to disconnect when the network element is still in Standby mode.
2 minutes	The network element automatically reverts to Run mode two minutes after the CSS disconnects.
10 minutes	The network element automatically reverts to Run mode ten minutes after the CSS disconnects.

After changing the Revert to Run mode setting from Never to 2 minutes or 10 minutes, you must manually put the base station in Run mode. Only then does the configuration change take effect. Thereafter, if the base station is left in Standby mode, it will automatically revert to Run mode.

Disconnection can occur in the following situations:

- You disconnect the CSS from the network element.
- The CSS session times out after communications fail.
- The network element restarts, for example after a power failure at the site.

NTP

A Tait network element can automatically synchronize its clock time with an NTP (network time protocol) server. If all network elements in a network do this, their clocks are synchronized, so that call records and other logs from one network element can be correlated with those from other network elements or from the trunking RFSS controller. For more information, see www.ntp.org.

NTP is generally used in trunking networks. It can also be used in conventional networks, particularly if an NTP server is already available. NTP can make diagnosis easier for Tait support if problems emerge.

Simulcast base stations **must** have NTP provided by a GPS-controlled NTP server. This enables them to check the alignment of the 1 PPS signal.

A diagnostic test is available for NTP, see "Time Synch (NTP) Test" on page 233.

NTP

If you select the NTP check box, the network element regulates its clock time from one or other of the servers you specify.

If you clear the NTP check box (the default), whenever the CSS connects to the network element, the network element updates its clock time to match the time on the CSS PC.

Server

Enter the IP address of a GPS-controlled NTP server. (This could be a dedicated NTP server for the TaitNet P25 digital network, your organization's NTP server, or a public NTP server.)

Alternate server

This box makes it possible for you to supply the IP address of a second device that can provide NTP time. However, we recommend that you leave the Alternate server box at its default value (0.0.0.0). If you do specify an alternate server, make sure that it is of equal quality, otherwise timing accuracy will be compromised, as the NTP daemon will vote between the two servers..

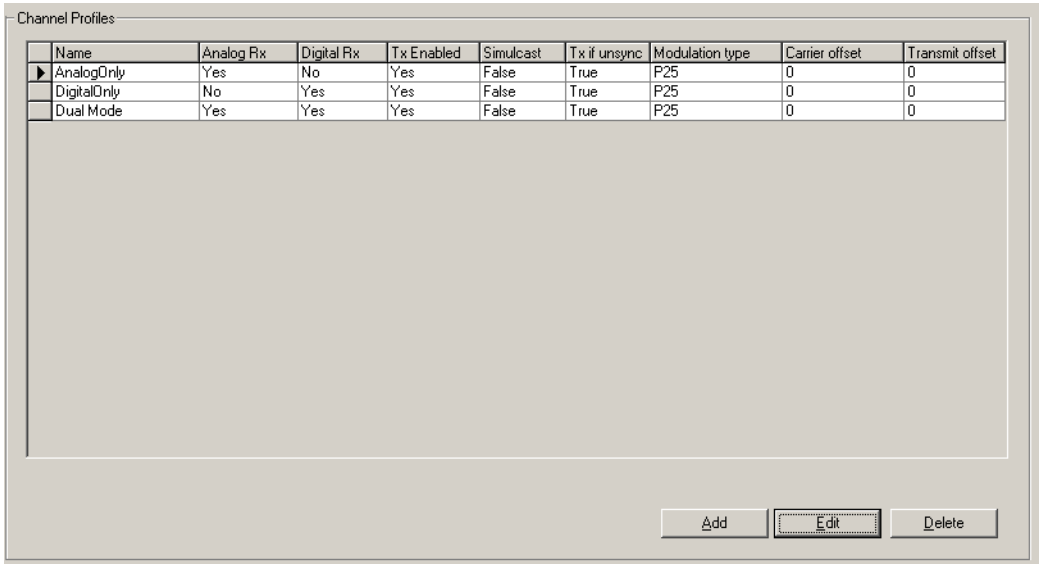
Specifying only one NTP server, as recommended, does mean that if the NTP server goes down, the network element has no NTP source. However, its own frequency reference has 0.5 ppm accuracy (which means a 1 second drift in about 23 days). Also, the NTP daemon creates a drift file, recording the drift of the local clock relative to the NTP server. If the server goes down, the daemon uses the drift file to correct the local clock.

RF Interface

The behavior of the RF interface is determined by the channel profile and the signaling profile that are assigned to the current channel in the channel table. You can also configure the sending of a morse code station ID.

Working with Channel Profiles

The Channel Profiles form (Configure > RF Interface > Channel Profiles) displays the list of profiles. You can add a new profile, or edit an existing one.



The form displays a row of information for each profile. An arrow appears alongside the profile selected on the form. To sort the display by a particular column, click the column heading.

The **Name** column indicates the name of the profile.

The **Analog Rx** and **Digital Rx** columns show you whether the profile lets the base station receive analog FM, digital P25, or both (dual mode).

If the **Tx Enabled** column displays No, the base station cannot transmit if its channel is assigned that profile.

The remaining columns are of interest for simulcast networks.

For more detail about these columns, and about other profile details, see "Editing a Channel Profile" on page 136.

Buttons along the bottom of the form let you add a new profile, edit the selected profile, or delete the selected profile.

Adding a Channel Profile

The base station requires at least one channel profile but you can define up to 16 of them. One is needed for each combination of parameter variations that the base station needs to provide. For example, the base station may need to operate normally in mid-band but sometimes in wideband. In addition, conditions may sometimes be noisy, so different receiver gating settings are sometimes required. For these options four profiles are needed, one for each combination of settings.

The following instructions do not deal with all configuration items. For more detailed information about the individual items, see "Editing a Channel Profile" on page 136.

Tip: Set up a test profile and assign it to a channel. Use this channel when testing the system before commissioning.

To add a channel profile

1. Select Configure > RF Interface > Channel Profiles. The Channel Profiles form appears.
2. Click a profile, and then click **Add**. A copy of the profile appears in the row below.
3. Click **Edit**. The Edit Channel Profile dialog box appears.
4. Configure the profile as needed. For details, see "Editing a Channel Profile" on page 136.
5. Click **OK** to confirm the changes and close the dialog box, returning you to the Channel Profiles form.

Editing a Channel Profile

Use the Edit Channel Profile dialog box to view the details of the selected channel profile and modify them.

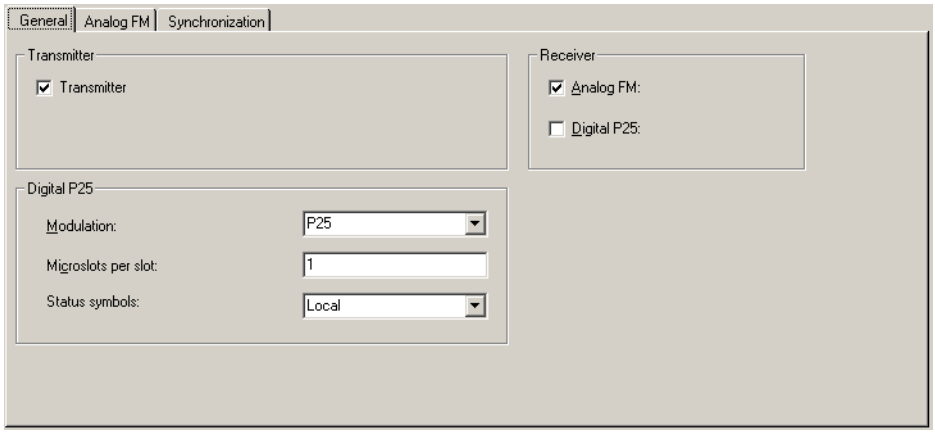
Profile name — Specifies the name of the profile. If you edit this name, make sure that the new name is unique.

Previous Profile — Displays the previous profile in the list, without requiring that you leave the dialog box. This confirms any changes you have made to the current profile, which means they cannot be undone.

Next Profile — Displays the next profile in the list, without requiring that you leave the dialog box. This confirms any changes you have made to the current profile, which means they cannot be undone.

General tab

The General tab defines general settings for the channel profile.



Transmitter

The Transmitter check box enables transmitter operation. You can clear it to disable the transmitter. A network element with a disabled transmitter and receiver can still function as a gateway.

Receiver

The Receiver area specifies which modes the base station receiver can operate in. You must select at least one mode. If both modes are selected, the base station functions as a dual-mode receiver. In dual mode, if the receiver achieves frame synchronization, it operates in digital mode. Otherwise, it operates in analog mode.

Analog FM

The base station can receive analog FM signals.

Digital P25

The base station can receive digital P25 signals.

Digital P25

The Digital P25 area contains general transmitter settings for P25 operation.

Modulation

Selects the modulation scheme used for digital P25 transmissions. TB9100 base stations always receive digital P25 signals using the C4FM modulation.

Option	Description
C4FM	The modulation scheme mandated by P25 Phase 1. Use this modulation scheme in non-simulcast systems.
CSM	Constant-envelope Simulcast Modulation. This is a modulation scheme designed to give improved performance in simulcast systems, compared to that obtainable using C4FM. You cannot use this modulation with SUs configured to receive C4FM.
Wide Pulse	Wide Pulse (also known as Wide) is a modulation scheme designed for simulcast systems. It is similar to C4FM but uses wide-band (25 kHz) channels. SUs must be configured to receive digital P25 signals on a Wide channel.

Microslots per slot

In conventional systems, most base stations will use the default value of 1 microslot per slot. With this setting, all status symbols are set to 'idle' or 'busy.' Busy means that a signal is being received on the uplink so that SUs should not transmit.

In trunking control channel operation, more microslots per slot are required. This sets up a slotted structure on the downlink. Status symbols are transmitted at every microslot boundary (every 7.5ms) but they are set to "Unknown," except at the slot boundary. We recommend 6 microslots per slot. This allows a SU to read the status symbol and transmit a TSBK before the next slot boundary, so that its status symbol is 'idle' and the next slot is available to other SUs. The maximum allowable value for control channels is 10.

Some SU signaling on the control channel uses multiple block trunking packets. Examples are requests for telephone interconnect calls and responses to authentication requests during registration. These will overlap into the next slot if there are only 6 microslots per slot. If SUs use a lot of this signaling, increasing the number of microslots per slot beyond 6 could increase control channel efficiency.

In trunked simulcast channels that handle packet data, we also recommend 6 microslots per slot, even though this setting can result in some collisions on the uplink.

Status symbols

Instructs the transmitter how to set status symbols. Generally, the option 'channel' is selected.

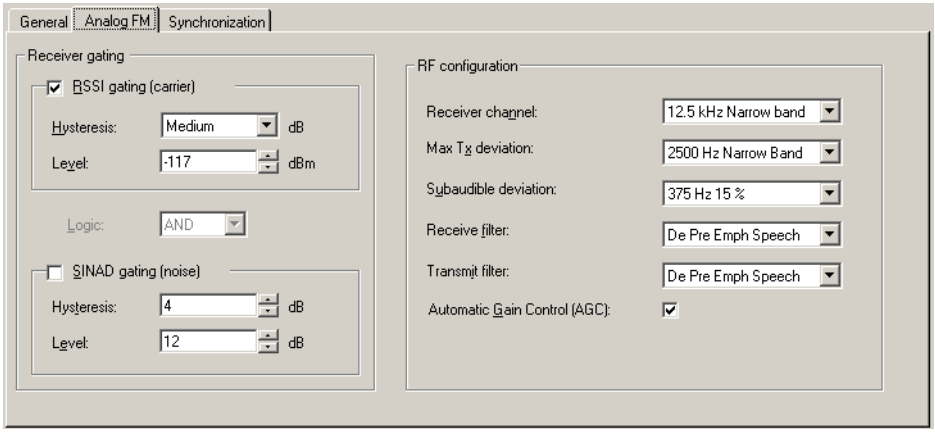
Option	Description
Local	Status symbols indicate the state of the local uplink. If the base station is receiving, status symbols are set to 'busy.' This option is only used for a particular TIA repeater conformance test, to verify that status symbols change from idle to busy when the uplink becomes busy.
Channel	Status symbols indicate the state of the channel group as a whole (as well as they can). You must select this option for simulcast, so that the transmissions all send exactly the same bits.

If you select 'channel,' the transmitter behaves in the following way:

- If the transmitted stream originated at an RF interface, the transmitter sets status symbols to busy. (If the channel group is simplex, status symbols are always set to busy).
- If the transmitted stream is outbound, the transmitter sets status symbols to idle. This is because the stream did not originate from RF. However, in a duplex channel group, the RF uplink could in fact be busy with another, inbound call.
- If the Transmitter is part of a control channel, it always sets status symbols to 'idle,' because it is not possible to know whether a member is receiving a TSBK at that very moment.
- During a synchronized transmission test, if you transmit Tone 1011, status symbols are set to 'unknown,' overriding the configuration. This is so that the transmitted bitstream matches the test pattern and equipment measuring the BER gives correct results.

Analog FM tab

The Analog FM tab configures analog FM operation of the receiver and transmitter.



Receiver gating

The Receiver gating area configures the way receiver gating (also known as receiver squelch) operates.

Analog gating can be based on:

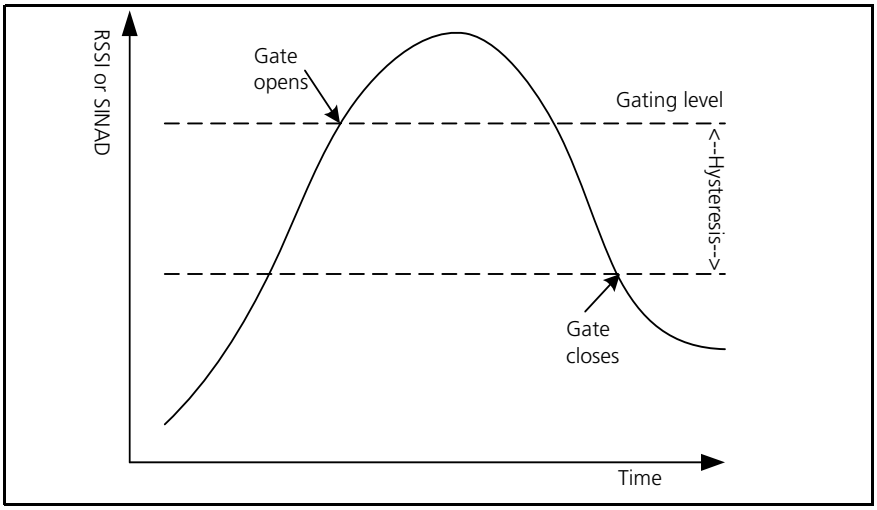
- RSSI
- SINAD
- RSSI and SINAD
- RSSI or SINAD

RSSI gating operates more quickly and is suitable for repeater links. SINAD gating takes longer but is more immune to noise interference and is suitable for the repeater itself or for a line-connected base station.

Gating in digital P25 mode is not configurable. The receiver unmutes when frame synchronization is achieved. If the signal subsequently deteriorates so that forward error correction is unable to compensate for errors, the voice stream is discontinued.

If analog gating is set at low levels for a dual-mode receiver, breakthrough of the digital P25 signal can occur in analog FM mode. The signal is good enough to unmute the receiver but not to achieve frame synchronization.

Tip: If possible, add subaudible signaling to dual-mode receivers. This prevents the analog receiver from briefly unmuting to a digital signal until frame synchronization is detected.



RSSI Gating (carrier)

Enables gating based on the base station's measurement of the received signal strength. This is also known as Carrier gating. This method is not recommended for low signal levels. If the level is set low (for example, -118 dBm) and the hysteresis is set to High, the gate may stay open permanently.

SINAD Gating (noise)

Enables gating based on the estimated SINAD (obtained by measuring the out-of-band noise). This is also known as noise gating.

Logic

When both RSSI and SINAD gating options are enabled, a drop-down list box provides options for the gating logic.

Option	Description
AND	The receiver gate opens when both RSSI and SINAD values reach the required level. It closes when either RSSI or SINAD fall below the required level minus their respective hysteresis.
OR	The receiver gate opens when just one of the RSSI or SINAD values reaches the required level. It only closes when both RSSI and SINAD fall below the required level minus the hysteresis.

Tip: Select OR and set the RSSI level high (for example -100 dBm). This gives quick gating when the signal level is high. When the signal level is low, gating occurs based on SINAD. This is slower but more accurate.

Level

The two Level boxes define the level (of RSSI or SINAD) required to enable receiver gating and pass the received audio. The RSSI level is in dBm. For equivalent values in microvolts, see "Converting Between Microvolts and dBm" on page 141.

Hysteresis

The two Hysteresis boxes specify how far the RSSI or SINAD must fall below the level set in the corresponding Level box to disable receiver gating and mute the received audio.

The Hysteresis box for RSSI gating provides the options Low, Medium, and High. Typically, these options correspond to hysteresis values of 1–2, 2–5, and 5–10 dB respectively. The actual hysteresis varies with the RSSI gating level (see below).

Choose a hysteresis level, and then test TB9100 operation, adjusting the setting as appropriate.

Gating Level	Low	Medium	High
-119 dBm	0.8	3.5	5
-118 dBm	1.1	3.4	5.9
-117 dBm	1.3	3.8	5.4
-116 dBm	1.9	3.9	6
-115 dBm	2.2	4.7	6.4
-114 dBm	2.4	4.7	6.4
-110 dBm	2.9	5.6	7.4
-105 dBm	3.4	6.1	8.1
-100 dBm	3.8	6.8	8.7
-95 dBm	4.1	6.8	8.6
-90 dBm	4.7	7	9.2

SINAD dB hysteresis is a recovered audio level measurement. It does not correlate to RF dBm levels.

Converting Between Microvolts and dBm

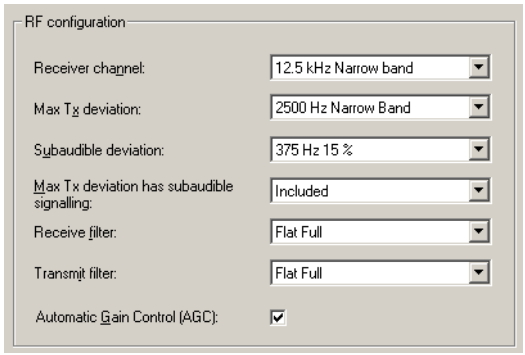
Use the following table to convert displayed levels in dBm into microvolts.

Level in Microvolts	Level in dBm	Level in Microvolts	Level in dBm
0.10	-126.99	10.00	-86.99
0.20	-120.97	12.50	-85.05
0.25	-119.03	15.00	-83.47
0.30	-117.45	17.50	-82.13
0.40	-114.95	20.00	-80.97
0.50	-113.01	30.00	-77.45
0.60	-111.43	40.00	-74.95
0.80	-108.93	50.00	-73.01
1.00	-106.99	60.00	-71.43
1.50	-103.47	70.00	-70.09
2.00	-100.97	80.00	-68.93
2.50	-99.03	90.00	-67.90
3.00	-97.45	100.00	-66.99
4.00	-94.95	150.00	-63.47
5.00	-93.01	200.00	-60.97
7.50	-89.49	250.00	-59.03

RF Configuration

In the Edit Channel Profile dialog, Analog FM tab, use the RF configuration area to specify the nominal channel spacing for the receiver and the transmitter. No hardware modification is necessary when the RF configuration is changed.

Your country may use Narrow band, Mid band and Wide band to refer to different channel spacings. Make sure that the option you select has the correct value.



Receiver channel

Specifies the receiver's nominal channel spacing. The available options are expressed both as a description (for example, Mid Band) and as the kHz value of the nominal channel spacing.

Option	Equivalent Rx IF Bandwidth
12.5kHz Narrow Band	7.5kHz
20kHz Mid Band	12kHz
25kHz Wide Band	15kHz

The Receiver channel box does not determine the actual spacing between channels. It determines the receiver IF bandwidth. For example, 20kHz Mid Band sets the receiver IF bandwidth to 12kHz. Normally, you would select this option if the channels in your band plan have a 20kHz channel spacing. However, your band plan may be irregular, or you may want to specify (when you enter frequencies into the channel table) a greater spacing between channels, for example, 50kHz.

Max Tx deviation

Specifies the highest deviation that the transmit channel is permitted to have. The available options correspond to the following channel spacings:

Option	Channel Spacing
2500 Hz Narrow Band	12.5 kHz
4000 Hz Mid Band	20 kHz
5000 Hz Wide Band	25 kHz

The Max Tx deviation box does not determine the actual spacing between channels. For example, 4000Hz Mid Band sets the maximum transmit deviation to 4kHz. Normally, you would select this option if the channels in the band plan have a 20 kHz channel spacing. However, the band plan may be irregular, or you may want to specify (when entering frequencies into the channel table) a greater spacing between channels, for example, 50 kHz.

FCC regulations do not permit mid-band or wide band transmissions in the 150-174 MHz and 421-470 MHz frequency bands. Accordingly, while the CSS does not prevent you programming the base station to transmit in this way, the transmitter will be disabled and the invalid channel alarm raised, unless the base station has the Unrestricted Wideband feature license.

Subaudible deviation

Specifies the deviation that CTCSS or DCS signaling will cause to the carrier frequency. Options are specified both absolutely in Hertz and relatively as a percentage of the selected Max Tx deviation. Gain will be applied to the CTCSS signaling to cause the deviation specified. If you subsequently alter the Max Tx deviation, the Hertz value of the subaudible deviation will alter, but not its percentage.

By default, increasing subaudible deviation correspondingly reduces speech deviation. This prevents over-deviation by ensuring that the total transmit deviation is not increased. However, you can choose not to reduce the speech deviation, see below.

Max Tx deviation has subaudible signalling

Specifies whether subaudible signaling is included in the actual maximum transmit deviation or adds to it.

Option	Description
Included	The subaudible deviation reduces the level of the audio deviation out of the limiter by the amount of subaudible deviation selected. For example, if a wide band channel is configured with a subaudible deviation level of 10% and a line input level of -10 dBm, its transmit deviation (with the subaudible signal filtered out) will be 2.5 kHz, when the line audio input is -10 dBm. The maximum in-limiting deviation will be 4.5 kHz, within the 5 kHz channel limit.
Superimposed	This is the default setting. The subaudible (10–300 Hz band) deviation does not alter the audio (0.3–3.4 kHz band) deviation transmit levels. The audio path signal thus uses all the allocated channel deviation and subaudible signals are summed on top of the audio signal, further increasing channel deviation. For example, if a wide band channel is configured with a subaudible deviation level of 10% and a line input level of -10 dBm, its transmit deviation (with the subaudible signal filtered out) will be 3.0 kHz, when the line audio input is -10 dBm.

Receive filter

The Receive filter drop-down lists let you select an audio filter (see table below) that will be applied to received analog FM signals. Select a full filter if you are passing subaudible signaling onto the line.

Audio filter	Description
Flat full	Passes audio fairly evenly across the audio range 67 Hz – 3.3 kHz.
Flat speech	Passes only audio in the speech range (300 Hz – 3.3 kHz).
De pre emph speech	Passes audio in the range 300 Hz – 3.3 kHz, de-emphasizing (attenuating) higher frequencies (receive filter) or pre-emphasizing them (transmit filter).
De pre emph full	Passes audio in the range 67 Hz – 3.3 kHz, de-emphasizing (attenuating) higher frequencies (receive filter) or pre-emphasizing them (transmit filter).

Transmit filter

The Transmit filter drop-down lists let you select an audio filter (see table above) for the transmit path.

Automatic gain control (AGC)

Specifies whether automatic gain control is applied at the RF stage. AGC provides enhanced high signal handling capabilities and receiver intermodulation protection. When signal levels are high, however, the minimum sensitivity may be degraded.

AGC is normally enabled, but Tait recommends disabling it in the following situations:

- The expected receive signal strength is < -107 dBm (1 microvolt) and strong interfering signals (> -30 dBm (7000 microvolts)) are anticipated at the receiver input.
- TIA/EIA or AS-4295 RF performance testing is being carried out.

Synchronization tab

The Synchronization tab enables and partly configures simulcast operation. (The Channel Group also configures simulcast.)

Simulcast

Select the Simulcast check box to enable the network element to function as part of a simulcast channel group.

Holdover duration

Enter the estimated time that the network element will retain synchronization if it loses its 1 PPS pulse but still has the external frequency reference. When this timer expires, the network element regards itself as unsynchronized and raises the Unsynchronized alarm.

If the 1PPS pulse is provided by GPS-disciplined equipment with an oven oscillator (such as the Tait T801-4), enter 1 hour. If the GPS-disciplined equipment has a Rubidium oscillator (such as the Spectracom 9283), enter 40 hours.

External reference equipment should be configured to stop sending the 1PPS pulse but continue with the external frequency reference when it loses GPS timing.

Local transmit offset

Enter a positive value in microseconds to delay the launch time at this transmitter. This adjustment is used to reduce the delay spread in the non-capture overlap zone.

Carrier offset

Enter a positive or negative value in Hertz to offset the transmit frequency from the configured value. A small offset may improve simulcast performance in non-capture overlap areas. Adding an offset changes the actual carrier frequency but not the transmit frequency displayed in monitoring and configuration forms.

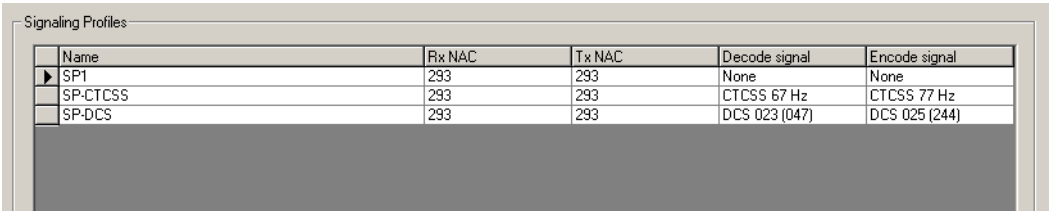
Transmit if unsynchronized

Specifies whether the simulcast base station will transmit when it is unsynchronized, the central voter is unsynchronized, or the voice stream arrives late.

If simulcast is not enabled for the base station, this check box has no effect.

Working with Signaling Profiles

The Signaling Profiles form displays a list of the current signaling profiles.



For each profile, the display shows you the NACs that are used for receiving and transmitting in digital P25 mode and the subaudible signaling that is used in analog FM mode.

Buttons along the bottom of the form let you add a copy of, edit, or delete the selected profile.

Adding a Signaling Profile

The base station requires at least one signaling profile. You can define up to 16 of them. The signaling profile defines the NACs that the base station transmits with and unmutes to, the subaudible signaling, and the tail timers. For more detailed information about the individual items in the profile, see "Editing a Signaling Profile" on page 148.

Tip: Set up a test profile and assign it to a channel. Use this channel when testing the system before commissioning.

To add a signaling profile

1. Select Configure > RF Interface > Signaling Profiles. The Signaling Profiles form appears.

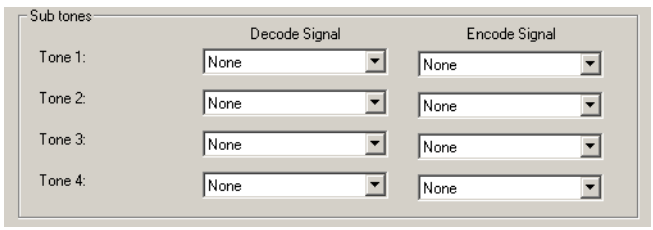
2. Click a profile, and then click **Add**. A copy of the profile appears in the row below.
3. Click the profile, and then click **Edit**. The Edit Signaling Profile dialog box appears.
4. In the **Profile name** box, enter a suitable name for the profile.
5. Under **NAC** enter the network access codes that the base station will operate on in digital P25 mode. Some systems require different values for transmitting and receiving.
6. If you want the base station to unmute to any NAC, select the **Accept any** check box.
7. For community repeater operation or to enable digital dispatch equipment to specify the transmit NAC, select the **From stream** check box.
8. Under **Subtones**, select the CTCSS tones or DCS codes that the base station will use when operating in analog FM mode. For more details, see "Configuring Subaudible Signaling for Analog FM" on page 146.
9. In the **Tail Timers** tab, configure the way that audio, signaling, and carrier end at the end of analog FM transmissions.
   a. If the network uses CTCSS signaling and the SUs are configured to respond to reverse tone bursts, enable and configure reverse tone bursts at the end of transmissions.
   b. You can enable a hang timer and specify the length of time that the base station continues to transmit carrier and subaudible signaling after audio has ceased.
   c. You can enable a soft-off timer and specify the length of time that the base station continues to transmit carrier after audio and subaudible signaling have ceased.
10. Click **OK** to confirm the changes and close the dialog box. The new profile appears in the Signaling Profiles form.

Configuring Subaudible Signaling for Analog FM

The following gives an overview of how to configure subaudible signaling for different system designs. See also "Subtones" on page 149.

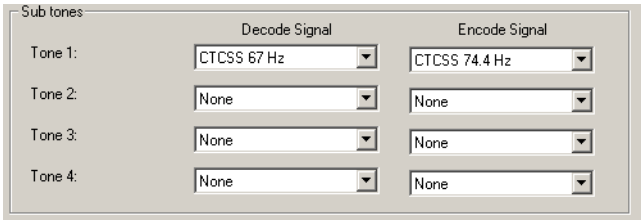
No signaling

Leave the Sub tones area at the default values. The receiver unmutes to any subaudible signaling and to none.



Single receive and transmit tone

This option can be used with channel groups. Select subtones for both Tone 1 boxes. When a call is received with Tone 1's decode signal, it is repeated using Tone 1's encode signal. If the call has another subtone or no subtone, the receiver does not unmute.



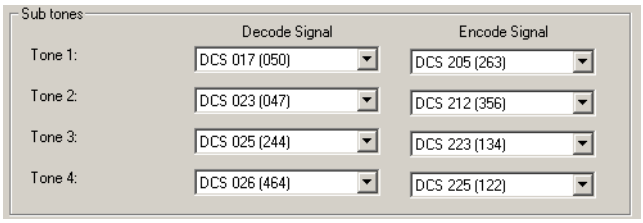
Dispatch operation

To configure the base station for line-connected operation, transmitting calls coming from the analog line or from a P25 console gateway, give Tone 1 the encode signal to use. This signaling will also be used when the base station repeats calls from a SU. Configure the signaling profile as above.

Line-connected base stations do not support multiple subtones. If you configure decode signals for tones other than Tone 1, the base station will transmit dispatch calls with the last used encode signal. For example, if a call is received with a Tone 3 decode signal and then the dispatcher makes a call, that call will use the Tone 3 encode signal.

Community repeater

This option can only be used with a single base station, as other base stations in the channel group do not know what decode signal has been received. Select up to four different subtones as decode signals and the same or different subtones as encode signals. When the base station receives a call that has one of the selected decode signals, it repeats it using the encode signal for the same tone. If the call has another subtone or no subtone, the receiver does not unmute. In this way, up to four different groups can use the channel. You cannot have a mixture of CTCSS tones and DCS codes. Make sure that you do not use a DCS code as well as its inverse.

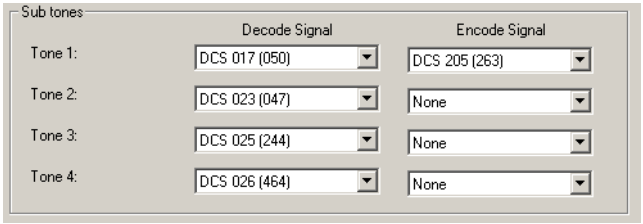


Task Manager actions

Subtones can be used to trigger Task Manager actions. First, assign the decode signal to a numbered tone, leaving the encode signal set to 'None' and then create a Task Manager task such as:

IF **Subaudible tone detected (Tone 2)** THEN **Start Timer (Timer 1)**

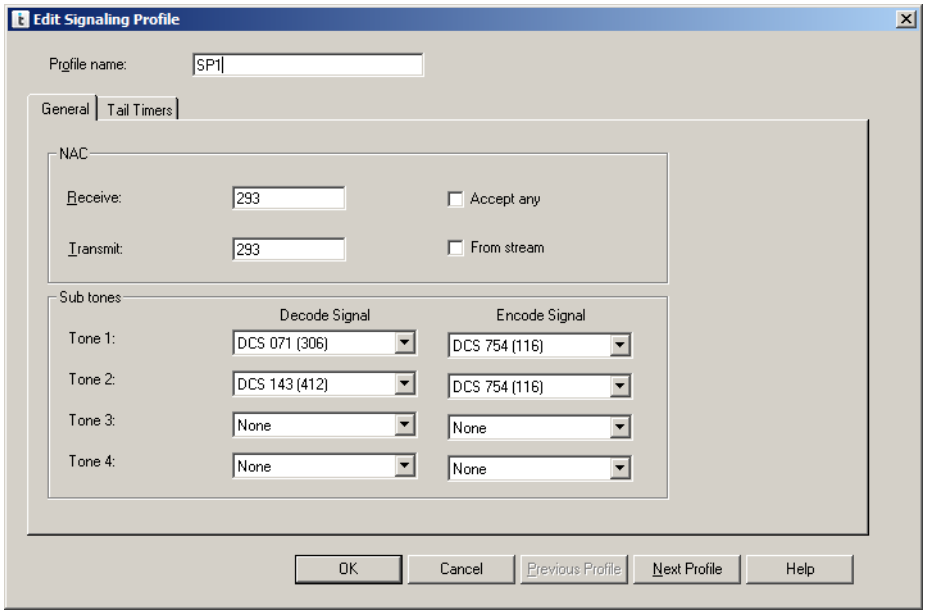
If Tone 1 is used for normal repeat or for dispatch operation, the other tones are available for Task Manager actions.



If Tone 1 is not used for normal calls, all four tones are available for Task Manager action.

Editing a Signaling Profile

Use the Edit Signaling Profile dialog box to view the details of the selected signaling profile and modify them.



Profile name — Specifies the name of the profile. This name is used in the Channel Table and Signaling Profile forms.

Previous Profile — Displays the previous profile. This means you don't need to return to the list of profiles.

Next Profile — Displays the next profile in the list.

General tab

In the Edit Signaling Profile dialog box, the General tab specifies the network access codes that the receiver recognizes and the transmitter applies. Network access codes only apply to digital P25 mode; in analog FM mode, the specified subtones are used.

NAC

Use the NAC area to specify the network access codes that the base station sends and receives. NACs are always entered and displayed as hexadecimal numbers. For more information, see the TaitNet P25 Conventional System Manual.

Receive — Specifies the network access code that the base station unmutes to. Enter a hexadecimal value (the default is 0x293). F7E and F7F are special values reserved by the P25 standard.

Accept any — Select this check box and the base station will unmute to any NAC. This is the equivalent of entering F7E or F7F. The NAC in the Receive box then has no effect.

Only select this check box if your application requires it. TB9100 receivers are highly sensitive in both analog and digital modes and can occa-

sionally falsely detect digital P25 signals. If the receiver is set to unmute only to a particular NAC value, the likelihood of false detections is greatly reduced. If not, spurious noise can be repeated. Furthermore, if the TB9100 receiver is set to dual mode, the false detection of a digital P25 signal can cause an analog FM call to drop out for up to 180 milliseconds.

For an equivalent feature in analog FM, select 'None' for the decode signal and assign any CTCSS tone or DCS code for the encode signal.

Transmit

Specifies the NAC that the base station uses when transmitting. The configured transmit NAC can be overridden by the NAC in the voice stream if the From stream check box is selected (see below). Enter a hexadecimal value (the default is 0x293). F7E and F7F are special values reserved for receivers by the P25 standard and are not permitted.

From stream

Select this check box and the transmitter will transmit using the NAC in the voice stream instead of the configured NAC. The NAC could be supplied by the calling SU (community repeater operation) or by the digital dispatch console. If the stream does not specify a NAC (or if it specifies F7E or F7F), the transmitter uses the configured transmit NAC.

Subtones

Use the Subtones area to specify the subaudible signaling that the base station will use in analog FM mode. The base station can recognize and use up to four different CTCSS frequencies or DCS codes when receiving and when transmitting. CTCSS attaches a subaudible tone to the carrier signal. DCS attaches a digital code. See also "Configuring Subaudible Signaling for Analog FM" on page 146.

If the SUs transmitting to or receiving from the base station are configured with inverted DCS codes, you need to program the base station with the equivalent normal DCS code. For details, see "Configuring the Base Station for Inverted DCS Codes" on page 150.

If you select a transmit DCS code, the base station will always transmit a DCS end tone for muting the receive audio. However, transmitting a CTCSS reverse tone burst is optional and configurable, see "Reverse tone burst" on page 151.

Decode Signal

Entries in the Decode Signal column indicate which sub-audible signaling the receiver will respond to. 'None' means that no particular signaling has been specified, so that the receiver will unmute to any calls, whether or not they have subaudible signaling. If one or more entries specify particular signals (that is, at least one decode signal does not have an entry of 'None'), the receiver will only unmute if the call has one of the specified decode signals.

When specifying CTCSS tones, select frequencies that are spread out across the available range. Do not select tones that are close to one another in frequency, as the tone reject bandwidth may not permit separating them. For example, if 67 Hz is received, both the 67 Hz and the 69.4 Hz decoders may operate.

When specifying DCS codes, you need to be aware that there is an inverse code that is exactly the same. For example, if you specify DCS 047 (023), the receiver will unmute to 047 and to 023. Make sure that you do not select one code for a tone and its inverse for another tone (for example DCS 047 (023) and DCS 023 (047), as the CSS does not check for this.

Tip: Decode signals can be used to trigger Task Manager actions. This makes it possible for the user of an analog FM SU to remotely control the base station.

Encode Signal

Entries in the Encode Signal column indicate which CTCSS tones or DCS codes the base station will use when repeating calls. If the encode signal for Tones 1-4 is 'None', the base station transmits without any subaudible signaling.

Tone n

The signaling profile can specify up to four different subtone combinations. When for example the base station receives a call with the decode signal specified for Tone 1, it repeats the call using the encode signal specified for Tone 1.

Configuring the Base Station for Inverted DCS Codes

DCS codes can be expressed as a normal or an inverted code. For each inverted code, there is an equivalent normal code. For example 023 inverted is the same as normal 047 and vice versa. In the Edit Signaling Profile dialog box, the Decode Signal and Encode Signal drop-down lists indicate for each normal code the equivalent inverted DCS code, by displaying it alongside in brackets. If the SUs are programmed with inverted DCS codes, configure the base station with the equivalent normal code. To ascertain that code, look up a table or follow this procedure.

To program the base station with an inverse DCS code

1. Note the inverted DCS code that the SU is programmed to transmit with, for example 023.
2. In the **Receive** drop-down list, scroll down until you find that code in the list of normal codes. The inverse equivalent (in this example, 047) is in brackets beside it. Note this code.
3. In the **Receive** drop-down list, scroll down again until you find the code you noted (in this example, 047). Select it. When you program this configuration into the base station, the receiver will unmute to the SU's inverse DCS code (in this example, 023, which is the same as the normal code 047).

Tail Timers tab

In the Edit Signaling Profile dialog box, use the Tail Timers tab to configure tail timers that the transmitter uses.

In analog FM, two tail timers give you flexibility in configuring tail timing. The total tail time is the sum of the hang time and the soft-off time.

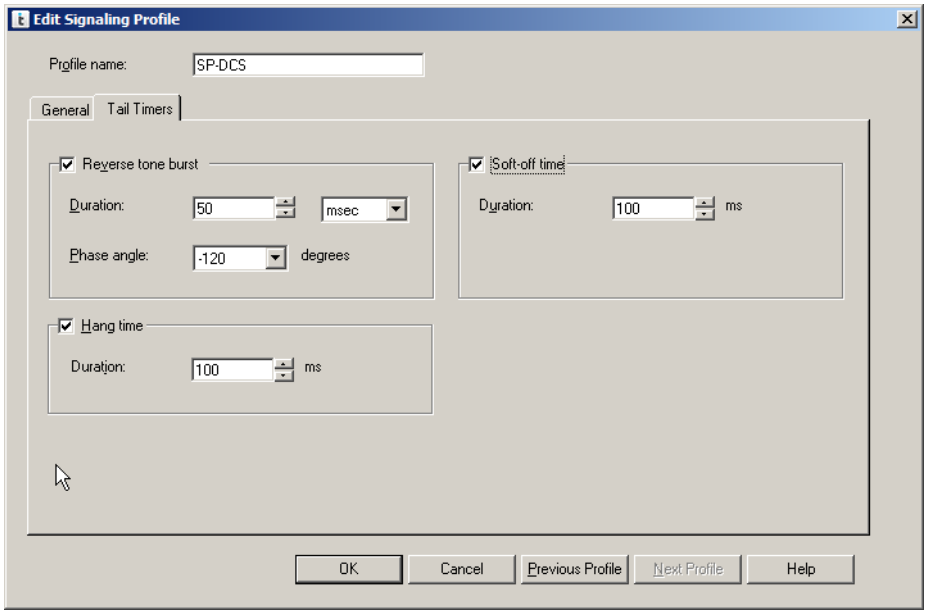
Tail timers are used to:

- eliminate squelch tail (the 'tish' sound caused when the CTCSS detector doesn't immediately re-mute the user's SU when carrier ceases)

- prevent users on different subtones from taking control of the repeater during a temporary lull in the conversation

In conventional digital P25, you can use the hang time. The soft-off time is not applied.

In trunked P25, the hang time should be disabled. The soft-off time is not applied. Trunked networks have a different type of hang time, which is configured in the site controller.



Reverse tone burst

The base station can send a reverse tone burst at the end of each transmission. This applies only to analog FM transmissions with a CTCSS tone. The reverse tone burst consists of the same tone, but is out of phase with it. In suitable SUs, this quickly mutes the receiver.

Transmissions with a DCS subtone have an equivalent: the DCS end tone. This consists of a 134 Hz tone that lasts 180 ms and is not configurable.

In the Edit Signaling Profile dialog box, Tail Timers tab, the **Reverse tone burst** check box enables the sending of reverse tone bursts.

Duration

The Duration box specifies the length of the tone burst. You can specify this in milliseconds or in cycles. If the burst has too many cycles, the SU may detect it again, re-opening the receiver gate. Specifying the duration in cycles for different CTCSS frequencies can help prevent this. Because the CSS permits the same range of values for milliseconds and for cycles, it is possible to specify a grossly excessive number of cycles. Please note that a 200 ms burst is equivalent to 13 cycles for a 67 Hz tone or 51 cycles for a 254.1 Hz tone.

Phase angle

The Phase angle box specifies the amount that the burst is out of phase with the original CTCSS subtone.

Hang time

The hang time is the length of time at the end of each transmission.

In the Edit Signaling Profile dialog box, Tail Timers tab, the **Hang time** check box enables this timer and the **Duration** box specifies the length of the hang time.

In analog FM mode

In analog FM mode, during the hang time, the base station continues to transmit subaudible signaling after Tx keying has ceased.

In conventional digital P25 mode

In digital P25 mode, during the hang time, the base station transmits terminator data units. If an SU user wants to verify that the channel is operational, he or she presses PTT briefly. The base station transmits voice during the press, and then terminator data units during the hang time. The SU receives them, displaying their RSSI and lighting its LED green, which indicates that the SU is receiving. These visible displays tell the user that the channel is available and indicate its signal strength. This performs a similar function to the go-ahead beeps on a trunked network and makes SU operation in conventional P25 more similar to trunking.

SUs need to have the correct setting for their Tx inhibit parameter (Also known as transmission politeness). If the setting is incorrect, the SU won't be allowed to transmit in digital P25 mode during the hang time. Tx inhibit can be set to 'None,' or (if the base station's channel profile is configured to have status symbols represent the status of the local repeater) to 'Correct Signaling.')

If the received signal fades, the hang time is not applied.

If the repeater is part of a chain of repeaters providing an RF link, the length of the hang time does not increase as the signal is passed down the chain.

If the base station is configured for dual mode without subaudible signaling, the actual hang time when transmitting digital P25 will be twice the configured value.

This hang time behavior in digital P25 mode has been implemented in response to a request by the US Department of the Interior. The department has also proposed that this feature be added to the P25 standards.

Soft-off time

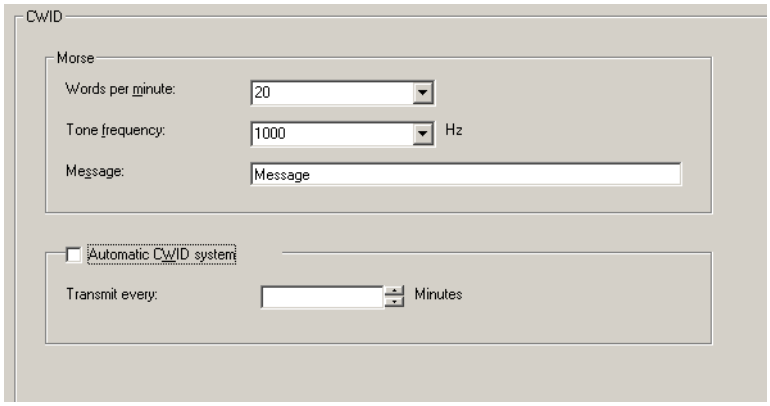
The base station can also send only carrier (carrier without modulation of any kind) at the very end of each analog FM transmission.

In the Edit Signaling Profile dialog box, Tail Timers tab, the **Soft-off time** check box enables the feature for analog FM transmissions and the **Duration** box specifies the length of time that only carrier is transmitted.

Configuring the CWID

In the CWID form (Configure > RF Interface > CWID) you can configure the way the base station broadcasts its identity using Morse code and set up the automatic sending of the CWID. In the USA, the FCC requires that base stations broadcast their identity.

Tip: Transmit using CWID before the radio system is commissioned; if there are any other users of the frequencies you have been assigned, this gives them advance warning.



In the Morse area, you define what the base station broadcasts and in the Automatic CWID system area, you can enable and configure the regular sending of identity broadcasts.

Morse

Use the Morse area (Configure > RF Interface > CWID) to specify a unique ID for the base station. The speed of transmission and the tone used can also be configured, but you should not need to alter the default settings.

The settings in this area apply to the automatic CWID transmission and to any CWID transmissions triggered by Task Manager action.

Words per minute — Specifies the speed of Morse code transmission. The 5-letter word PARIS is used to establish the number of words per minute. This word corresponds to 50 dots.

Tone frequency — The frequency of the tone used to transmit the Morse code.

Message — Enter into this box up to 30 characters to be transmitted as the station ID. You can enter any character or digit that the international Morse code alphabet supports (A-Z, 0-9, and punctuation marks). These characters will be transmitted using the International Morse Code convention. You can also enter spaces. They result in a silence equivalent in duration to seven dots.

Automatic CWID system

In the Automatic CWID system area (Configure > RF Interface > CWID) you can enable and configure the automatic sending of the base station's CWID according to the configuration in the Morse area. The licensing authority may require that the base station regularly identifies itself.

If a call is in progress when a CWID is due for transmission, the call has priority and the CWID is delayed until the voice over ends. If a CWID is being transmitted, a voice call will interrupt it. The CWID transmission is analog FM, irrespective of the base station's configuration.

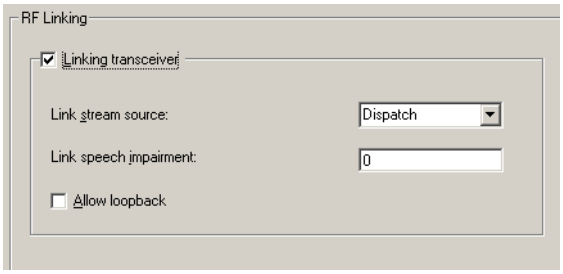
Automatic CWID system — Select the Automatic CWID system check box to enable the regular sending of the base station CWID.

Transmit every — Specifies the interval in minutes from the end of one CWID transmission to the start of the next. For example, if the interval is one minute and the transmission takes 20 seconds, the CWID will be transmitted every one minute 20 seconds.

Enabling RF Linking

If the connected base station is to be a dedicated linking transceiver, use the RF Linking form to enable and configure RF linking. Otherwise, leave the Linking transceiver check box cleared.

A linking transceiver forms one end of an RF link that joins a channel group to a remote base station or channel group. As an RF link cannot carry voting and switching information, each linking transceiver must be configured to give the streams it receives fixed information about the source and quality of the stream. The other members of the channel group use this information to make voting and switching decisions. For information about RF linking, see the TaitNet P25 Conventional System Manual.



Linking transceiver

Select the Linking transceiver check box and the TB9100 modifies its operation to suit the role of linking transceiver. The TB9100 then does the following.

- It uses the channel group interface's voting and switching rules at the RF interface.
- It flags calls received on the RF interface with a source derived from configuration instead of indicating the actual original source. The configuration can specify 'subscriber' or 'dispatch.'
- It puts a configured value for impairment into received voice streams, instead of inserting a value based on signal quality. (Impairment values are only included in subscriber streams.) Otherwise, calls received over the RF link would almost always win the vote, irrespective of the signal quality of the originally received signal.

Link stream source

The Link stream source box specifies whether the linking transceiver will flag the streams it provides to the channel group as coming from a dispatcher (line interface) or a subscriber (SU). Select the appropriate option based on your system design. The channel group that the linking transceiver belongs to will use this information when voting and selecting voice streams.

Link speech impairment

The Link speech impairment box specifies an impairment value. This is only used if the Link stream source box above specifies ‘subscriber’ (Impairment is only used in voting voice streams from a subscriber.) The channel group that the linking transceiver belongs to will use this information when voting. Select a value between 0 and 15. If the value is lower than that of other subscriber streams received by the channel group, the link stream will win the vote. If the value is higher, the link stream will lose.

Allow loopback

The Allow loopback box only has an effect if RF repeat is enabled. If Allow loopback is enabled, the linking transceiver always repeats. If it is disabled, the linking transceiver only repeats if the signal has not been received over its own RF interface.

Normally, the check box is cleared. This ensures that endless loops cannot occur. The linking transceiver cannot transmit voice streams if they arrived at the channel group from the linking transceiver's RF interface.

Select the check box if the linking transceiver is the local end of the link and the main channel group has multiple remote links. When loopback is allowed, the linking transceiver is permitted to re-transmit voice streams that it provided to the channel group. Make sure that loopback is not allowed at the remote linking transceiver, otherwise an endless loop will occur.

Channel Group

Using the CSS, you can define the identity of the network element and configure its behavior as part of a channel group. Qualified network engineers can modify the quality of service provided to different types of IP packets.

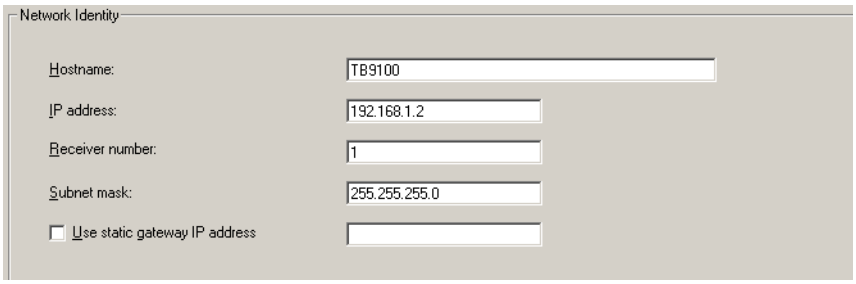
Network Identity

The Network Identity form (Configure > Channel Group > Network Identity) displays the network element's network settings. These settings are normally only changed at installation time.

Each Tait P25 network element has a unique name and IP address. The default settings provided by the factory must be changed when the network element is installed. This also applies to standalone base stations, which do not belong to a channel group.

See the Installation and Operation manual for instructions on changing the network identity. If you give the network element an unknown IP address or subnet mask, the CSS will be unable to connect to it.

When you program a configuration into a network element, the CSS checks whether the network identity (hostname, IP address, receiver number, and subnet mask) is the same as that of the network element. If there is a difference, you are given the choice of overwriting these items or keeping the existing ones, while updating the rest of the configuration. If you do change the network identity, the changes only take effect when the network element is reset.



Hostname

The name of the network element. This is the human-readable equivalent of the network element's IP address and appears on the status bar when you are connected. The default name is TB9100 but you should make sure that each base station, P25 console gateway, and trunked analog gateway on the network has a unique name. It is a good idea for this name to be the same as the name in the connection list (Tools > Connections). A blank name is not permitted.

This name is a hostname and has all the restrictions that apply to hostnames (for example, you cannot use spaces).

If you change the hostname, although the change takes effect immediately, the CSS will only show the new name on its status bar after the network element is reset.

IP address

The unicast IP address of the network element in dotted quad format. The default address when the network element leaves the factory is 192.168.1.2. This address is used for example in communications with the CSS.

There should be a line in the CSS connections list (Tools > Connections) that contains the name of the network element and its IP address, so that this CSS knows what IP address to connect to. The names programmed into the network elements should be the same as the names in the connection lists.

Receiver number

The receiver number uniquely identifies the network element as a member of the channel group. You need to assign unique receiver numbers to all channel group members (including P25 console gateways). Assign lower numbers to members that are closer to the center of the network. If there is a central voter, give it the lowest receiver number (for example, 1). Receiver numbers must be in the range 1–255. 0 is a special case. The DFSI uses the receiver number 0 to address commands to all receivers.

Voice streams contain the receiver number of the member originating the stream. Voting and switching use the receiver number when selecting a vote winner. (If other things are equal, the voice stream from the channel group member with the lower receiver number wins.) CSS monitoring forms need receiver numbers before they can indicate where the transmitting source came from or who is winning the vote. The DFSI uses receiver numbers to address commands to individual members of a channel group.

Subnet Mask

The subnet mask for the router that the network element is connected to. Enter the mask required by the IP addressing plan for the network. 255.255.255.0 and 255.255.0.0 are common subnet masks. Other masks such as 255.255.255.240 are possible but selecting them requires an understanding of subnet masks. Subnet masks are in dotted quad format but must convert to a 32-bit binary number consisting of all 1s followed by all 0s.

Use static gateway IP address

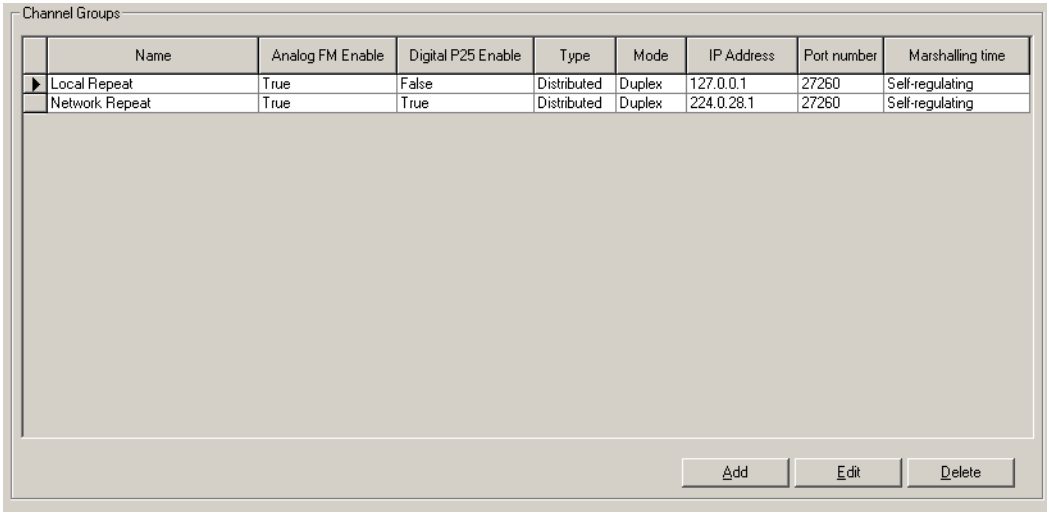
When this check box is cleared, the network element uses Proxy ARP (RFC 1027) to find out which host on the LAN will forward packets destined for the network. The routers recommended by Tait support this protocol.

Select the check box and enter an IP address into the adjacent box if you need to specify a fixed gateway address, for example because the network uses routers that are not recommended or has no local router at all.

If you select this check box, be careful when programming the configuration into other network elements. The CSS allows you to program the new configuration while keeping all of the old network identity except for the gateway IP address settings. Even if you opt to keep the existing network identity, you still need to edit the gateway IP address settings.

Working with Channel Groups

The Channel Groups form (Configure > Channel Group > Channel Groups) displays information about the channel groups that the network element can be part of. You can add channel groups and edit them.



The Type column indicates the type of voting. The Marshalling Time column applies only to synchronized channel groups and indicates whether this time is fixed or self-regulating. For more detail about the columns in the table, see "Editing a Channel Group" on page 159.

At any particular time, the network element is a member of the channel group specified by the current channel in the channel table.

Single Network Elements and Channel Groups

Single base stations are not actually part of a channel group. However, their channel definitions still reference a channel group. They need to use a special channel group definition for single base stations: 'Local Repeat.' This specifies 127.0.0.1 as the channel group IP address, which disables channel group operation and most settings in the Edit Channel Group dialog box.

However, the preamble setting still applies and determines how large the transmit buffer is. The default setting of 40 ms is intended for internal jitter only. You may have to increase the preamble, if the base station is a traffic channel or has a DFSI interface to dispatch equipment. For example, voice arriving at the base station's trunking interface has travelled from another base station via the trunking site controller and is likely to have significantly more jitter.

Make sure that all channels in the channel table reference the Local Repeat channel group.

Adding a Channel Group

1. Select Configure > Channel Group > Channel Groups.
2. Click **Add**.
3. Click **Edit**. The Channel Groups dialog box appears.
4. If desired, edit the name of the group.
5. Under **VoIP transport**, specify which call types the digital line can send.

6. Under **Voting**, select the type of voting. Voting can be centralized at one member, or there can be switching only. See the System Manual for an explanation of these options.
7. Under **Voting**, specify the voting mode (simplex or duplex). See the System Manual for an explanation of these options.
8. Enter into the **IP address** box the multicast IP address for the channel group as defined by the addressing plan for the network. Multicast addresses are from 224.0.0.0 to 239.255.255.255. Do not use a reserved address, for example, all addresses between 224.0.0.0 and 224.0.1.255. The full list of reserved addresses is published by IANA, see http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml. If the base station is single, enter 127.0.0.1. If the channel group has only two members, the unicast IP address of the other member can be used.
9. Generally, you can use the default port number.
10. Under **Channel control**, specify whether dispatcher commands only affect the channel group member that the dispatch equipment is connected to (Individual), or whether they affect the whole channel group (Collective).
11. Click **OK**.

Editing a Channel Group

In the Channel Groups form (Configure > Channel Group > Channel Groups), select a channel group, and then click **Edit** to modify it.

When editing a channel group, make sure that all channel group members have compatible channel group settings. Check these settings in the Group Status form (Monitor > Channel Group > Status).

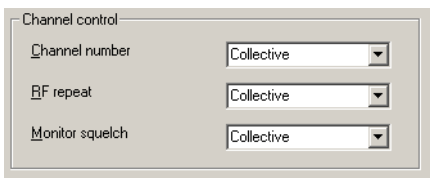
Name — The name of the channel group. Each channel group must have a unique name.

IP address — Specifies the IP address (normally multicast) that the channel group member belongs to. The member sends its voice stream to this IP address and (if the address is multicast) accepts any voice stream that is addressed to this IP address.

Port — The port number that the network elements in the channel group use for the voice stream. Generally, the default port number is used.

Channel control

The Channel control area determines whether channel control commands are applied to the individual network element or to the whole channel group. These settings apply to dispatcher commands received over the analog line or the DFSI interface. Generally, the same setting is used for all channel commands.



Channel number — If Collective is selected, a channel change command is propagated to the channel group. If Individual is selected, a channel change command only affects the network element with the interface to the dispatch equipment.

RF repeat

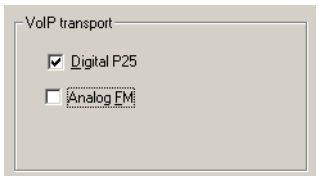
If Collective is selected, a command to enable or disable RF repeat is propagated to the channel group. The channel table must specify that RF repeat is DispatchControlled. If Individual is selected, the command only affects the network element with the interface to the dispatch equipment.

Monitor squelch

If Collective is selected, a Monitor command is propagated to the channel group. If Individual is selected, the command only affects the network element with the interface to the dispatch equipment.

VoIP transport

In the VoIP transport area you can specify which types of call can be passed to the channel group along the network element's digital line. Normally, both types are enabled, but analog FM can be disabled if the bandwidth of the linking infrastructure is insufficient to support it. Either may be disabled to assist with troubleshooting. The settings in this area have no effect on data calls.



Digital P25

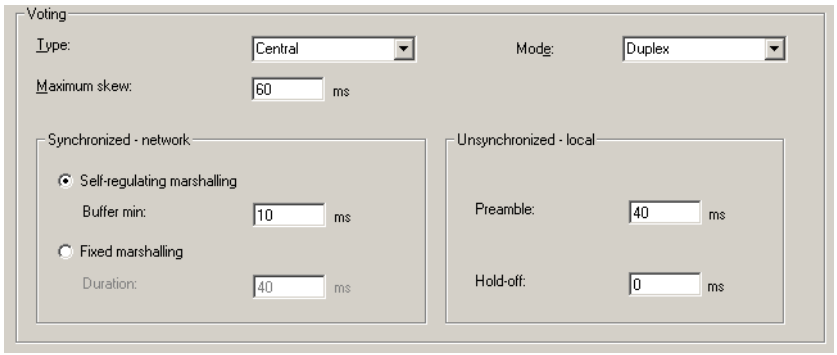
Enables the network element to send digital P25 voice to the channel group. The digital P25 voice stream is in the form of IMBE packets, which are compressed and low bandwidth.

Analog FM

Enables the network element to send analog FM voice to the channel group. The analog FM voice stream is in the form of G.711 packets, which are uncompressed and require a bandwidth of 64kbit/s.

Voting

The Voting area configures the way the network element handles voting. See the System Manual for a more detailed explanation of voting and its options.



Type

Voting in a channel group is always centralized. Members can be central voters or satellite voters that send streams to and receive streams from the central voter.

Type	Description
Central	Select Central if you want this channel group member to be the central voter. In a simulcast channel group, the member must have a transmitter. Other members will not vote their RF streams or switch any streams, but will send them to the central voter. The central voter sends a voted RF stream back to all members of the channel group for repeating. The member will only take over as central voter after ensuring that all other channel group members are in agreement. Select Central also if you want this channel group member to be a backup central voter.
Satellite	Select Satellite if the member is not expected to be the central voter.

Mode

The channel group can operate in duplex or in simplex mode. All channel group members should have the same mode setting. The mode setting is implemented by the voter.

Mode	Description
Duplex	The channel group can simultaneously handle an inbound (SU to dispatcher) and an outbound (dispatcher to SU) call.
Simplex	The channel group handles only one call at a time. It selects the call with the highest priority. Dispatcher calls always win over subscriber calls.

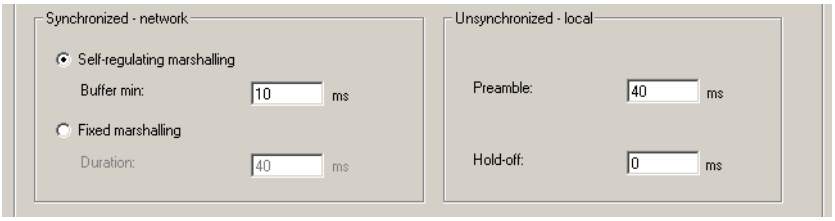
Maximum skew

The maximum skew defines how late a voice stream can be and still be voted on. It applies only to the central voter. If the maximum skew is 60 ms, a voice stream that arrives at the central voter more than 60 ms after the first voice stream will be discarded. While networks with a large link delay or jitter need a large maximum skew, the central voter does not need to wait for the maximum skew before producing its voted output. Instead, it waits until it has received a packet from each source that it knows about (has received a NID from). Once it has received a packet from each of these sources, it votes on them. If a packet is delayed, it waits up till the maximum skew time before voting.

100 ms is the largest skew that the central voter can handle. You can reduce this value to provide a small gain in voice delay in exchange for possibly excluding valuable voice streams from the voting process. This will occur for example if a voice stream arrives too late because of jitter caused by queuing at switches or routers.

Synchronized – Network

The Synchronized - network area configures voter operation in a synchronized, centrally voting channel group. The settings that are programmed into the central voter affect the operation of the whole channel group. The settings in satellite voters have no effect.



Self-regulating marshalling

When you select self-regulating marshalling, the central voter dynamically adjusts the marshalling duration based on feedback from the other members. It adjusts the marshalling duration to provide the furthest member with the transmit buffer size that you specify in the Buffer min box. We recommend self-regulating marshalling if the network can automatically change to a redundant configuration with different delay characteristics.

Buffer min

Enter a minimum buffer size that is sufficiently large to handle the network jitter. The central voter will regulate the marshalling duration so that the furthest member will have this buffer level when it begins transmitting a call. The value generally used is the worst case one-way latency (measured between the central voter and the satellite) + 40 ms.

Fixed marshalling

When you select fixed marshalling, the central voter adds the configured fixed marshalling duration to the timestamp. The transmitters will transmit in concert at a time defined by the voting time plus the fixed marshalling duration (plus any local transmit offset). We recommend fixed marshalling if predictable delay characteristics are mandated and the network timing is fixed.

Duration

Enter a sufficiently long fixed marshalling duration to allow the voted stream to reach the furthest member in time and to provide enough transmit buffer to handle the network jitter. The value generally used is twice the worst case one-way latency (measured between the central voter and the satellite) + 40 ms.

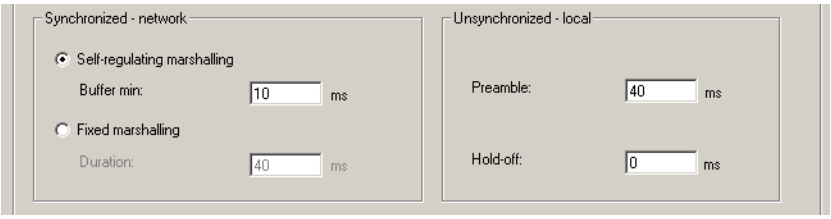
Transmit if isolated

Select this check box if you want the base station (satellite or central voter) to operate as a single base station when it loses its connection to the channel group. It will then locally repeat any RF it receives. If the channel group is simulcast, the base station must also be configured to transmit when unsynchronized.

If this check box is selected, garbled audio can result when the connection to the central voter is lost. This is because the base stations in the channel group lose synchronization. It only occurs in simulcast channel groups and only if the base stations have overlapping coverage and their signal strength is similar.

Unsynchronized – Local

The Unsynchronized - local area configures operation in an unsynchronized channel group. Each member must be programmed with appropriate settings. Members of synchronized channel groups also need these settings, if they are configured to transmit when unsynchronized. They use them if a voice stream arrives late or if the member is unsynchronized.



Preamble

Specifies the required level of the transmit buffer before the base station begins transmitting a call. It is expressed in milliseconds and is equivalent to the length of time that the base station waits after receiving a voice stream from the channel group before beginning to transmit it. During this time, the transmit buffer fills and the base station transmits a preamble. In digital P25 mode, the preamble consists of a high deviation test pattern. In analog FM mode, the preamble is carrier only. The higher the level of the transmit buffer, the longer the preamble and the greater the voice delay.

Generally speaking, the aim is to keep the preamble as short as possible (to minimize the voice delay) but as large as required by the system design. Single base stations still need an preamble to handle internal jitter. 40 ms is certainly large enough for this purpose, but a smaller buffer may suffice.

The maximum available buffer size is 300 ms. If the base station has an antenna relay, the effective maximum is 260 ms; entering a preamble larger than 260 ms will not lengthen the preamble.

Hold-off

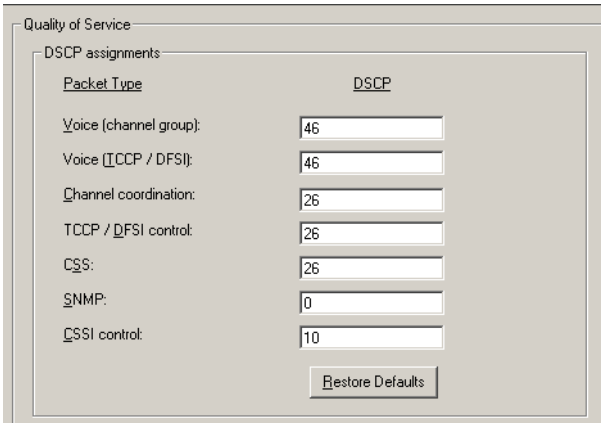
Specifies the length of time that the base station may wait after receiving the start of a stream before beginning to transmit the preamble. The purpose of this timer is to allow all the transmitters in the channel group to begin transmitting at about the same time. This is important if the receiving SUs are scanning or voting. (SU scanning works best if the base stations can all begin transmitting within approximately +/-10 ms of each other.)

In channel groups with centralized voting, only the transmitter in the member with the central voter applies the hold-off. The other members only apply the preamble.

For single repeaters, leave the hold-off at the default of 0 ms.

Quality of Service

You can use the Quality of Service form (Configure > Channel Group > QoS) to alter the default assignment of DSCP values to the different types of packet that the member sends on its Ethernet interface. The selected DSCP values are put into the headers of the IP packets (see RFC 2474 and RFC 2475). The DSCP value for Syslog messages is not configurable. The CSS can also be configured to use a specific DSCP value for its communications (select Options > Settings).



Changes should only be made by qualified network engineers. They could bring benefits where the available network bandwidth is limited. Routers and switches can be configured to apply different quality of service tools based on the DSCP value. Control channels and central voters could be given higher DSCP values than traffic channels and satellite voters.

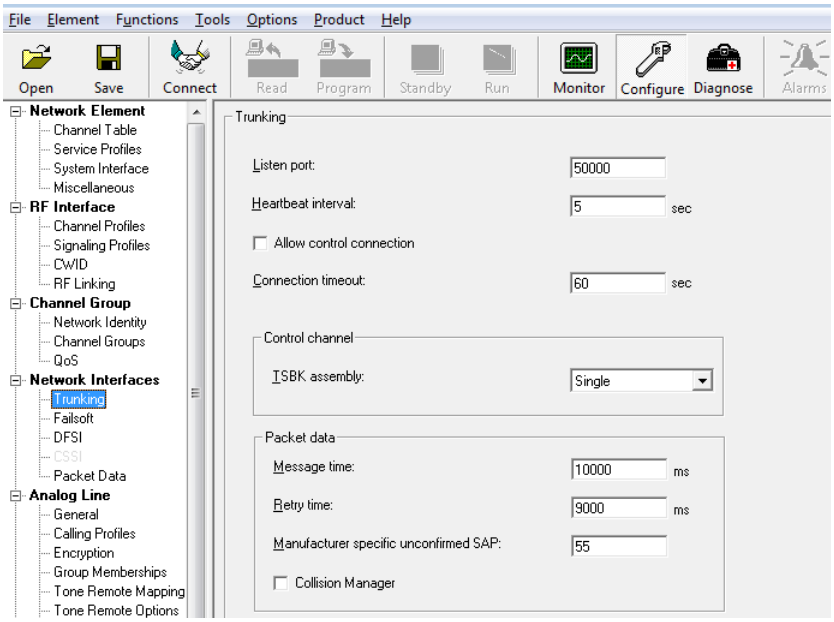
Restore Defaults — Restores DSCP values to their original defaults.

Network Interfaces

A network element can be a master, with an interface to a trunking site controller, a failsoft gateway, with interfaces to dispatch equipment and to a group control tree, or a console gateway, with a DFSI interface to digital dispatch equipment. You can enable and configure these interfaces using the items under Network Interfaces in the menu tree.

Trunking

Use the Trunking form (Configure > Network Interfaces > Trunking) to set up the channel group member's interface to the trunking site controller. This is required for control channels and for traffic channels.



Listen port
: Tells the member which UDP port to listen to for messages from the site controller.

Heartbeat interval
: Specifies the interval between heartbeat messages that the member sends to the site controller.

Allow control connection
: Select this check box to enable the member to become the channel group master. This allows the trunking site controller to establish a control connection to the member, making it the master.

Connection timeout
: Specifies how long the master waits before concluding that the control connection is lost. This should be a multiple of the heartbeat interval, so that several heartbeats must fail to arrive before the timeout.

Control channel

Configures operation of the master when the site controller has instructed the channel group to be a control channel.

TSBK assembly
: Specifies how many TSBKs can be sent in one outbound signaling packet.

Option	Description
Single	Outbound signaling packets contain a single TSBK. This is the default setting and will be suitable for most systems. It is the best setting where coverage is marginal.
Double	Outbound signaling packets can contain up to two TSBKs.
Triple	Outbound signaling packets can contain up to three TSBKs. This may bring performance improvements in busy sites with lots of call requests and registrations. More TSBKs can be transmitted per framesync and NID. However, SUs will take longer to find the control channel and noise will have a greater impact on channel efficiency.

Packet data

Durations for the following packet data timers are configurable. They are used when sending confirmed data over the RF interface. (The site controller determines whether data is handled as confirmed or unconfirmed data.)

Message time

If the message time elapses and the confirmed data message is still undelivered, the master discards the message.

Retry time

When the base station has sent a block, it waits for the retry time before re-sending the block. (If an ACK is received during the retry time, the base station sends the next block. If a NACK is received, it immediately re-sends the block.) In the absence of an ACK, it will keep re-sending until the message time elapses.

The retry timer starts after the last block is sent over the air, so the gap between sending and re-sending stays the same, irrespective of packet size.

Tip: If the data application applies its own retry policy, having the base station using retries as well can cause problems. Set the message time to be shorter than the retry time to disable layer 2 retries.

Manufacturer specific unconfirmed SAP

Trunked traffic channels that are to carry data for the P25 TaitNet Data Service (PNDS) need to be configured with SAP 0x55. This configuration setting alters the way the trunked traffic channel handles uplink data if it is sent by SUs using the Tait manufacturer ID (0xD8). Otherwise it has no effect.

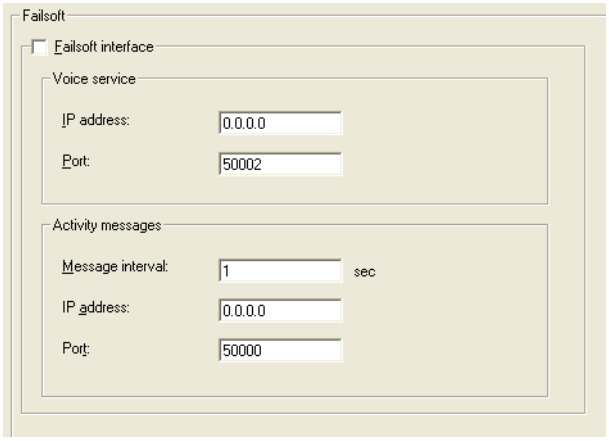
Collision Manager

When selected, this setting improves performance for trunking channels or for conventional channels dedicated to packet data. For other applications leave cleared.

Failsoft

Use the Failsoft form (Configure > Network Interfaces > Failsoft) to enable and configure a network element for failsoft mode. Failsoft is an optional mode of channel group operation. It is only available for trunked networks. For an overview of failsoft mode, see the trunked system manual.

If you are connected to a trunked analog gateway, and select that product type, the CSS disables Failsoft in the menu tree. Select Product > Base Station to enable the display.



Failsoft interface — Select the Failsoft interface check box to allow the network element to operate as a failsoft gateway or a failsoft repeater.

Voice service

Enter the IP address and port number for the failsoft voice service.

Activity messages

Failsoft repeaters and failsoft gateways send activity messages when they are operational (in failsoft mode).

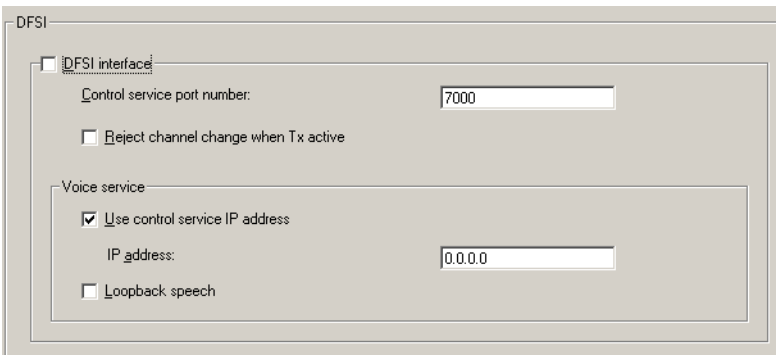
Message interval — Specifies the time between activity messages.

IP address — Specifies the destination IP address of activity messages.

Port — Specifies the port that activity messages are sent to.

DFSI Interface

The channel group member that acts as a gateway between the channel group and the digital dispatch console must have a Digital Fixed Station Interface. Use the DFSI form (Configure > Network Interfaces > DFSI) to enable and configure this interface.



DFSI interface — Select this check box to enable the DFSI interface. A Digital Fixed Station Interface feature license is also required.

Control service port number — Specifies the number of the port on which the gateway member will listen for control service messages. This can usually be left at the default of 7000.

Reject channel change when Tx active

When this check box is selected, the dispatcher cannot change channel if the channel is already transmitting. The TIA standard for the DFSI interface (TIA-102-BAHA section 8.3.2.5.3) requires this behavior. It prevents the dispatcher from inadvertently clearing an existing call when changing the channel.

When this check box is cleared, dispatchers can change channel even if that channel is already active. This setting may be preferred for safety reasons, because it does not lock dispatchers out of channels that are permanently transmitting (for example, because of a stuck microphone or continuous interference with RF repeat enabled).

Voice service

Use control service IP address

Select this check box if you want the member to send voice streams to the IP address of the DFSI control service. Otherwise clear the check box and enter the destination IP address into the box below.

IP address

Specifies the IP address that the member sends voice streams to. This can be a multicast address. The member uses the port specified for the voice service in the digital dispatch console's connect message.

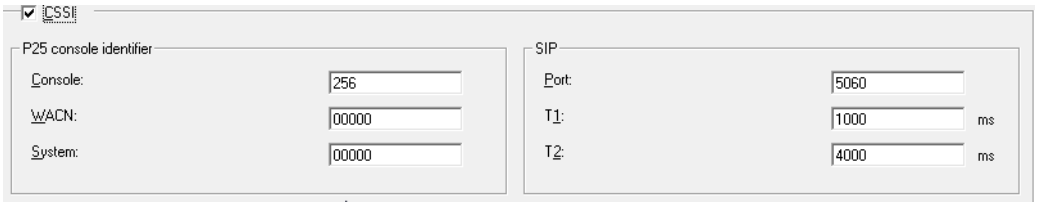
Loopback speech

Select this check box if the dispatch equipment using the DFSI needs to receive the voice streams that it sends. For example, dispatch equipment could use the loopbacked voice streams to make one dispatcher's voice available to other dispatch positions.

CSSI Interface

Use the CSSI form (Configure > Network Interfaces > CSSI) to enable and configure the CSSI interface of a trunked analog gateway. The CSSI interface connects the gateway to the P25 trunked network.

The timers and other parameters in this form will be configured at commissioning time and should not normally be changed in an operational network. Many will be left at the default values recommended by the TIA standard.



CSSI

Select the CSSI check box to enable the gateway's CSSI interface. Now it can communicate with one or more RFSS controllers, provided that it has the CSSI feature license.

P25 console identifier

This area defines the identifiers used by the gateway.

Console

Enter a suitable decimal ID that uniquely identifies the gateway and the console connected to it. The RFSS controller gives priority to consoles with lower Console ID.

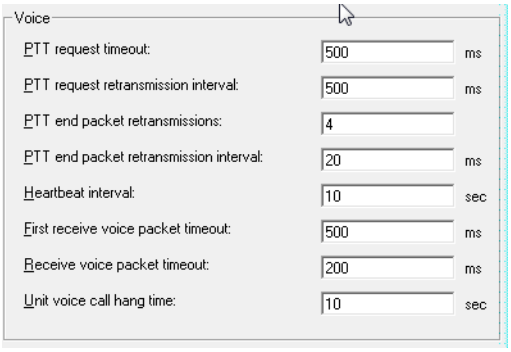
WACN	The 20-bit hexadecimal ID of the wide area communications network that the console belongs to. Enter the value used by the RFSS controllers.
System	The 12-bit hexadecimal ID of the system that the console belongs to. Enter the value used by the RFSS controllers.

SIP

Port	UDP port number that the gateway uses for sending and receiving SIP messages. (The CSSI interface uses the SIP protocol for setting up sessions between participants in a call.) The gateway must use the same port as the RFSS controller. Port 5060 is the standard port number for SIP messages and should not be changed.
T1	Defines the duration of the T1 timer used by the SIP protocol.
T2	Defines the duration of the T2 timer used by the SIP protocol.

Voice

The following timers and other parameters configure the operation of the gateway. Most can be left at their default values.



PTT request timeout	The length of time that the gateway waits after transmitting a PTT request, before concluding that the request has not been answered. The gateway should wait long enough for a mode change at the transmitting sites (400 ms).
PTT request retransmission interval	The interval between retransmissions of the PTT request. Applies only to unit-to-unit and ISSI group calls.
PTT end packet retransmissions	The maximum number of times that the gateway will retransmit PTT transmit end packets. Applies only to unit-to-unit and ISSI group calls.
PTT end packet retranmission interval	The interval between retransmissions of the PTT transmit end packet. Applies only to unit-to-unit and ISSI group calls.
Heartbeat interval	The interval between heartbeats that the gateway sends on the CSSI RTP voice stream. These heartbeats indicate to the trunked core network that the gateway is still participating in the call.
First receive voice packet timeout	The maximum length of time that the gateway will wait for the first voice packet to arrive. Applies only to inbound calls.

Receive voice packet timeout

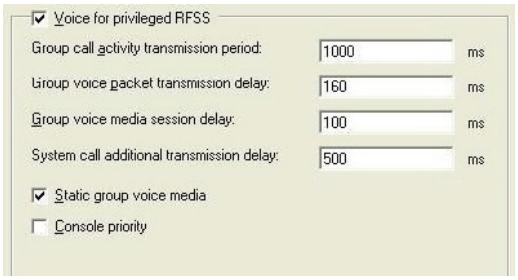
The maximum length of time that the gateway will wait for the next voice packet to arrive. Applies only to inbound calls.

Unit voice call hang time

The maximum length of time that a unit to unit call can have no voice activity. When this time is exceeded, the gateway leaves the voice call multicast address.

Voice for Privileged RFSS

The Voice for Privileged RFSS area contains timers and other parameters that configure the operation of the trunked analog gateway's interface to a privileged Airbus DS RFSS controller. The settings may need adjusting, particularly if network performance is not within the specified requirements. For more details, see the section on the trunked analog gateway in the P25 trunked system manual.



Voice for privileged RFSS

Selecting the Voice for privileged RFSS check box enables the gateway to connect to its home RFSS as a privileged RFSS. This means using a subset of the CSSI protocol together with the Airbus DS protocols GCT (Group Control Tree) and RVP (RFSS Voice Protocol) for group calls.

We recommend that you select this check box if the gateway is part of a Tait network with Airbus DS controllers. Clear the check box if the gateway is part of a Tait TN9400 network. TN9400 networks fully comply with the P25 CSSI standard and do not support the privileged RFSS setting.

Group call activity transmission period

This parameter is not normally changed. It determines the interval between group call control messages that the gateway sends using the group control tree protocol. If the interval is too short, the broadcast messages could overload the network. Lengthening the interval increases the risk that radios will miss the beginning of the call.

Group voice packet transmission delay

The gateway delays outbound group voice calls by this amount, so that the site controllers have time to join the multicast address and allocate a traffic channel before voice starts. Select a suitable value that reflects the network delay and the call setup time. There should be enough delay so that the start of the call is not normally lost. There is a trade-off between minimizing call setup time and minimizing the risk of cutting off the start of the call. In version 2.03 networks, this timer is started when the dispatcher presses PTT. In networks that are version 2.04 and above, this timer is started when the gateway receives a PTT grant or when the PTT request timeout timer expires.

Group voice media session delay

The length of time that the gateway waits after indicating that it is about to send a PTT request before sending that request on the group voice media tree. The purpose of the timer is primarily to allow IMG(s) (ISSI media gateways) time to join the multicast tree for the call.

System call additional transmission delay

This parameter provides an additional delay to the above delay for system calls (calls to 65535 or to the configured system call ID, see "System call ID" on page 196). This is needed to give radios time to exit from group calls and join the system call. While this timer is running, the gateway puts queued beeps on the analog line, to indicate to the dispatcher that a call is waiting. This delay is also applied to announcement group calls for which the Associated group override is enabled.

Static group voice media

If this check box is selected, the gateway opens a connection to the group voice media tree as soon as it registers its talkgroup and maintains that connection as long as it is registered as belonging to the talkgroup. The connection is maintained, provided the talkgroup continues to be registered. This prevents speech loss caused by the loss of a call setup message on the multicast group control tree.

Console priority

Selecting this check box gives console calls priority over all calls on the talkgroup including emergency calls. This is customary when the trunked analog gateway links legacy analog dispatch equipment to the trunked network. However, in privileged RFSS mode, the trunked analog gateway can also be used to link a conventional channel to the trunked network. In this case, voice calls should not have priority over other SUs.

To enable voice calls to be given a fixed priority level so they don't preempt other users (networks with privileged RFSSs only), select the Voice for privileged RFSS check box and clear the Console priority check box.

Registration

Re-registration period

The re-registration period specifies the time interval between group affiliation messages that the gateway sends to the RFSS controller. Like any SU, the gateway must send these messages, asking to join the group.

Supplementary data timers

The Supplementary data timers area displays default values for timers used by supplementary data. You should not normally need to change these values.

Response Tx timeout

When this timer expires, the gateway will stop waiting for the dispatch console to acknowledge an inbound supplementary data message.

Response Rx timeout

When this timer expires, the gateway will stop waiting for the called party to acknowledge an outbound supplementary data message.

Conventional Packet Data

A network element can be configured to function as a packet data gateway for use in a P25 conventional network. This function is not used in trunked networks. The following network elements are suitable for this role:

- standalone base station
- base station in a channel group (must be the central voter)
- P25 console gateway (must be the central voter)

Use the Conventional Packet Data configuration page (Configure > Network Interfaces > Packet Data) to enable and configure operation as a packet data gateway.

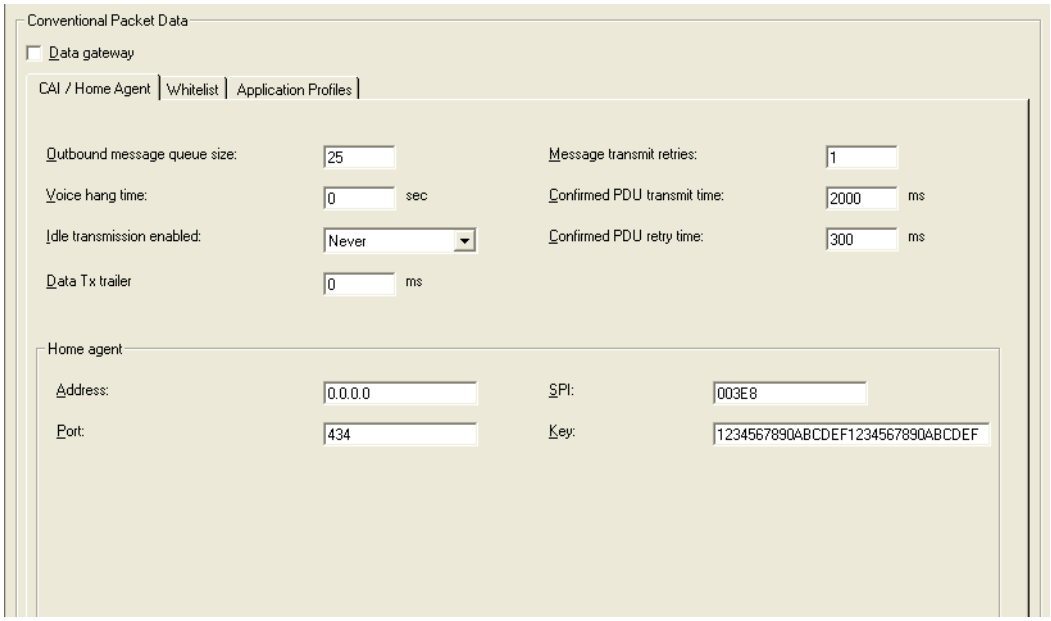
Data gateway

Select this check box to enable the network element to operate as a data gateway. The network element must have a Conventional Packet Data Services feature license.

CAI / Home Agent

The CAI / Home agent tab configures the gateway's interfaces. One interface is to P25 radios over the P25 common air interface (CAI) and the other is to the home agent over IP.

The main area of the CAI /Home Agent tab contains settings that affect the RF interface between the base station and the radio. If the data gateway is a base station, it provides the RF interface itself. If the data gateway is a console gateway or a central voter, the channel group provides the RF interface and these settings affect what the data gateway sends to the channel group for transmission over the air.



While most settings can be left at their defaults, those affecting retries (Message transmit retries, Confirmed PDU transmit time and Confirmed PDU retry time) should be adjusted to reflect the particular network and the data applications it supports.

Outbound message queue size

The maximum number of messages waiting to be sent over the CAI that the data gateway's queue is permitted to hold.

Voice hang time

The voice hang time specifies how long the data gateway waits after voice transmission on the channel group ends before it can begin transmitting packet data.

Idle transmission enabled

This drop-down list specifies the situations when the otherwise idle channel transmits ETDUs or LCWs. These contain status symbol information, which indicates whether the uplink is busy.

Option	Description
Never	The channel never transmits ETDUs or LCWs when it is idle
Always	The channel always transmits ETDUs or LCWs when it is otherwise idle
RF receive	The channel only transmits ETDUs or LCWs when it detects that a radio is transmitting on the channel. The channel transmits ETDUs to tell the other radios on the channel not to transmit data.
RF receive & hangtime	The channel transmits ETDUs or LCWs when it detects that a radio is transmitting on the channel and also during the voice hang time. This ensures that radios on the channel do not transmit data when there is an increased risk that the transmission will be overridden by voice. Otherwise, if the data transmission is overridden for the configured number of retries, the data message does not get through.

Data Tx trailer

Configures the length of time during which the channel transmits ETDUs after data has been transmitted. This occurs regardless of the Idle transmission enabled setting above.

Message transmit retries

The number of layer 3 retries that the data gateway undertakes. Layer 2 retries are configured by the two settings below.

Confirmed PDU transmit time

The maximum length of time that the gateway waits before sending the next PDU. This timer applies to confirmed data, which the gateway currently always uses. It starts when the packet is sent and continues to count down through retries. It only expires if no positive acknowledgement is received.

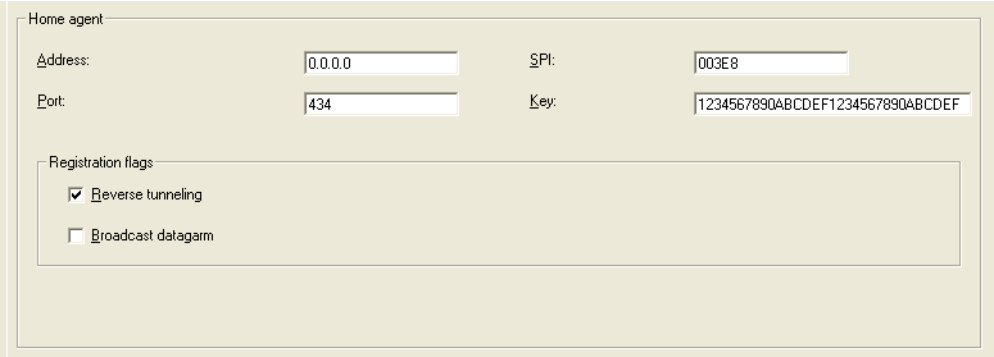
Confirmed PDU retry time

The length of time that the gateway waits after sending a PDU before re-sending it. If the gateway receives a NACK for the PDU, it immediately resends. If it receives no response, it waits until this timer expires and then resends the PDU. If it has not received an ACK when the Confirmed PDU transmit time expires, it continues with layer 3 retries or discards that PDU and sends the next one in the queue.

Tip: If the data application applies its own retry policy, having the gateway using retries as well can cause problems. Set the Confirmed PDU transmit time to be shorter than the Confirmed PDU retry time, to disable layer 2 retries.

Home agent

The data gateway functions as a foreign agent and so must be configured for mobile IP communications with the home agent.



Address — The IP address of the router or switch functioning as the home agent.

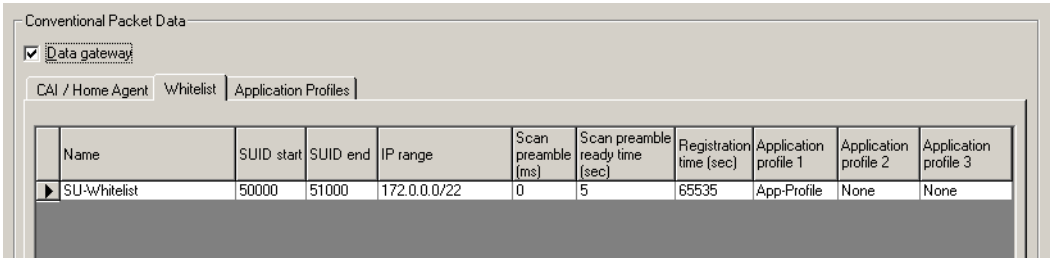
Port — The port number that the data gateway uses and expects the home agent to use. This should not normally need to be changed from the default.

SPI — The Security Parameter Index. This must be a hexadecimal number greater than or equal to 0x100. Enter the value that the home agent uses. The data gateway uses the SPI and the key to authenticate itself to the home agent.

Key — Enter the same 32-digit hexadecimal number as was entered into the home agent. We recommend that you copy and paste it from the home agent router's configuration. The data gateway uses the SPI and the key to authenticate itself to the home agent.

Whitelist

The Whitelist tab (Configure > Network Interfaces > Packet Data) specifies blocks of SUIDs that are allowed to use the data gateway and allocates IP address ranges to them. It also configures how the gateway will handle communications with radios, based on the block of SUIDs that they belong to.



Name — The name of the block of addresses.

SUID start — The first number in the SUID block.

SUID end — The last number in the SUID block. When the data gateway receives inbound data, it only accepts that data if the sender's SUID is included in the whitelist.

IP range

The block of IP addresses that have been assigned to the block of SUIDs. This is entered and displayed using slash notation. For example, 172.1.16.0/24. The /24 means that the first 24 bits of the 32-bit IP address are to be considered as the network ID, so that the block of IP addresses consists of the possible address values specified by the remaining 8 bits. These are the IP addresses from 172.1.16.1 to 172.1.16.254. (172.1.16.0 and 172.1.16.255 are not included because they have special uses.)

The data gateway will dynamically assign IP addresses from this block to radios as they register. When a radio registers, the gateway assigns the next available IP address. If a radio registers and there are no free IP addresses left, the registration will fail and the data gateway generates a SYSLOG message indicating this.

When the data gateway receives IP data, it removes the header with the care-of address, checks the whitelist to make sure that the destination IP address is within one of the defined blocks, removes the header with that address as well, and then transmits the data to the SUID corresponding to the IP address.

Scan preamble

The number of milliseconds that the gateway transmits preamble before sending data. This preamble gives SUs that are scanning for suitable channels time to find this one and tune to it before the data is transmitted. If the gateway is a standalone base station or the central voter in a simulcast channel group, leave the scan preamble at the default of 0, as a preamble is not needed. If the gateway is part of a non-simulcast channel group, the scan preamble needs to be long enough to enable radios to scan and vote before data starts to be transmitted.

Scan preamble ready time

This timer starts when a data transmission ends. If the gateway sends data after the timer has expired, it sends the scan preamble before sending the data. If the timer has not expired, no preamble is sent.

Registration time

The length of time in seconds that a packet data registration remains valid for. The default is 65535 seconds (approximately 18 hours). This is also the maximum setting. When this timer expires, the KMF will not be able to contact the radio. The home agent may use a shorter registration time.

If the available IP addresses are shared by a large number of radios, you may want to shorten the registration time to prevent running out of IP addresses. Make sure that the registration time is longer than radio users' shift time.

Registration expiry occurs silently, so radio users will not know that their radio has lost registration (the TIA standards do not provide a message for telling radios that their registration has expired). This is likely to be a problem for mobile radios that are left permanently on. Automatic re-registration is scheduled for the next data gateway release. In the mean-time, radio users can manually initiate re-registration by power cycling the radio or changing channel and then changing back again.

Application profile 1

Selects a defined application profile for use by this block of addresses. An application profile is a group of settings that configure the protocol conversion between IP and CAI.

Application profile 2

Leave this at the default setting of None. This release of the data gateway only supports assigning one application profile.

Application profile 3

Leave this at the default setting of None. This release of the data gateway only supports assigning one application profile.

Adding a Block of Radio Addresses to the Whitelist

Before radios can participate in data communications using the data gateway, their SUIDs, and the IP addresses they can be given, must be declared to the data gateway's whitelist. Blocks of SUIDs and IP address ranges must not overlap. Within a network, the IP address range must be unique to the particular data gateway. The same IP address ranges must be programmed into the mobile IP router or switch. For basic information about each parameter in the whitelist, see "Whitelist" on page 174.

To add a block of radio addresses to the whitelist

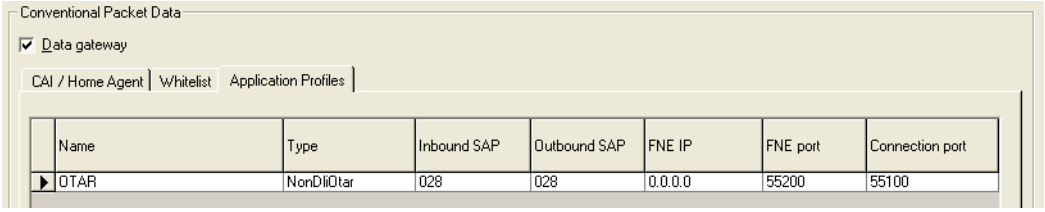
1. Select Configure > Network Interfaces > Conventional Packet Data and then click the Whitelist tab.
2. Click Add to add a new row to the table. This is a copy of the previous row.
3. Enter a name for the block of addresses.
4. Enter the start and end SUID addresses.
5. In the IP range column, enter a range of IP addresses, using slash notation. This is the same information, using the same notation, as must be entered into the mobile IP router or gateway. The IP address block must be unique to this data gateway, to prevent the same IP address being allocated to different SUs by different data gateways. The IP address block can be smaller than the SUID block.

Tip: To assign a single range of IP addresses to more than one block of SUIDs, enter two or more rows into the table, giving each one the same IP address range. To assign more than one range of IP addresses to a single block of SUIDs, proceed similarly; enter two or more rows into the table, giving each one the same block of SUIDs. The blocks must be exactly the same; one cannot be a subset of the other.

6. If the data gateway is part of a non-simulcast channel group, assign a Scan preamble time in seconds to the block. This needs to be long enough to give radios time to scan the channels in their list and vote for the data gateway's channel. If the data gateway is part of a simulcast channel group or in a standalone base station, a scan preamble is not used. Leave the Scan preamble time at its default of 0.
7. Assign a Scan preamble ready time in seconds to the block. This needs to be slightly longer than the equivalent parameter in the radios. The radio parameter determines how long the radio waits after activity on the channel before beginning to scan. For Tait radios, it is the Group hold time (if the radio has not transmitted on the channel) or the Transmit group hold time (if the radio has transmitted on the channel). Default values are 5 and 8 seconds respectively.
8. Adjust the Registration time if needed.
9. Assign one application profile to the block. Application profiles must have been previously set up, see "Application Profiles" on page 177. Currently, only application profiles of the type Non-DLI OTAR are supported.
10. Save the configuration and program it into the network element.

Application Profiles

The Application Profiles tab (Configure > Network Interfaces > Data Gateway) lists the current application profiles and lets you edit them or add to them. The data gateway uses application profiles to tell SUs which application outbound data is intended for and to provide the destination IP address for sending inbound data to.



The current release only supports the OTAR data application. The default application profile should be used and edited to provide the IP address and port of the KMF.

Name — The editable name of the connection.

Type — The type of connection. Currently, only Non-DLI OTAR is supported. In this connection type, the data gateway receives DLI OTAR data from the KMF and converts this into non-DLI OTAR for sending over the CAI, and vice versa.

Option	Description
No Connection	There is no connection over the CAI
Non-IP data	Data can be sent over the CAI. IP addresses are not contained in the data
Non-DLI OTAR	OTAR messages can be sent over the CAI. IP addresses are replaced by the SUID and not sent over the CAI.
IP data	Data in the form of IP packets can be sent over the CAI. The data is addressed to the radio's SUID and the IP address is part of the payload.

Inbound SAP — The SAP is a hexadecimal number that the data gateway will look for in the inbound data stream. If the data gateway receives a PDU from an SU with this SAP, it will forward it to the IP address in the FNE IP column. For Non-DLI OTAR, enter 0x28.

Outbound SAP — The SAP that the data gateway will put in PDU headers when it receives data from a data server with the IP address in the FNE IP column. For Non-DLI OTAR, enter 0x28.

FNE IP — The IP address of the fixed network equipment that sends or receives data for this application via the data gateway.

FNE Port — The data gateway uses this port when sending data to the FNE.

Connection Port — The data application uses this port when sending data to an SU via this data gateway.

Adding an Application Profile

In this release, there is no need to add application profiles.

Analog Line

TB9100 base stations and gateways have an analog line. The behavior of the analog line is determined by the current calling profile. The calling profile assigned to the current channel is the default calling profile. A dispatcher command can select a different calling profile.

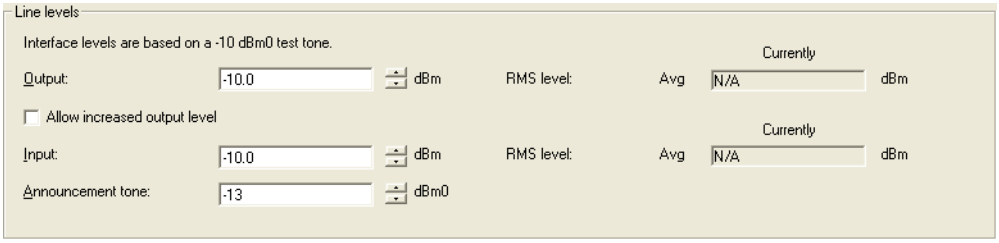
Line levels for the audio and for MDC1200 output must be set. The types of signaling used by the console system must be enabled and configured.

General Analog Line Settings

In the General form (Configure > Analog Line > General), you can set levels for the analog line. You can also enable MDC1200 signaling, set its level, select configuration options and monitor the signaling received.

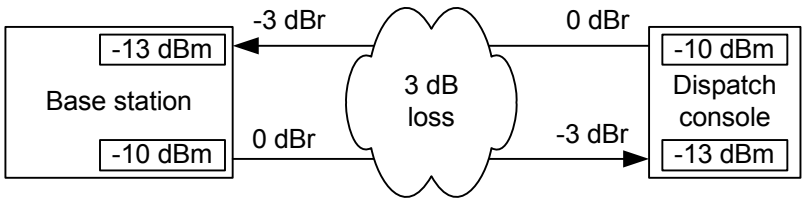
Setting Line Levels

Line levels are set in the General form (Configure > Analog Line > General) To help you, the form displays the current line levels at the analog line interface. These are measured in the digital domain and adjusted to represent the actual values at the interface pins.



Levels need to be set correctly so that the line output level does not exceed acceptable limits and so that the signal arriving at the network element switch is neither so strong that it risks exceeding the maximum value nor so weak that signal quality is affected. The levels that you enter are the absolute levels in dBm that a -10dBm0 test tone would have at the line interface.

The levels you set should implement the network level plan. In the following level plan for a very simple network, a dispatch console is directly connected to the base station along lines with a 3dB loss. The plan specifies 0dBr for each output. This is achieved by setting line levels in both the dispatch console and the base station at -10 dBm for the output and -13dBm for the input.



Output

The Output box specifies a nominal line level for the analog line output. When a TB9100 base station is receiving an analog FM signal at 60% maximum deviation, it applies a gain so that it outputs audio at this level. Enter a value based on the level plan for the network. For example, if the level plan specifies -0dBr at the analog line output, enter -10 dBm. This results in an average power level at the transmission reference point of -10 dBm, allowing 10 dB for speech peaks. You can verify the accuracy of the setting by using RF test equipment to supply a signal at 60% deviation, and reading the output in the RMS level box.

The output level is currently limited to a maximum of -10 dBm. This is to ensure compliance with telecommunication company requirements.

Allow increased output level

The Allow increased output level check box makes it possible to override the analog line's normal upper limit of -10 dBm. Telco approval generally requires that this limit is not exceeded. Select the check box to allow you to select an output level that is above -10 dBm. You can then select levels up to +1.5 dBm.

Input

The Input box specifies the line level that the network element expects on the analog line input. When the base station receives audio at this level, it applies a gain so that it transmits at 60% maximum deviation, when in analog FM mode. Enter a value based on the level plan for the network. For example, if the level plan specifies -3dBr at the analog line input, enter -13dBm. Audio sent from the transmission reference point at -10dBm will arrive at the analog line interface at -13dBm. You can verify the accuracy of the setting by looping back the analog line and using the base station's own ability to send a 1kHz test tone, measuring the maximum deviation using RF test equipment.

Announcement tone

(Trunked analog gateway only) The Announcement tone box specifies the line level of tones such as call queued, call start, call denied, and encryption warning. The gateway provides these tones to the console.

Using Deviation Measurements to Set the Input Line Level

Traditionally, technicians use transmitter deviation measurements to set line levels. While line levels in a TB9100 can be correctly set without measuring the deviation, some may still wish to use this method.

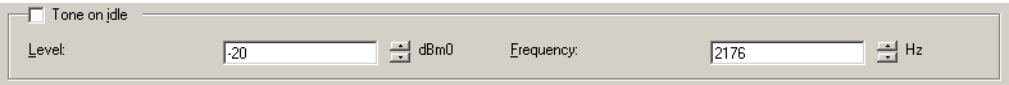
To set the input line level

1. Apply a 1kHz tone at the required reference level at the line input.
2. Set the base station to analog FM mode. (In digital P25 mode, the C4FM modem uses fixed deviation patterns that represent specific symbols. The deviation cannot be used for setting the line level.)
3. Adjust the input level (Configure > Analog Line > General) until the deviation is 60% of peak.

After the line level is set, you can also check for a transmitted tone in digital P25 mode. However, you must first change the tone frequency to 500Hz; the IMBE vocoder does not reproduce fundamental tones above about 500Hz.

Tone on idle

In the General form (Configure > Analog Line > General) you can configure the analog line to produce a tone on idle. When there is no call on the line out, a tone is sent. Dispatch equipment may need this tone as a signal that there is no inbound audio.



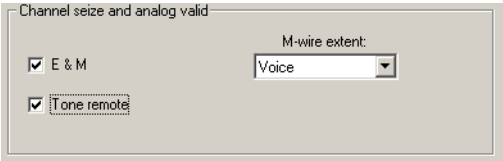
Tone on idle — Select the Tone on idle check box to enable tone on idle.

Level — Specifies the level of the tone.

Frequency — Specifies the frequency of the tone.

Channel seize and analog valid

Use the General form (Configure > Analog Line > General) to specify which signaling methods can be used by the analog line.



E & M — This check box enables E & M signaling. When the E line goes low, the network element interprets this as a . When the network element puts a valid signal on the analog line, it asserts its M line.

M-wire extent — When E & M signaling is enabled, the M-wire extent box determines the range of audio that is accompanied by M-wire signaling. It is important to select the correct setting if the dispatch console or linking equipment detects M-wire signaling.

Option	Description	Use
Voice	The M-wire is active when the network element is providing voice on the analog line.	This is the default setting. Use it to leave the analog line behavior the same as it was in versions prior to 3.30.
Voice and tones	The M-wire is active when the network element is providing voice, encryption tones or call progress tones.	Choose this setting if the M-wire is only used to unmute a speaker at the dispatch console.
All audio	The M-wire is active when the network element is providing any kind of signal. This includes the above as well as MDC1200 and tone on idle.	Choose this setting if the M-wire is used to control transmission equipment such as a microwave link to the dispatch center.

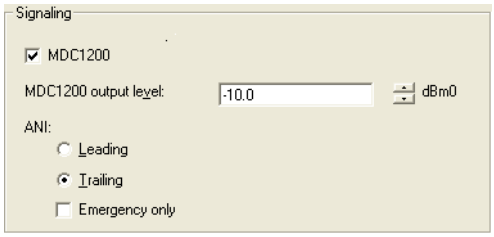
Tone remote

This check box enables the use of tone remote signaling for (tone remote signaling for other purposes such as Task Manager action and changing calling profile is always enabled). When the network element receives LLGT (keytone), it interprets this as a . The LLGT must have the properties (including the guard tone frequency) specified by Configure > Analog Line > Tone Remote Options.

If MDC1200 and supplementary services are enabled, dispatch equipment can only seize the channel if it sends MDC1200 signaling along with keytone. Keytone alone is not sufficient. Moreover, for technical reasons, the channel will be seized even if the Tone remote check box is cleared.

Setting MDC1200 Options

Use the General form (Configure > Analog Line > General) to set configuration options for MDC1200 signaling.



MDC1200

The MDC1200 check box enables MDC1200 signaling across the analog line, provided the network element has an MDC1200 signaling on analog line license. If MDC1200 signaling is used for for supplementary services (functions such as call alert, status request, which are enabled through service profiles), you also need to make sure that the analog line decodes MDC1200 before seizing the channel (in the current calling profile, Channel Seize after MDC 1200 is set to Yes).

MDC 1200 signaling must be sent to the network element before digital P25 voice transmission can begin. This is an inherent characteristic of the MDC1200 and digital P25 standards and necessarily increases the end-to-end delay, or causes the start of the call to be lost, or to interfere with the MDC1200 signaling. Which of these outcomes occurs will depend on the dispatch equipment. Sending guard tone, a single function tone, and the PTT ID takes at least 280ms.

Make sure that you include the MDC 1200 signaling time when calculating the end-to-end delay of the system. You may be able to configure the dispatch equipment to achieve a balance of initial voice loss and end-to-end delay.

Supplementary services

Select this check box to enable the analog line to handle supplementary services, converting between MDC1200 and P25 formats. The MDC1200 check box must also be enabled for the Supplementary services check box to have any effect. E&M and/or Tone remote also need to be selected in the Channel seize and analog valid area above. Selecting the Supplementary services check box enables supplementary services signaling in general; the services themselves are individually enabled or disabled in a service profile (Configure > Network Element > Service Profiles).

When this check box is selected, dispatch equipment can only seize the channel for a voice call if it sends MDC1200 signaling along with keytone. Keytone alone is not sufficient.

Enabling supplementary services means that the analog line can receive MDC1200 signaling for supplementary services and convert it into the P25 equivalent for transmission over the air, and vice versa. The base station cannot immediately transmit the supplementary services TSBKs, but must first decode the MDC1200 signaling, so that it can determine whether to begin transmitting a voice call or a TSBK. Selecting the Supplementary services check box therefore delays the channel seize.

The Supplementary services check box should only be selected if the dispatcher actually uses these services, because it increases the call setup time. However, it can be selected if MDC1200 signaling is causing noise at the beginning of a voice call.

For technical reasons, selecting this check box enables channel seize through keytone in the presence of MDC1200 signaling, even though the Tone remote check box is not selected. If the analog line does not use keytone signaling, leaving the Supplementary service check box cleared will prevent unintended channel seizes.

MDC1200 output level

Defines the level of MDC1200 signaling in dBm0. This applies only to MDC1200 signaling that the network element has generated from P25 signaling. -10 dBm0 corresponds to the level that MDC1200 is normally sent over the air (60% deviation).

ANI

Specifies for incoming digital P25 calls when the MDC1200 ANI message is added to the voice stream sent on the analog line. The setting you choose must match the setting of the console system.

Option	Description
Leading	The ANI message is supplied to the console at the beginning of the voice over. As this information is not available until after the P25 voice stream has begun, the network element must wait for it before forwarding voice on the analog line.
Trailing	The ANI message is supplied to the console at the end of the over. Delay is minimized, but the identity of the caller is not available until the end of the over.

Emergency only

When MDC1200 and Emergency only are enabled, the analog line provides MDC1200 ANI signaling for emergency calls only. This is suitable for dispatch equipment that does not mute when the gateway de-asserts its M-wire. It provides an audible indication that there is an incoming emergency voice call. When there is an emergency voice call, dispatchers hear the noise of the MDC1200 ANI signaling. Ordinary voice calls do not result in signaling noise. All other MDC1200 features (for example, status messages) are unaffected.

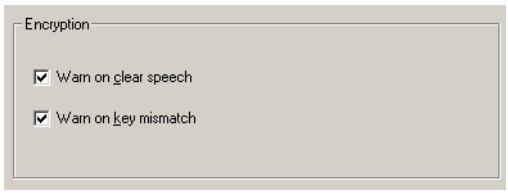
If Emergency is enabled, we recommend that the Leading option is selected, so that the signaling noise is played out at the beginning of the emergency call.

Monitor

Enable the Monitor check box to monitor any MDC1200 commands coming from the console system. The MDC1200 code for this command appears in hexadecimal in the **Event** box and the MDC1200 value of any destination addresses appears in the **Address** box.

Enabling Encryption Warnings

The General form (Configure > Analog Line > General) specifies whether warnings about encryption are sent on the analog line.



Warn on clear speech

When this check box is selected, a single beep (1500Hz) is sent on the analog line at the end of the voice over whenever a clear digital P25 transmission is passed to the analog line. Clear the check box if the system doesn't use encryption.

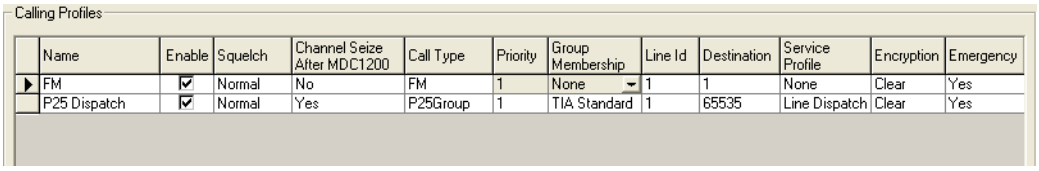
Warn on key mismatch

When this check box is selected, three beeps (500Hz) are sent on the analog line at the end of the over if there is a mismatch between the received call and the current calling profile. A mismatch occurs if the call uses a key other than the one selected in the current calling profile, if the selected key is missing, or if the current calling profile specifies clear communications but the call uses a key. If any key matches the key used by the call, that call is decrypted. The dispatcher may need to change to a calling profile that uses the key used by the caller, so that the caller can decrypt the reply.

Working with Calling Profiles

The Calling Profiles form (Configure > Analog Line > Calling Profiles) displays the list of calling profiles. You can add a new profile and edit an existing profile. A calling profile defines the properties of calls that the dispatcher makes and receives. Think of the analog line as equivalent to a SU; the calling profile defines the identity and behavior of that SU. Included in the calling profile is a service profile, which specifies what services the analog line supports, and a group membership, which specifies the groups it belongs to and therefore can listen in to.

By default, the analog line uses the calling profile specified by the current channel. Dispatcher commands can select a different calling profile. If the console system uses MDC1200 signaling, aspects of the calling profile can be overridden.



The form displays a row of information for each profile.

To create a new profile, click **Add**, and then click in each column as needed to edit it. To delete a profile, select it and click **Delete**.

Name

The name of the profile.

Enable

The Enable column contains a check box. When this check box contains a tick, the profile is enabled. When the check box is cleared, the profile is disabled. This has the effect of disabling the analog line interface, if the current channel or a dispatcher command has selected this calling profile.

If the analog line is not used, it may be desirable to disable the current calling profile to prevent unauthorized access to the channel group. You may want to disable the analog line temporarily. You can also set up a disabled calling profile and assign it to a channel in order to be able to disable the analog line interface through channel selection.

Squelch

Specifies what the analog line unmutes to. If the squelch is Normal, the network element switches any winning voice stream onto the analog line. If the squelch is Selective, the network element only switches a voice stream onto the analog line if it is addressed to the current calling profile's line ID or to a group listed in the current calling profile's group membership. The Squelch setting has no effect on analog FM calls.

If the connected network element is a trunked analog gateway, select Normal squelch. It will not work with Selective squelch. The trunking controllers only provide the trunked analog gateway with voice streams that are destined for it. You must also always specify a group ID in the Group column.

Channel Seize After MDC1200

If you select Yes, the analog line delays seizing the channel until after it has decoded the MDC1200 signaling. Otherwise, it immediately sets up a call using the information in the calling profile.

Select Yes to enable the analog line to handle MDC1200 signaling for unit to unit calls, for outgoing emergency alerts and for supplementary services. The MDC1200 check box must also be enabled (see Configure > Analog Line > General) If this check box is enabled, incoming emergency alerts are always converted into emergency ANI.

The Channel seize after MDC1200 column enables supplementary services signaling in general; the services themselves are individually enabled or disabled in a service profile (Configure > Network Element > Service Profiles).

Selecting Yes delays the channel seize, increasing call setup time. The analog line must decode the MDC1200 signaling so that it can determine whether there is a voice call or a TSBK, before seizing the channel.

We recommend that you only select Yes if the dispatcher actually uses these services, because it increases the call setup time for all dispatcher-initiated calls.

Tip: Create two calling profiles, one with a delayed channel seize and another without. The dispatcher can then use the former as required, but use the latter for ordinary operation, reducing the setup time for most calls. This is particularly useful for trunked operation.

Call Type

Specifies the type of call for dispatcher-initiated calls. The network element will turn the audio on the analog line into the specified type (P25 group, P25 individual, or analog FM). The analog line can always pass calls of any type to the console. If you select analog FM, inapplicable columns are not editable.

If the console uses MDC1200 signaling, the call type setting can be overridden as follows. If the Call type column specifies analog FM, the channel group makes an analog FM call. If the Call type column specifies P25 group or P25 individual, the channel group makes a P25 call of the type specified by the MDC1200 signaling. The line ID and destination addresses specified by the calling profile are overridden.

Select AutoReply and the network element allows the dispatcher to automatically reply to the last incoming call without needing to select the appropriate calling profile. However, when initiating a call, the dispatcher may still need to select a profile.

When the dispatcher makes a call and AutoReply is selected, the network element turns audio on the analog line into the call type of the last incoming call. If that call was P25, it defines the new call accordingly. It specifies the appropriate destination address: for individual calls it uses the source ID of the incoming call and for group calls it uses the destination ID. To encrypt the call it uses the default encryption key for the active calling profile.

Tip: If you select AutoReply, map a function tone to the 'Cancel P25 unit call' action, which the dispatcher can use to end an SU-to-SU call or to enable calling the default destination instead of the source of the last incoming call (see "Mapping Tone Remote Commands" on page 190). You can also use Task Manager to revert from an AutoReply calling profile to a standard calling profile when a timer expires after an incoming call.

Priority

The Priority setting only affects outgoing calls made by trunked analog gateways. Calls with a higher priority pre-empt calls with a lower priority. You can give the gateway's outgoing calls a priority between 1 and 7. 7 is the highest priority. 0 means that the priority is not set. Give the gateway a higher priority than the SUs in the group (the priority of SUs is set in the RFSS controller using the TTM) so that the dispatcher can pre-empt calls being made by SUs.

Group Membership

Selects one of the available sets of group IDs and assigns them to the console. Calls to these groups will be routed over the analog line to the console.

Group

When the trunked analog gateway product is selected, the Group Membership column changes to a Group column, with the default of 0 (no group). Instead of selecting a set of groups from the group memberships table, you enter a single group ID. This ID must be a normal talkgroup ID that is known to the RFSS. It specifies the group that the trunked analog gateway affiliates to. Once the gateway is affiliated to its group, the trunked network will include it in calls to that group. A trunked analog gateway can only belong to one group at a time.

Line ID

Defines the individual ID of the analog line (digital P25 calls only). The network element will pass incoming individual calls with this destination ID to the analog line. The Line ID is also used as the source ID of all outgoing calls.

In base stations and P25 console gateways, the analog line has additional IDs that are derived from the groups in the current group membership.

This is done to support the way Status Messages are implemented. Some SUs send Status Messages to an individual ID that is derived from the talk group assigned to the SU's current channel. To derive this ID, the SU adds 0xFEF000 to the talk group. For example, talk group FFFF becomes individual ID 0xFFEFFF. Talk group 0x000A becomes individual ID 0xFEF00A. These additional line IDs mean that Status Messages from these SUs are passed to the analog line. If the analog line uses MDC1200, it converts the configured Line ID (not the received ID) to MDC1200 and passes it on to the console system.

Destination

Defines the unit or group ID that the call will be sent to (digital P25 calls only). If the call type is P25 individual, enter an individual ID.

If the call type is P25 group, the following applies.

Product	Destination Type	Description
P25 console gateway or base station	Group call	Enter a group ID. Make sure that the group membership profile assigned to the channel and to the analog line includes that group, otherwise the network element will not respond to communications from other group members.
	System call	Leave at the default value of 65535 (FFFF in hexadecimal). This is a special group ID that sends the call to all SUs on the system. It is also known as an unaddressed voice call.
Trunked analog gateway	Group call	Enter the same group ID as is in the Group column.The dispatcher can only make group calls to the group that the gateway belongs to.
	Announcement call	Enter the announcement group ID. This ID must have been defined for the RFSS using the TTM. It must be the announcement group for the group specified in the Group column.
	System call	Leave at the default value of 65535 (FFFF in hexadecimal).

MDC1200 signaling can override the Destination setting.

Service Profile

Selects one of the available service profiles that specifies which services are available to the dispatch console (digital P25 calls only). The services the dispatch console is able to receive are determined by the service profile assigned to the current channel of the base station receiving the transmission.

Encryption

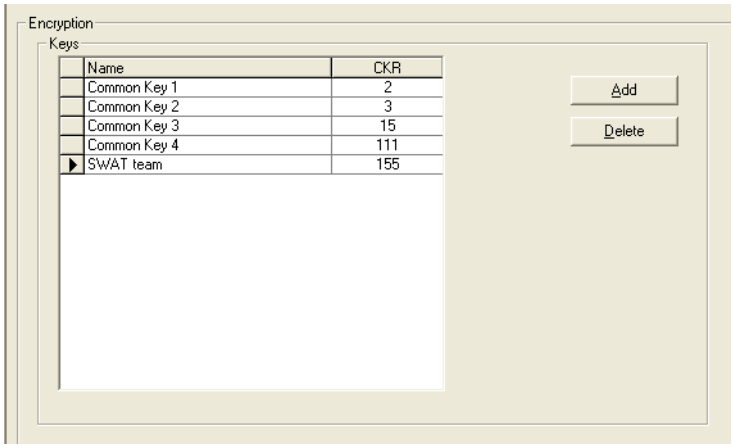
Specifies the analog line's encryption behavior. If 'Clear' is selected, the analog line does not encrypt calls and does not expect to have to decrypt them. Click in the column to display a drop-down list of keys. The key list comes from the Encryption form (Configure > Analog Line > Encryption). If a key is selected, the analog line encrypts outbound digital P25 calls using the secure key data for that key. It always decrypts inbound P25 calls if it has the key, but may sound a warning if a call does not use the expected key.

The encryption setting has no effect on analog FM calls.

Emergency — Specifies whether calls that the dispatcher makes are emergency calls (digital P25 calls only). This setting is overridden when the console uses MDC1200 signaling.

Encryption

In the Encryption page (Configure > Analog Line > Encryption) you can set up encryption so that a dispatcher can communicate securely with radios in the fleet.



Keys

In the Keys area, you can give suitable key names to the CKRs that the fleet is using. These key names are then available for assigning to calling profiles. You can also delete named keys from the keys list.

The Keys area contains a table consisting of up to 16 rows, each containing a named key and a CKR number. Click on a column header to sort the table by that column. An arrow to the left of the table indicates which row is currently selected.

Name — The name of the key. When you add a row to the Keys table, the CSS gives it a default name. You can leave this name as is or edit it to make it more meaningful, for example 'Beat 1' or 'Special duties.' The name appears in a drop-down list in the Calling profiles form. Calling profiles refer to keys by name, not by CKR.

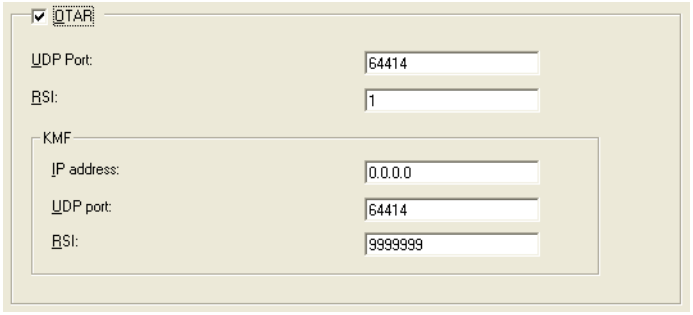
CKR — The CKR to be associated with the key. Enter the CKR of secure key data that has been or will be loaded into the gateway.

Add — Adds a new row to the Keys table.

Delete — Deletes the selected row from the Keys table. This has no effect on the underlying secure key data.

OTAR

The OTAR area enables and configures OTAR communications (key management messages) between the network element and its Key Management Facility. These communications are IP based and use Ethernet, not an RF interface.



OTAR — Select the OTAR check box to enable OTAR communications. If the check box is cleared, encryption keys must be loaded into the network element manually using a key fill device.

UDP port — The UDP port on which the network element listens for OTAR communications.

RSI — The radio set identifier of the network element. This must be the same as the Line ID of the current calling profile. The network element uses the RSI to uniquely identify itself to the KMF.

KMF

The KMF area specifies details about the Key Management Facility that will manage encryption keys in the network element.

IP address — The IP address of the KMF.

UDP port — The port on which the network element will listen for OTAR messages from the KMF.

RSI — The unique identifier of the KMF. The network element will only acknowledge OTAR messages that come from a KMF with this RSI. KMFs are given the default RSI of 9999999. This only needs changing if the KMF has been given a different RSI, for example if a network has more than one KMF.

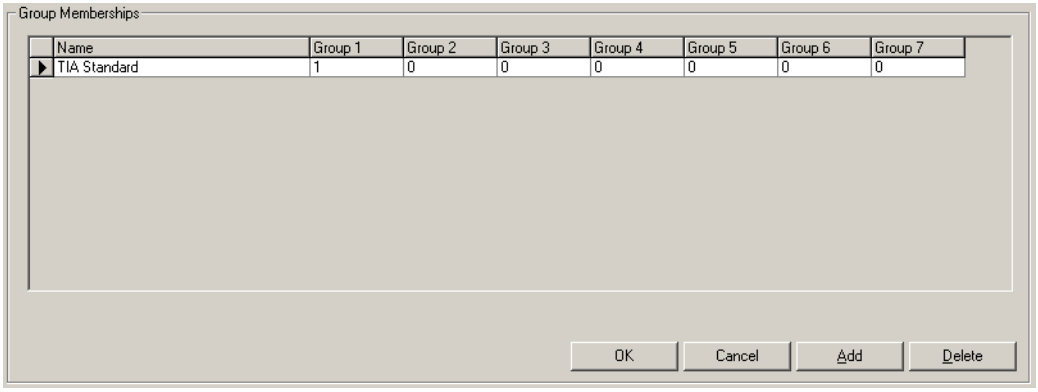
Defining Group Memberships

The Group Membership Table form (Configure > Analog Line > Group Memberships) lists sets of groups. You can add new group memberships or edit existing ones.

If the calling profile specifies selective squelch, the network element only switches digital P25 calls to the analog line if they are to groups that are in the current group membership or to the individual ID specified by the current calling profile. The current calling profile selects the current group membership. The group membership has no effect on the RF interface.

If the calling profile specifies normal squelch, group memberships have no effect.

You can enter up to ten sets of groups, each containing up to seven P25 group IDs.



To add a set of groups

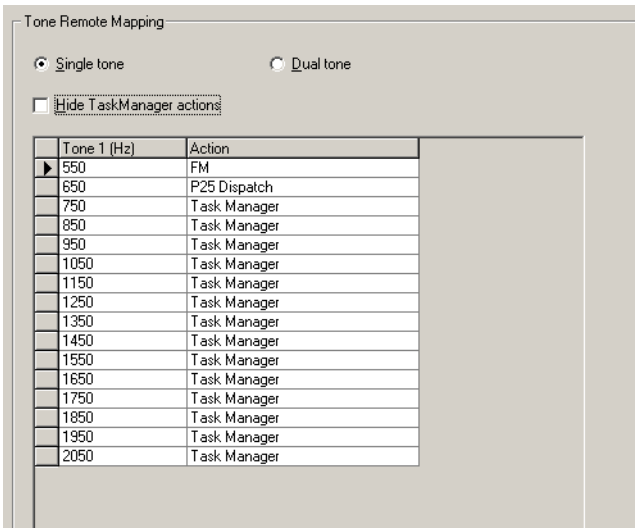
1. Click **Add**. A new row appears in the table.
2. In the **Name** column, enter a suitable name or description for the set of addresses.
3. Enter a P25 group ID into the Group 1 column. These are 4-digit hexadecimal numbers.

If you enter nothing (leave the columns empty), one group is still specified: 65535 (0xFFFF). The network element will always pass calls to the group address 65535 on to the analog line.

4. Repeat for subsequent group columns until you have entered all the groups that the dispatcher needs to listen to.
5. Click **OK** to confirm the changes and close the form.

Mapping Tone Remote Commands

The Tone Remote Mapping form indicates what actions function tones trigger. You can map tone remote function tones to calling profiles or to the Cancel P25 unit call action. Function tones can always trigger Task Manager actions. If you map a tone remote function tone to a calling profile, when the console sends the function tone, the analog line switches to that calling profile. If you want the function tone to do something other than select a calling profile or the Cancel P25 unit call action, create an appropriate Task Manager statement with **Tone remote detected (nnn)** as the input.



To map a function tone to an action

1. Select Configure > Analog Line > Tone Remote Mapping.
2. Select **Single tone** or **Dual tone**, based on the kind of function tones that the console system will produce. This configures the analog line for the detection of single-tone or dual-tone function tones. If you select Single tone, one tone column is displayed. If you select Dual tone, there are two columns.
3. If necessary, clear the **Hide Task Manager actions** check box.
4. In the row displaying the function tone frequency (or combination of frequencies, for dual function tones), click in the **Action** column. An arrow button appears.
5. Click the arrow to drop down a list of the available actions, and select the one you want.
   a. To have the function tone select a calling profile, select that profile. (The drop-down list displays all calling profiles that have been created.)

b. To have the function tone cancel any SU to SU calls in progress, so that the dispatcher can immediately start a call, select 'Cancel P25 unit call.'

   This setting is necessary for trunked analog gateways, because trunked SU-to-SU calls have a hang time; the dispatcher would otherwise need to wait for the call to finish and for the hang timer to expire.

   This setting can also be used for P25 console gateways. It enables the dispatcher to pre-empt an existing individual call. If the current calling profile has autoreply enabled, this option will also override the autoreply, so that the dispatcher calls the configured call destination instead of replying to the sender of the previous call.

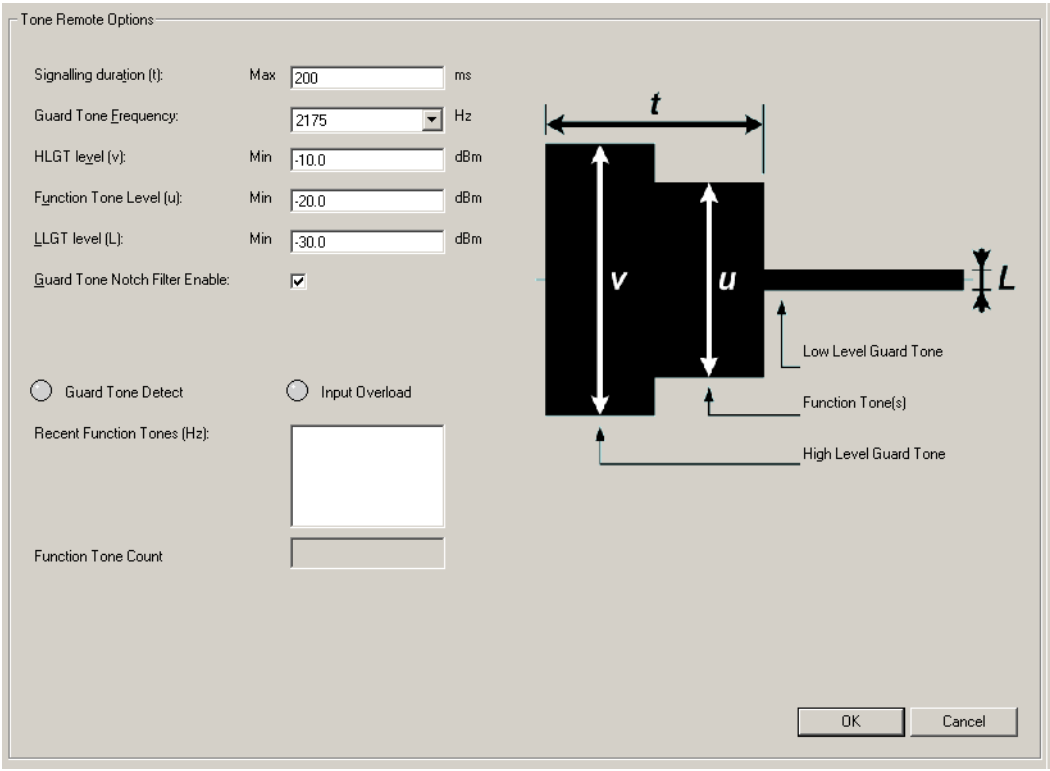
c. Otherwise, leave the function tone with the default setting 'Task Manager.' If there are any Task Manager actions with the function tone as input, the function tone will trigger them. If there are no actions with this function tone as an input, the function tone will have no effect.

6. Click OK to confirm your changes.

Setting Tone Remote Options

Console systems can use a variety of frequencies and levels for the tone remote control of the gateway or base station. In the Tone Remote Options form (Configure > Analog Line > Tone Remote Options), you specify the parameter values that the connected equipment uses. A graph of tone remote signaling shows you visually the meaning of the parameters. Some values can be ascertained from the console system documentation, others may depend on the console system configuration. The console system and the network element must have compatible settings.

The Tone Remote Options form also has some monitoring items. You can use them to confirm that tone remote detection is working properly.



Signaling duration	The maximum time that the analog line will listen for HLGT and function tones. This time begins when the analog line detects HLGT. Any function tones received after this time has elapsed are not detected.
Guard tone frequency	The frequency that the console system uses for the guard tone. HLGT and LLGT use the same frequency. If the console system is going to use MDC1200 with analog FM SUs, this frequency should be well above 2100 Hz, so that the notch filter does not remove significant amounts of energy from the MDC1200 signaling.
HLGT level	HLGT must exceed this minimum level for the network element to detect the tone.
Function tone level	Single tone or dual tone function tones must exceed this minimum level for the network element to detect them.

LLGT level	LLGT must exceed this minimum level and be less than the minimum HLGT level for the network element to detect the tone.
Guard tone notch filter	When this check box is enabled, the network element removes the LLGT from the audio before sending it to the voter. Normally, the notch filter is enabled.

Monitoring Controls

Once the tone remote options are set up, you can confirm that the analog line is correctly detecting and decoding them. Send some tone remote signaling from the console system and check the display of the following monitored items.

Guard tone detect	Displays green when the analog line recognizes HLGT or LLGT.
Input overload	Displays red if the level exceeds the limit that the analog line can handle. If overloads occur, the analog line cannot correctly detect tones.
Recent function tones	Displays the frequencies of the last four function tones detected by the analog line interface. If the analog line detects a function tone, its characteristics lie within the limits of the parameters defined in this Tone Remote Options form.
Function tone count	Displays the number of function tones that have been detected. When you send a number of function tones from the console system, check that the count increments by that number.

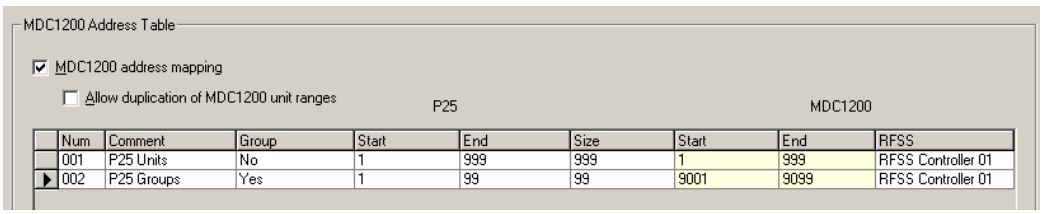
Mapping MDC1200 Addresses

The MDC1200 Address Table (Configure > Analog Line > MDC1200 Address Table) tells the gateway how to convert individual and group numbers from P25 to MDC1200 and vice versa. For example, when the dispatch console calls a group, the gateway converts the destination MDC1200 address to its P25 equivalent, which the channel group uses over the air. Similarly, when a SU calls the dispatcher, the gateway converts the SU's P25 address to the equivalent MDC1200 address, which the dispatch console displays as the caller ID.

If the gateway is a trunked analog gateway, the address table is also used for call validation. Calls cannot be made to or from P25 addresses unless they are within the address ranges defined in this table.

The existing rows in the table can be modified or further rows can be added. The default mappings convert in such a way that the MDC1200 numbers displayed on the dispatch console are highly similar to the equivalent P25 numbers.

By default, check boxes enable the mapping defined in the table below and do not allow overlapping MDC1200 address ranges. These default settings can be altered if required by particular system designs.



	Num	Comment	Group	Start	End	Size	Start	End	RFSS
	001	P25 Units	No	1	999	999	1	999	RFSS Controller 01
▶	002	P25 Groups	Yes	1	99	99	9001	9099	RFSS Controller 01

In the default mappings, the first table row maps P25 individual addresses between 1 and 999 to MDC1200 addresses 0001–0999. The second row maps P25 talkgroup addresses between 1 and 99 to 9001–9099.

The RFSS column is only enabled if you are configuring a trunked analog gateway. This column allows you to assign different address ranges to different RFSS controllers.

The following two check boxes are normally left at their default settings:

MDC1200 address mapping

Clearing this check box disables the mapping of P25 and MDC1200 addresses. This is only supported for trunked analog gateways. It enables defining the full P25 address ranges in the address table, which may be required for call validation. It may also be required, for example, if the dispatch console does not support MDC1200. For outbound calls, the destination address must be defined by a calling profile (Configure > Analog Line > Calling Profiles.)

Allow duplication of MCD1200 unit ranges

Normally, MDC1200 address ranges must be unique, so that a MDC1200 address always corresponds to only one P25 SUID or group ID. Selecting this check box makes it possible for the P25 SUID ranges to overlap. This configuration is only supported for P25 console gateways. For outbound calls, the gateway will convert the MDC1200 address to a P25 address using the first matching MDC1200 address range. For inbound calls, P25 IDs will be converted to the mapped MDC1200 addresses.

Adding an Address Mapping

If there is a need to map additional addresses to the ones already mapped, follow these steps.

1. Select Configure >Analog Line > MDC1200 Address Table.
2. Click **Add**. A new row appears in the table.
3. In the **Comment** column, enter a name or remark to identify the block of addresses.
4. In the **Group** column, select Yes to map P25 group addresses or No to map P25 individual addresses.
5. Under **P25**, enter into the **Start** column the lowest P25 address in the block. Enter into the **End** column the highest address in the block.

   We recommend using group and individual addresses between 1 and 9999. However, valid group addresses are 1-65535 (0xFFFF) and individual addresses 1-16777215 (0xFFFFFF). Generally, you can't include addresses that have already been mapped, but you can re-use addresses from a block of group addresses in a block of individual addresses and vice versa. This is because a P25 group address is not identical to a P25 individual address with the same number; they have different byte sizes.

   The size of the block is calculated and appears in the **Size** column.
6. Under **MDC1200**, enter into the **Start** column the beginning of the equivalent MDC1200 block of addresses. MDC1200 addresses must normally be in the range 1-9999. You can't normally include addresses that have already been mapped. The end of the MDC1200 address range is automatically calculated and appears in the **End** column.

Some analog console systems will not allow Radio Enable/Radio Disable, Radio Check, Radio Monitor or Status Report (Status Request) if the hexadecimal MDC1200 radio address has an E or F in it. For assis-

tance with mapping addresses with this or other similar special requirements, contact Tait.

7. Click **OK** to confirm the changes and close the form.

Tip: To shift a range, edit the address in the P25 or MDC 1200 Start column. To change the size of a range, edit the P25 size or the P25 address in the End column.

SU Numbering Example

The following example shows how a county Sheriff's department could number its SUs.

	P25 Start Address	P25 End Address	MDC1200 Start Address	MDC1200 End Address
Officer handportables	1	99	0001	0099
In-vehicle mobiles	201	299	0201	0299
Talkgroups	1	20	9001	9020

Officer handportables, in-vehicle mobiles, and talkgroups each have their own number range. This example uses the default mapping and results in MDC1200 numbers that are highly similar to the P25 numbers.

Address Mapping for a Trunked Analog Gateway

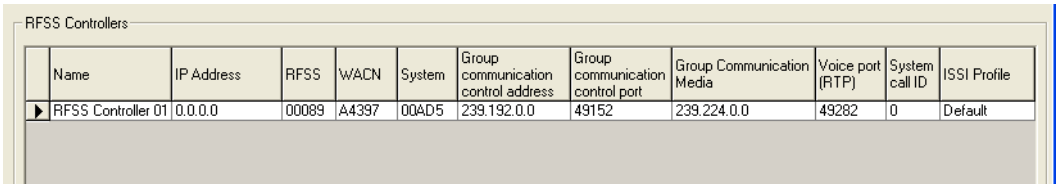
Most trunked analog gateways will only participate in calls to and from groups that are homed at the same RFSS. Individual calls will also only be made to or received from radios belonging to that RFSS. In this case the default address mappings can be used and need to be assigned to the RFSS controller. (The RFSS controller must have been previously defined in Configure > Analog Line > RFSS.)

However, if the dispatcher needs to be able to change back and forth between groups that are homed at different RFSSs, the P25 group address range must be divided up among the RFSS controllers. In this, the gateway configuration will reflect the RFSS controllers' configuration. Each group that the dispatcher can use must belong to an address range that is assigned to the correct RFSS controller. When the dispatcher changes group, the MDC1200 address table tells the gateway which controller is the home RFSS for that group.

If the dispatcher wants to make or receive individual calls to or from radios that belong to different RFSSs, the individual address range needs to be divided up similarly, and assigned to the appropriate RFSS controller.

Declaring RFSS Controllers

In the RFSS Controllers form (Configure > Analog Line > RFSS), you need to tell the trunked analog gateway about the RFSS controllers that it might connect to. It needs details of the home RFSS controllers for all the groups that it is able to belong to. If it only ever belongs to one group, only one RFSS controller needs to be declared.



Enter the parameter values for each RFSS controller. You can obtain most of them by logging in to the TTM as a technical user.

Name	Enter a suitable name for the RFSS controller.
IP Address	The IP address of the RFSS controller.
RFSS	The RFSS ID of the RFSS controller.
WACN	The wide area communications network ID of the RFSS controller.
System	The system ID of the RFSS controller.
Group communication control address	(Privileged RFSSs only) IP address that the gateway uses for sending and receiving group control tree protocol messages.
Group communications control port	(Privileged RFSSs only) UDP port number that the gateway uses for sending and receiving group control tree protocol messages. The gateway must use the same port as the RFSS controller. The RFSS controller uses port 49152 for group communications control messages and TTM users cannot view or change it.
Media base IP address	(Privileged RFSSs only) The base multicast IP address that the gateway uses to compute the multicast address to use with a group call voice stream. The base IP address and a group's WUID are added together to obtain the multicast IP address to use for calls to that group.
Voice port (RTP)	UDP port number that the gateway uses for sending and receiving all voice packets. The gateway must use the same port as the RFSS controller. The RFSS controller uses port 49282 for voice packets.
System call ID	(Privileged RFSSs only) If a group of type 'System' has been created for an RFSS using the TTM, you can enter the number of this group into the system call ID for that RFSS. When the dispatcher calls this number, the gateway will allow extra time for call setup, so that radios in group calls have time to leave their call. A system group includes all radios in that RFSS. They will join in a call to that group unless they are in an emergency call. Other RFSSs are not involved.

The system call ID is additional to 65535, the number reserved by the P25 standards for a system-wide call. The dispatcher can always use 65535 and the gateway will allow extra time for call setup. This system call includes other RFSSs if they are interconnected via ISSI.

ISSI Profile

The ISSI profile assigned to this RFSS controller. When the trunked analog gateway communicates with this RFSS, it uses the settings in this profile. These settings define minor variations in the communications protocols between RFSS controller versions. The default profile uses the settings for the current RFSS controller version.

ISSI Profiles

Select Configure > Analog Line > ISSI to display a list of ISSI profiles. ISSI profiles define minor variations in the communications protocols between RFSS controller versions. When the trunked analog gateway communicates with an RFSS, it uses the settings in the profile assigned to that RFSS controller.

The following table indicates which settings to use with different RFSS controllers.

RFSS Controller Version	Space in status param	Use warn codes 72 and 73	Group call scale hang time
2.04 E26 and above	No	No	Yes
2.04 E20 or before	Yes	Yes	Yes
TN9400 1.1	No	No	No

Group call send delayed bye

If this is set to Yes, after the group call hang time expires, the trunked analog gateway will wait another 300ms for the RFSS to send a SIP BYE-indication before sending its own BYE-indication. If this parameter is set to No, it will silently consider the call to be terminated. Select the option that reflects the way you want the system to operate.

Group call Tx on PTT timeout

This parameter defines the default behavior when the trunked analog gateway does not receive a PTT grant in response to its group-call PTT request. If this is set to Yes, the go-ahead is given for the voice transmission. If it is set to No, the call is denied. Select the option that reflects the way you want the system to operate.

Group call scale hang time

Set this parameter to Yes if the trunked analog gateway is connected to a Airbus DS RFSS controller. This controller advises the group hang time in seconds, whereas other RFSS controllers advise in tenths of seconds.

Part F Alarms

The CSS can monitor the current status of a network element's alarms. Many alarms have thresholds that you can alter to suit the application. Unwanted alarms can be disabled.

You can run multiple instances of the CSS software and use them to simultaneously monitor alarms at several network elements.

To view a list of recent alarms, display the system log (Monitor > Data Logging > System Log).

Topics

Monitoring Alarms

The Status form (Monitor > Alarms > Status) shows the current status of alarms in the base station or gateway. The CSS must be connected to one of these network elements before it can display any alarms.

LED-like icons indicate the status:

- Red (flashing) means that the alarm is active.
- Green means that the monitored condition is OK and that there is no alarm.
- Gray means that the alarm has been disabled or that the monitored condition is not available; for example, Final 2 alarms are gray if there is no Final 2 stage.

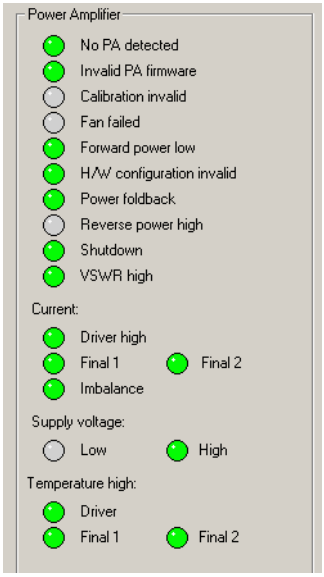
Alarms are triggered when a monitored condition crosses a defined threshold. Some thresholds are fixed and built into the module firmware. Others are configurable in Configure > Alarms > Element Thresholds and Network Thresholds. Some parameters such as high voltage and high reverse power have two thresholds. When the configurable threshold is crossed, the network element generates an alarm. When the built-in threshold is crossed, the network element responds by protecting itself against damage.

If the network element is a gateway, a receive only base station, or does not have a PMU, many alarms will not apply and should be disabled (see "Disabling Unwanted Alarms" on page 208).

Tip: Use Task Manager to configure an automatic response to alarms. In general, each alarm has an equivalent Task Manager input. When the alarm occurs, Task Manager executes any tasks with that alarm as an input.

Power Amplifier

The Power Amplifier area shows the alarm status of the PA associated with the reciter that the CSS is connected to. When a fault is no longer active, any actions (for example, inhibiting transmission) are reversed.



No PA detected

The reciter cannot obtain a response from a PA over the control bus. The PA may still be operating but the system has lost the ability to monitor PA alarms, carry out diagnostics, change configuration, or detect PA fan failure.

1. The reciter has no associated PA. You should disable this alarm.
2. The network element uses a third-party PA which does not use the control bus and cannot respond to the reciter.
3. The control cable or exciter cable is not connected.
4. The PA is faulty and unable to communicate with the exciter.

Invalid PA firmware

The firmware in the PA is invalid.

1. Use the CSS to download the PA firmware.
2. Return the PA to Tait.

Calibration invalid

This alarm can only be triggered on startup, when the PA carries out self-tests. It indicates that settings stored in firmware have values outside acceptable limits. In response, the base station disables the transmitter. Re-calibrate the PA using the Calibration Software or send it to a service center for repair.

Fan failed

The PA told the reciter that its fan is on, but the reciter cannot detect fan motion. The base station takes no action when this alarm occurs, but it will act if the PA temperature becomes too high.

The fan has failed. Replace it.

Forward power low

The PA forward power output is below the configured minimum limit. If the VSWR is also raised, check for a load mismatch. Otherwise, there may be a fault in the output driver(s).

H/w configuration invalid

The PA has an invalid hardware configuration. Either the driver is not present or the configuration says that there is a Final 2 output stage but no Final 1, which is impossible.

Power foldback

The PA has detected a fault condition and has reduced its power output to a minimal level to prevent damage.

Check the other alarms to see what fault condition or conditions have caused this. If the fault condition clears, the PA automatically returns to its previous power output level and the alarm changes to green.

Reverse power high

The PA's reverse power is above the configured maximum. Check for a load mismatch. With a resolution of only 1 W, this alarm is not sensitive if the power output is lower than 20 W. Check the VSWR fault alarm instead.

Shutdown

The PA has detected a fault condition and has disabled the transmitter to prevent damage. Check the other alarms to see what fault condition or conditions have caused this.

VSWR high

The VSWR is above the configured threshold. A normal VSWR is ≤ 2:1. A high VSWR automatically means reduced output power. If the VSWR increases to 10:1 or more, the PA folds back its power output to a minimal level. If the VSWR returns to 5:1 or less, the PA recovers.

Check for a load mismatch on the PA's RF output.

Current

The Current group of alarms detects excessive or inappropriate current draw. If an alarm shows red, the PA needs servicing.

Alarm	Description
Driver high	The driver is drawing excessive current. A fixed limit has been exceeded.
Final 1	The Final 1 output stage is drawing excessive current. A fixed limit has been exceeded.
Final 2	The Final 2 is drawing excessive current. A fixed limit has been exceeded.
Imbalance	One of the final stages is drawing significantly more current than the other.

Supply voltage

The PA can detect whether its power supply voltage is too high or too low.

Supply voltage low

The PA supply voltage is 26 V or less, probably because the battery is running low. The fault condition disappears when the voltage exceeds 26.1 V.

Supply voltage high

The PA supply voltage is 29 V or more.

1. If the PA is obtaining power from a third-party power supply instead of from a PMU, check that the power supply is correctly configured.
2. The PMU is faulty and needs replacing.

The base station is not type-approved for operation when the supply voltage is outside the specified range.

Temperature high This group of alarms shows whether the temperature in the driver, Final 1, or Final 2 output stage has exceeded the user-configurable threshold. As the alarms serve to give early warning of a potential problem, operation continues as normal.

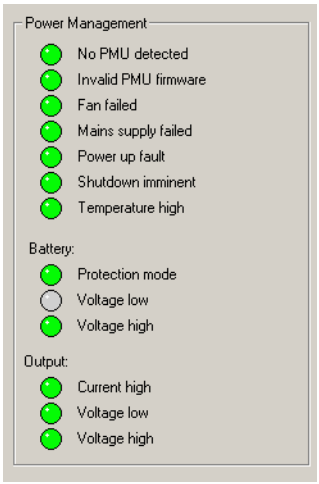
If a PA temperature continues to rise and exceeds its built-in threshold (185 °F/85 °C for the driver or 203 °F/95 °C for the final stage), the PA folds back its power output to 10% of the configured power level (for example, a 50 W PA would produce 5 W).

When the temperature returns to normal (hysteresis is 9 °F/5 °C), the alarm clears.

To see the actual temperatures, select Diagnose > Modules > PA Control Tests.

Power Management Unit

The Power Management Unit area shows the alarm status of the PMU. The CSS must be connected to the channel module in position 1 of the subrack.



No PMU detected The channel module is unable to detect the PMU on the control bus. Only the channel module in position 1 can communicate with the PMU. If the channel module is in position 1, the fault may be in the communication path and the PMU itself is still operating satisfactorily. However, in this case the system loses the ability to monitor PMU alarms, carry out diagnostics, change configuration, or detect PMU fan failure.

Invalid PMU firmware The firmware in the PMU is invalid.

1. Use the CSS to download the PMU firmware.
2. Return the PMU to Tait.

Fan failed The PMU told the channel module that its fan is on, but the channel module cannot detect fan motion. The network element takes no action when this alarm occurs, but it will act if the PMU temperature becomes too high.

The fan has failed. Replace it.

Mains supply failed	The mains power supply to the PMU is absent or its voltage is outside acceptable limits. The PMU is using DC power from its battery source.
Power up fault	The PMU has detected an internal error and will reset itself. If the reset is successful, the alarm will clear.
Shutdown imminent	A battery is currently being used to power the network element and its voltage has fallen below the configured power shutdown voltage. The PMU will stop operating 30 seconds after activating this alarm. The main value of this alarm is to trigger a syslog message or an SNMP trap just before the PMU shuts down.
Temperature high	One of the PMU temperature sensors has detected a temperature that is above the fixed limit.

Battery

The PMU measures the voltage of its battery input.

Battery protection mode	Battery protection mode is on. The network element is operating on mains power, but the battery voltage is below the configured power shutdown voltage. If mains power fails, the PMU will shut down to protect the battery.
Battery voltage low	The battery voltage is below the configured alarm threshold. This threshold may have been set to alert you to the risk of damage to the battery from overdischarge. If the voltage falls further to below the configured shutdown voltage, the PMU automatically shuts down to protect the battery and the modules in the subrack.

When this alarm is triggered, the auxiliary power output shuts down. This can have important effects on the system, depending on what the auxiliary power output is used for.

1. The system has been operating on battery power; the battery has become flat and mains is restored. No action required.
2. The battery is not being charged. Check the PMU's auxiliary output line, if it is being used for charging. Otherwise check the 3rd party charger. Recharge the battery.
3. The battery cannot be adequately charged. Replace it.
4. The minimum battery voltage is set too high.

Battery voltage high	The PMU's battery voltage is higher than the configured maximum. The network element takes no action until the voltage reaches the fixed maximum, when it shuts down.

Output

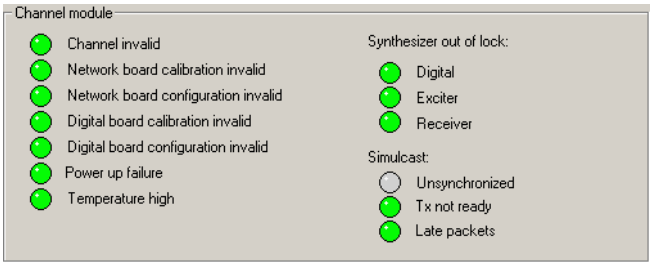
The PMU measures the voltage and the amperage of its DC output to the PA and to the channel module.

Output current high	The PMU is providing more than 15 A of current and is automatically limiting its output, lowering the output voltage. There is a short circuit or the PMU is faulty.

Output voltage low	The PMU's DC output (nominally 28V) is lower than the fixed minimum of 24V.
Output voltage high	The PMU's DC output (nominally 28V) is higher than the fixed maximum of 32V.

Channel Module

The Channel module area shows the Alarm status of the channel module.



Channel invalid

(Rare) The network element has received an instruction to select an invalid channel number and has stopped operating.

The channel could be invalid for one of the following reasons:

1. The current channel definition no longer exists.
2. Task Manager has selected a channel that no longer exists.
3. The channel definition has an invalid index to other information. For example, it specifies channel profile 3 when there is no such profile.
4. There are one or more channel definitions in the channel table that configure mid-band or wide band transmission in a restricted frequency and the network element does not have an Unrestricted Wideband feature license.

Network board calibration invalid

The network element cannot operate properly because the analog line has not been calibrated, or because the calibration procedure has not been properly completed, deleting the old calibration value, but not storing a new value. This alarm is not triggered when the analog line goes out of calibration.

- Use the Calibration Software to calibrate the analog line.

Network board configuration invalid

The configuration data has become corrupted. Open the corresponding configuration file stored on the CSS PC and program it into the network element.

Digital board calibration invalid

The network element cannot operate properly because the digital board does not have valid calibration settings. This could be because a calibration procedure has not been properly completed, deleting the old calibration value, but not storing a new value. This alarm is not triggered when the reciter goes out of calibration.

1. Use the Calibration Software to adjust the frequency setup.
2. Use the Calibration Software to fully calibrate the reciter.
3. Calibrate the reciter TCXO.
4. Replace the reciter.

Digital board configuration invalid

The configuration data has become corrupted. Open the corresponding configuration file stored on the CSS PC and program it into the network element.

Power up failure

The channel module has failed one or more of its initialization self-tests and has gone into Failure mode. The transmitter and receiver are disabled and any system interface outputs are deactivated.

This alarm will not show if the channel module cannot communicate with the CSS.

1. Reset the network element. This may clear the fault.
2. Send the channel module to a Service Center.

Temperature high

The temperature of the reciter has exceeded the built-in threshold of 162.5 °F (72.5 °C). To see more details about the reciter and its fan, select Monitor > Modules > Channel Module.

1. Check to make sure that the PMU and PA fan alarms are off. Failure of these fans could cause a high reciter temperature.
2. The reciter fan has failed and needs replacing.

Synthesizer out of lock

The channel module has three different synthesizer alarms.

Synthesizer out of lock: Digital

One or more of the DSP and sampling clocks is out of lock. In response, the base station disabled the receiver and the transmitter.

1. The base station is configured for an external reference of a particular frequency, but the actual frequency of the external reference is different.
2. The master synthesizer is unable to lock onto the frequency. The base station will run, but the accuracy of its receive and send frequencies cannot be guaranteed. Send the reciter for repair.

Synthesizer out of lock: Exciter

The exciter synthesizer is unable to lock on to the frequency it is configured to operate at. In response, the base station disabled the transmitter.

1. Check that this frequency is within the exciter's RF frequency range.
2. Do a diagnostic test to determine the reciter's switching range, and then check that the frequency is within the exciter's switching range.
3. If the frequency is outside the switching range, use the Calibration Software to alter the switching range. Otherwise send the reciter for repair.

Synthesizer out of lock: Receiver

The receiver synthesizer is unable to lock onto the frequency it is configured to operate at. In response, the base station disabled the receiver.

1. Check that this frequency is within the receiver's RF frequency range.
2. Do a diagnostic test to determine the lock range, and then check that the frequency is within that range.
3. If the frequency is outside the lock range, use the Calibration Software to alter the switching range. Otherwise send the reciter for repair.

Simulcast

The channel module monitors the status of its simulcast operation.

Unsynchronized

The channel module is unsynchronized, for example because it lost its 1 PPS signal and the holdover timer has expired. See Monitor > Synchronization > Simulcast for the reason.

Tx not ready

The base station is not ready to transmit. The exciter is carrying out a training sequence to optimize the frequency deviation. It does this on start-up and when the transmit frequency is changed. This alarm should clear within 20 seconds as the reciter returns to normal operation.

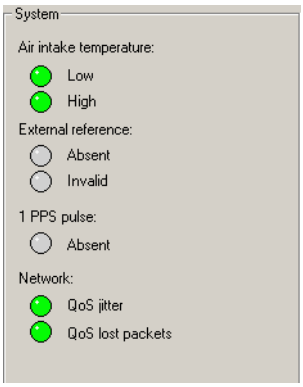
Late packets

The base station is receiving packets for transmission, but they are arriving too late for the transmission to be synchronized.

1. If this occurs only occasionally, there may be a network latency problem.
2. If it occurs frequently, you may need to adjust the transmit timing parameters of the central voter (in the Voting area of the Edit Channel Group dialog box).

System

The System area displays alarms that are triggered by system conditions. These alarms do not indicate network element faults. Set a threshold for these alarms if this is appropriate for the system.



Air intake temperature

The base station is normally fitted with a sensor that measures the air temperature at the PA fan intake and determines whether it is above or below the configured limits.

Air intake temperature low

The temperature is below the configured minimum. The base station is not designed for operation below the default minimum.

Air intake temperature high

The temperature has exceeded the configured maximum. The PA can sustain full-powered continuous operation at an air intake temperature of up to 60 °C. Fan operation and PA power foldback are unaffected by this alarm; it is the heatsink temperature, not the air intake temperature, that turns a base station fan on or folds back PA power.

This alarm may trigger if the air intake temperature threshold is higher than the PA fan control threshold temperature. The heatsink heats the temperature sensor when the fan is not providing a cooling airflow, resulting in an inflated air intake temperature. To prevent spurious alarms, make sure that the fan threshold temperature is 10 °C below the air intake temperature alarm threshold.

External Reference

The base station can detect whether an external reference is present and whether it is usable.

External reference absent

The base station did not detect an external reference frequency source. It is now using its own source.

1. There is no external reference source. Many applications do not need one. You can disable the alarm (Configure > Alarms > Control).
2. The source has become unplugged.
3. The source is not working.

An external reference is critical for simulcast applications and for K-band operation.

External reference invalid

An external reference frequency is connected to the base station, but the base station cannot lock on to its channel frequency using that reference. It is now using its own source.

1. The base station is configured (Configure > Network Element > Miscellaneous) to expect a 10MHz frequency, but the source is 12.8MHz (or vice versa). There are likely to be other, spurious alarms. Disconnect the external reference and use the CSS to program the correct reference frequency.
2. The reference source is faulty.

1PPS pulse

Network elements in a simulcast system must have a 1PPS pulse. This alarm should be disabled for other systems.

Absent

The network element is not receiving a 1PPS pulse. More precisely, the configured threshold for the number of missing 1PPS pulses has been exceeded. If the network element loses its 1PPS pulse but is still receiving its external reference, it phase-locks its transmit clock to the external frequency reference in order to maintain synchronization. This is referred to as holdover mode. When the holdover duration expires, the network element becomes unsynchronized. The Unsynchronized alarm in the Channel module area indicates whether the network element is synchronized.

Network

Most network alarms give early warning that the network is becoming congested.

QoS jitter

The incoming voice stream has a delay variation equal to or greater than the configured threshold (see "Interarrival jitter" on page 212). This alarm can be caused by jitter in the network infrastructure or (more often) by a fade on the RF uplink. The alarm is triggered by delay variation from any source and is not specific to QoS problems in the infrastructure.

QoS lost packets

The number of lost packets in the incoming voice stream has equalled or exceeded one or more of the configured thresholds (see "Loss rate" on page 212 and "Loss per call" on page 212).

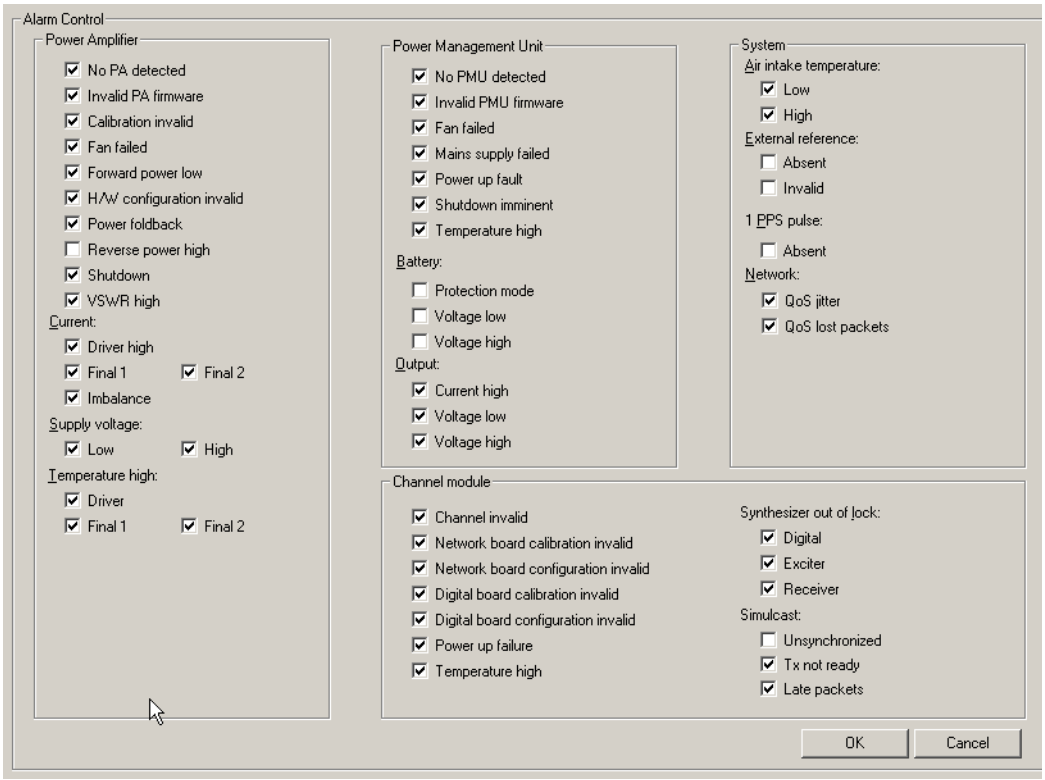
Disabling Unwanted Alarms

You can disable any of the network element's alarms. Some alarms may not be appropriate for the system.

If you disable an alarm, it is disabled in the Alarm status form and in any diagnostics forms where it appears. It also does not turn on the control panel alarm LED or result in a SNMP trap. However, the alarm still generates a syslog message, which the network element stores in its log and optionally sends to a syslog collector. Disabling an alarm disables its syslog message to the level of Notice. In addition, any Task Manager tasks with that alarm as an input are still processed.

If you are configuring a receive-only base station, we recommend disabling the No PA detected alarm.

For detailed information about individual alarms, see "Monitoring Alarms" on page 199.



To disable unwanted alarms

1. Select Configure > Alarms > Control.
2. Clear the check boxes of the alarms to be disabled.
3. Click **OK**.

Configuring the Alarm Display for Gateways

P25 console gateways and P25 trunked analog gateways lack many of the functions of the base station, so many alarms do not apply to them.

1. Disable the No PA detected alarm.

   The gateway module will always trigger this alarm, as there is no PA. None of the other PA alarms apply, but they do not need to be disabled as they will not be triggered.

2. If the gateway does not have a PMU, disable the No PMU detected alarm. If there is a PMU and it cannot be battery powered, disable the battery alarms.

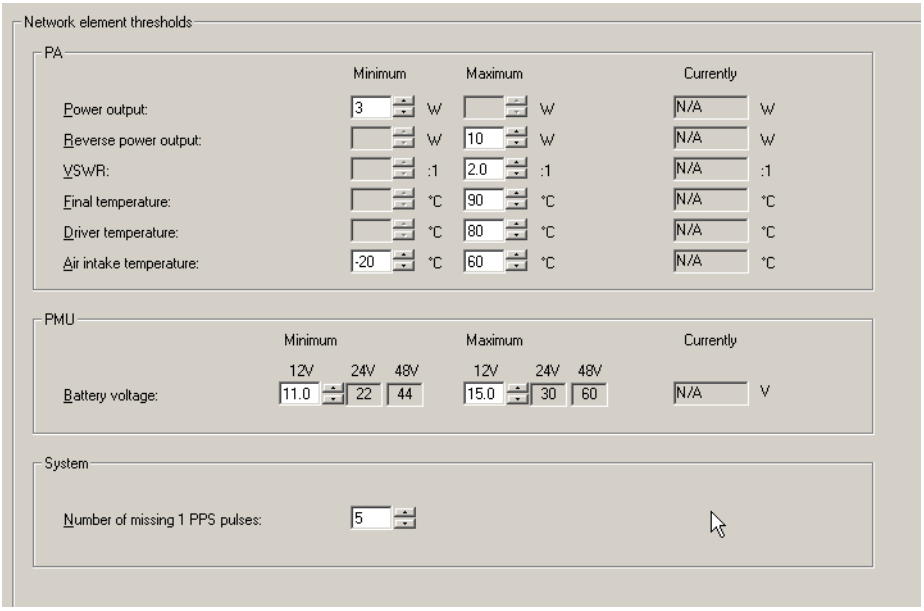
3. Under System, disable the External reference and 1 PPS pulse alarms.

4. Under Channel module, disable the Digital board calibration invalid alarm. The digital board does not need a valid calibration, as the gateway does not have an RF interface. Also disable the Synthesizer out of lock and the Simulcast alarms.

Altering Network Element Alarm Thresholds

The Network Element Thresholds form (Configure > Alarms > Element Thresholds) displays all configurable alarm thresholds.

Some alarm thresholds are fixed; they are built in to the network element and cannot be changed. Others have default values that can be adjusted to better reflect the system's operating conditions or monitoring procedures. This can be important if an alarm is used as an input in Task Manager tasks.



The Minimum column displays lower thresholds. The Maximum column displays upper thresholds. Most parameters have only one threshold. The read-only Currently column displays the current value of the parameter to help you select a suitable threshold.

To adjust a threshold, edit its value or click one of the adjacent arrows, and then click **OK** to confirm the changes and close the form. When the current value of a parameter goes above the maximum or below the minimum, the network element triggers the corresponding alarm. The alarms that these thresholds apply to are described in "Monitoring Alarms" on page 199. The equivalent Task Manager inputs are described in "Alarm Inputs" on page 252.

PA

PA alarm thresholds are stored in the PA itself: the PA must be connected to the reciter when you program them.

Power output

The minimum value defines the lower limit for the PA forward power output. When the output falls below this limit, the base station triggers the alarm Forward power low and the Task Manager input PA forward power low becomes true.

Reverse power output

The maximum value defines the upper limit for the PA's reverse power. When the reverse power exceeds this limit, the base station triggers the alarm Reverse power high and the Task Manager input Reverse power high becomes true.

When using a 5 W PA, or any PA set to 20 W or less, disable this alarm and use the VSWR alarm instead. The resolution of the reverse power measurement is only 1 W, so the reverse power alarm would only trigger if there is a serious antenna fault. VSWR has a better precision and reliably detects load failure.

VSWR

The Maximum column defines the upper limit for the VSWR. When the VSWR exceeds this limit, the base station triggers the alarm VSWR high and the Task Manager input VSWR fault becomes true. The hysteresis is fixed at 0.2. For example, if the threshold is 1.5:1, when the VSWR falls to 1.3:1, the alarm is cleared and the Task Manager input becomes false.

Final temperature

The Maximum column defines the upper limit for the operating temperature at the Final 1 and Final 2 stages of the PA. When the temperature exceeds this limit, the base station triggers one of the Temperature high alarms and the Task Manager input PA temperature high becomes true.

Driver temperature

The Maximum column defines the upper limit for the operating temperature at the driver stage of the PA. When the temperature exceeds this limit, the base station triggers one of the Temperature high alarms and the Task Manager input PA temperature high becomes true.

Air intake temperature

The Maximum column defines the upper limit for the air intake temperature that is measured at the PA. When the temperature exceeds this limit, the base station triggers the Air intake temperature high alarm and the Task Manager input PA air intake temperature high becomes true.

The Minimum column defines the lower limit for the air intake temperature that is measured at the PA. When the temperature falls below this limit, the base station triggers the Air intake temperature low alarm and the Task Manager input PA air intake temperature low becomes true.

PMU

PMU alarm thresholds are stored in the PMU itself: the PMU must be connected to the reciter or gateway module when you program them.

Battery voltage

The Minimum column defines the lower limit for the battery voltage that is supplied to the DC-DC converter. Different limits apply, depending on which nominal voltage the DC-DC converter is designed for. When the voltage falls below the relevant limit, the network element triggers the Battery voltage low alarm and the Task Manager input Battery voltage low becomes true.

The Maximum column defines the upper limit for the battery voltage that is supplied to the DC-DC converter. Different limits apply, depending on which nominal voltage the DC-DC converter is designed for. When the voltage exceeds the relevant limit, the network element triggers the Battery voltage high alarm and the Task Manager input Battery voltage high becomes true.

Both the upper and lower limits have a hysteresis of 0.1 V.

System

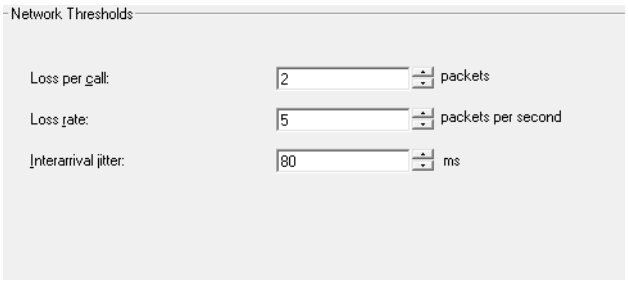
Number of missing 1 PPS pulses

Defines the number of 1 PPS pulses that must fail to arrive at the reciter of a simulcast base station before triggering the 1 PPS pulse absent alarm. Adjust this value to avoid false triggering of the alarm when packets are occasionally not sent or lost, while not unduly delaying the alarm in cases of genuine failure.

Altering Network Alarm Thresholds

The Network Thresholds form (Configure > Alarms > Network Thresholds) displays thresholds that are mostly for measures of the quality of service of the network link to other channel group members. Generally, you can leave defaults as they are. When a threshold is reached, an alarm condition results. The aim of adjusting them is to ensure that alarms trigger before the quality of service deteriorates under network load, giving some advance warning.

Tip: Select Monitor > Interfaces > Channel Group to view current values for quality of service measures. These can help in the setting of appropriate thresholds.



Loss per call

Number of packets lost in one voice over that will trigger an alarm. This threshold is designed for detecting a sudden acute loss of service. The network element calculates the packets lost from a jump in the sequence number from one packet to the next. If the selected number of packets or more are lost, the network element raises the QoS lost packets alarm.

Generally, you can leave this threshold at the default; good network links should not lose packets at all. If network links are heavily loaded, you may want to increase the threshold. A loss of 50 packets roughly corresponds to a gap of one second.

Loss rate

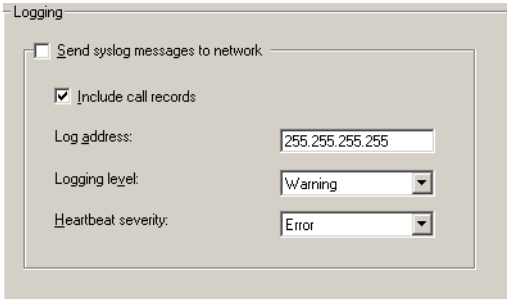
The number of packets lost per RTCP interval (one second). If this threshold is reached, the network element raises the QoS lost packets alarm. The loss rate is designed for detecting a longer-term chronic degradation in quality of service.

Interarrival jitter

The allowable jitter for packets arriving at the network interface. The jitter is calculated for each over and if it reaches this threshold, the network element raises the QoS jitter alarm.

Logging to a Syslog Collector

You can use the Logging form (Configure > Alarms > Logging) to enable and configure the sending of some or all system log messages to a central syslog collector. Messages are sent in the syslog format.



Send syslog messages to network

Select this check box to have the network element send its log messages over the digital line.

Syslog messages can cause voice drop-outs. A switched network does not have QoS and so cannot give voice packets priority. If the network element's logging level is low (Notice or Trace), syslog messages may combine with voice to exceed the available bandwidth, causing voice drop-outs. See the System Manual for guidance on bandwidth allocation and syslog bandwidth requirements.

Include call records

Clear this check box if you do not want call records sent to the syslog collector. This is generally done in trunked networks as call records are provided by the site controller. Call records are still stored in the network element and can be downloaded, viewed, and saved using the CSS.

Log address

Enter the IP address of a host running syslog collector software. Use dotted decimal notation. The network element will send its log messages to this address.

Logging Level

Select the lowest level of messages to be sent to the log address. All messages at or above this level will be sent. This setting does not affect call records. The different syslog message levels are as follows:

Level	Description
Emergency	Alarm conditions that make the network element unusable.
Alert	Alarm conditions that require immediate action to prevent failure.
Critical	Alarm conditions that indicate a trend towards failure, for example, high temperature.
Error	Alarm conditions that indicate an error within the network element's interfaces.
Warning	Events that do not affect behavior, but that may be of significance to operators or maintainers.
Notice	Events that may be helpful to operators or maintainers.
Trace	Tait-internal messages.

Select 'Warning' to minimize the loading on the linking infrastructure. The network element only sends messages if there is a problem.

Select 'Notice' to make sure that you do not lose the system log. All system log messages are sent to the syslog collector. If the network element resets, its system log is cleared, but the syslog collector still has its log of messages.

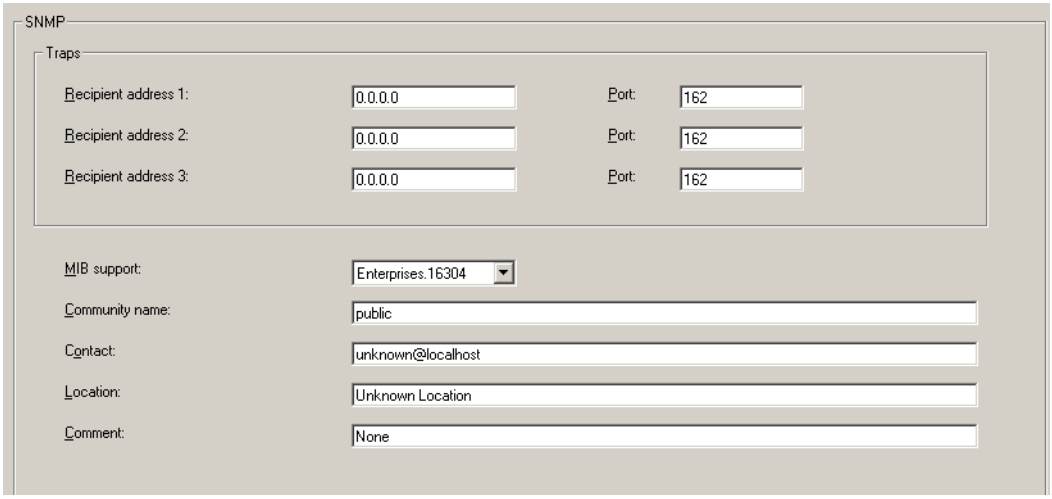
Select 'Trace' to provide the syslog collector with the maximum detail possible. This is not normally needed.

Heartbeat severity

Select a severity level for the heartbeat message. Make sure that you select a level that is not lower than the logging level, otherwise heartbeat messages will not be sent. The syslog collector can be set up to raise the alarm when it ceases to receive the heartbeat because a network element has failed.

Configuring the SNMP Agent

Use the SNMP form (Configure > Alarms > SNMP) to configure the operation of the SNMP agent within the base station or gateway. This is only needed if the network has an SNMP-based network management system. An SNMP (external trunking) feature license is required.



Traps

The Traps area allows you to specify the network identity of up to three different SNMP-based network management systems.

Recipient address — The IP address of the network management system to which SNMP traps are sent. If all boxes are left at the default of 0.0.0.0, no SNMP messages are sent.

Port number — The port number that SNMP messages are sent to.

MIB support — Indicates which MIB the SNMP agent will use.

Option	Description
Enterprises.3570	Choose this MIB if your network is a TN9400 trunked network or has a Tait Enable network management system.
Enterprises.16304	Choose this MIB if your network uses Airbus DS trunking controllers and the What'sUp Gold network management system. (If the network uses Airbus DS controllers but you have your own network management system, the Enterprises.3570 MIB is to be preferred.)

The MIB you choose must be provided to the network management system.

Community name — The community name that must be included in SNMP get requests. The base station's SNMP agent will only accept SNMP messages that have this community name.

Contact	Standard MIB-II data item that will be returned on a GET request for the OID 'SysContact.' You can specify the person to be contacted when a SNMP trap occurs.
Location	Standard MIB-II data item that will be returned on a GET request for the OID 'SysLocation.' You can specify the location of the network element.

Part G Diagnosing

Using the CSS, you can carry out diagnostic tests on the base station or gateway and its modules. For many tests, the network element must be in Standby mode. However, you can view any diagnostic form in Run mode.

Generally a diagnostic form displays relevant information, so that you can monitor network element status before, during, and after the test. Often you can combine different tests.

Some diagnostic tests check aspects of the network element. Others provide a simple function (for example, looping back the analog line) that facilitates setting up or trouble-shooting the network element's interface to external equipment.

Topics

RF Interface

Line Interfaces

Modules

Carrying Out Diagnostic Tests

Most diagnostic tests are carried out in a similar way. The following gives general instructions on how to do it.

When you start a test, the network element uses its existing settings such as frequency and level, unless you entered different values. When a test comes to an end or is stopped, the network element always returns to the configuration it was in before the test began. For example, after making a test transmission at a manually selected frequency, the network element reverts to the frequency it was previously configured for.

Some tests can only be carried out when the network element is in Standby mode. Colors in the square alongside the Start test button indicate the supported modes: yellow means Standby mode and green means Run mode. Hover the mouse over the square and a tooltip specifies the supported modes.

To carry out a diagnostic test

1. Connect to the network element. You can be remotely connected, but you do need to be on site to test the control panel and the speaker.
2. Click **Diagnose**.
3. In the navigation pane, select an item. The corresponding form appears.
4. In the form, check the network element's current status.
5. If the rectangle alongside the **Start Test** button is yellow and gray, click **Standby** on the toolbar.
6. Click **Start Test**.

   This either carries out the test or it enables other buttons on the form so that you can carry out a test. The item in the navigation pane turns red and the Start Test button changes to Stop Test.

   During the test, the network element will respond to any faults that occur (if, for example, the PA overheats, it will fold the power back) but there will be no alarm notification, because Task Manager is not active in Standby mode.
7. If desired, navigate to other forms to view monitoring screens or check the network element's configuration. Some tests also allow you to simultaneously carry out other tests.
8. If necessary, click **Stop Test** to end the test (some tests end automatically). Selecting Run mode or disconnecting the CSS also ends the test.

RF Interface

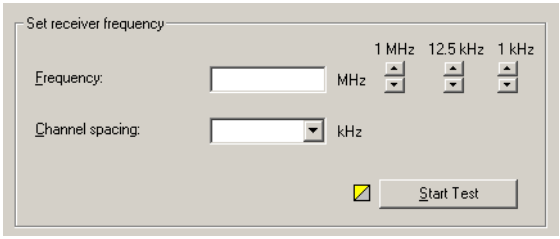
The CSS can carry out a variety of tests on the connected base station's RF interface. You can receive on any frequency and bandwidth, scan the switching range and display the signal strength, test synthesizer lock ranges, and transmit carrier, FM, or C4FM.

Receiver Tests

In the Receiver form (Diagnose > RF Interface > Receiver) you can carry out various tests on the TB9100 receiver.

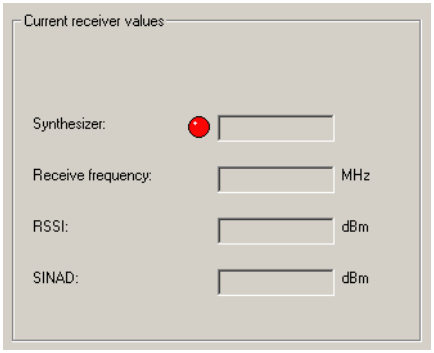
Testing Receiver Operation

The Set receiver frequency test provides a quick way to check that the receiver is operating. You manually set the receiver frequency and do not need to alter the base station's configuration. The test can be carried out on analog FM or digital P25 transmissions.



1. Connect an RF source to the reciter or arrange for a suitable SU to transmit a signal.
2. Select Diagnose > RF Interface > Receiver. In the **Frequency** box, enter the frequency for receiving on. Alternatively, use the arrow buttons to shift the frequency up or down.
3. In the **Channel Spacing** box, select a value from the drop-down list.
4. On the toolbar, click Standby.
5. Click **Start Test**.

   The Current receiver values area displays information about the received signal.



The Synthesizer LED indicates whether the receiver synthesizer managed to lock onto the frequency. The Receive frequency box displays the receiver's current operating frequency. The current RSSI and SINAD are also displayed.

The SINAD is approximate and is obtained by measuring the out-of-band noise. This value should not be relied upon to make calibrated measurements.

The speaker may not give any indication that a signal has been received.

6. If desired, modify the receive frequency by clicking the up or down arrows. (You can repeat this as often as you want.)

   The Stop Test button turns into a disabled Starting Test button until the new frequency has been tested. The form now displays the new values.

7. Click **Stop Test** when you are finished.

Testing Receiver Sensitivity

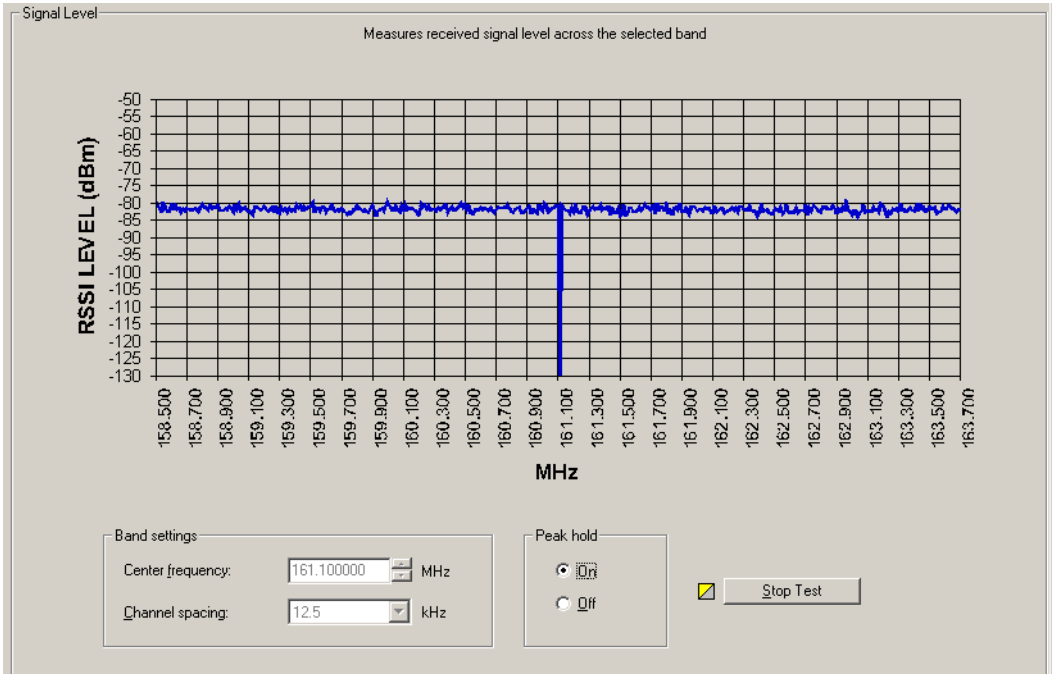
You can carry out a basic test of the receiver's sensitivity without using test equipment. The test only works if a 50 ohm load is connected to the receiver's RF input and no RF signal is being received. You can set this up by connecting up a test set and switching its RF off.

1. Disconnect the receive antenna and connect a 50 ohm load.
2. Select Diagnose > RF Interface > Receiver.
3. On the toolbar, click Standby.
4. Click **Start Test**. The box alongside indicates whether the receiver passed or failed the test. The test is carried out at the frequency and channel spacing defined by the current channel.

   If the test result is 'fail' and the receiver was not receiving any RF, the receiver front end is not properly tuned and/or the RSSI calibration is inaccurate. Use the calibration software to tune the receiver front end and re-calibrate the RSSI.

Measuring Received Signal Levels

You can measure the strength of RF signal that the base station receives across a band of frequencies. A bar graph displays the results.



This test indicates what signals are out there; it does not determine the receiver's sensitivity.

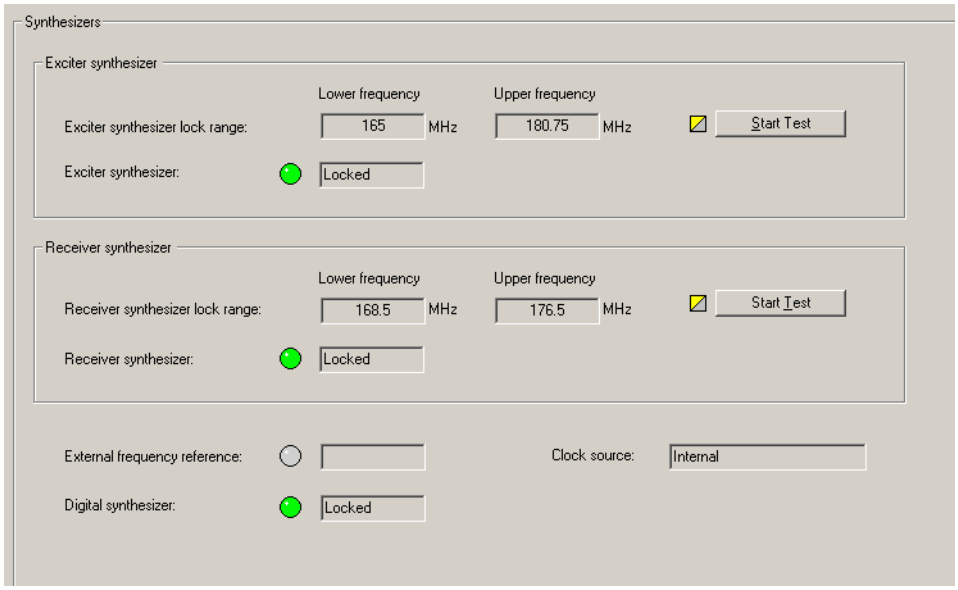
To measure signal levels

1. Select Diagnose > RF Interface > Signal Level.
2. In the **Center frequency** box, specify the middle frequency of the band to be tested. This can be any frequency within the receiver's switching range.
3. In the **Channel spacing** box, select a value from the drop-down list. This specifies the size of the step from one frequency to the next. If this corresponds to the channel spacing, the test will measure the signal levels of the different channels in the band.
4. Under **Peak hold**, select On and the display will show the strongest signal received on any pass. This means signals from infrequent users are more likely to be included. Select Off and the display will only show the results of the most recent pass.
5. On the toolbar, click **Standby**.
6. Click **Start Test**. The base station sets the receiver to a frequency, measures the RSSI, increments the frequency by the value in the Channel spacing box, measures its RSSI and so on for 101 steps below and above the specified center frequency. Once it has completed a pass over all 101 frequencies, it begins the next pass. You can leave the test running as long as you wish.
7. Click **End Test** to stop the test.

   The graph displays the measured RSSI values and annotates the x-axis with the correct frequency values.

Determining Synthesizer Lock Ranges

You can test the reciter's synthesizers to determine the range of frequencies that the receiver and the exciter can operate on. Use these tests to check that the reciter is calibrated correctly for the channels that it will operate on.



LEDs indicate whether the synthesizers were locked. The **Clock source** box indicates whether the reference frequency is internal or external to the base station.

To test the exciter or receiver lock range

1. Select Diagnose > RF Interface > Synthesizers.
2. On the toolbar, click Standby.
3. Click **Start Test** in the Exciter synthesizer or Receiver synthesizer area.

   The exciter or receiver checks all the channel frequencies in the band that the base station is type-approved to operate in.
4. In the **Lower Frequency** and **Upper Frequency** boxes, view the results of the test. These values report the range within which the synthesizer is able to lock onto the specified frequency.

The reported ranges are conservative. In fact, the base station will be able to transmit and receive outside the range, but with reduced transmit output and receive sensitivity.

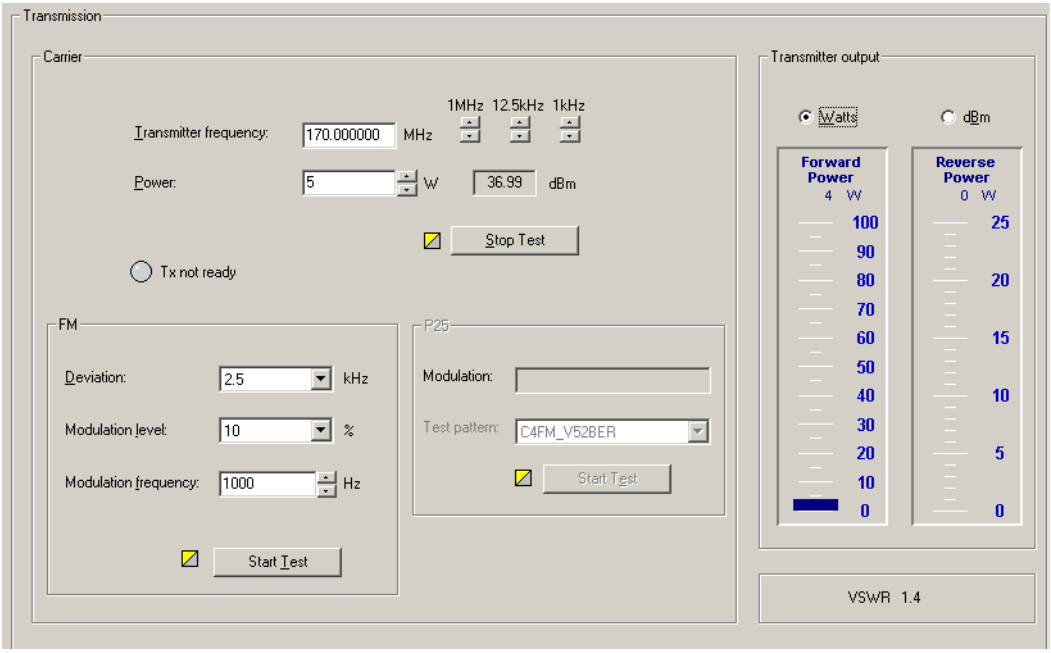
K-band base stations have two exciter synthesizers, each covering a different band. The diagnostic test will show the range of one synthesizer **but the exciter will also be able to operate on frequencies within the range of the other synthesizer.** When the reciter was last calibrated, the synthesizer to be displayed was chosen.

5. Click **Stop Test**. The exciter and receiver frequencies revert to what they were before the start of the test.

Transmission Tests

In the Transmission form (Diagnose > Power Amplifier > Transmission) you can set up and start a carrier-only test transmission. If desired, you can modulate the carrier by starting a FM test or a C4FM test while this carrier test is running.

Tip: Alternatively, test the transmitter by pressing the Carrier button on the control panel. This transmits using the current configuration.



Carrier	The Carrier area initially displays values from the current channel configuration. You can configure and start a test transmission.
Tx not ready	If the Tx not ready LED is red, the transmitter is not ready to transmit. It is training its VCXO to optimize the frequency deviation. The LED should turn green within 20 seconds and the transmitter should begin transmitting.
Transmitter output	The Transmitter output area displays forward and reverse power gauges. You can choose whether to view the values as watts or dBm. Underneath is the VSWR.
FM	In the FM area, you can configure and start analog FM modulation, once a Carrier test is running.

If the current channel profile disables the transmitter (see "Transmitter" on page 137), you can still carry out a carrier test and a FM test.

P25	Once a Carrier test is running, you can use the P25 area to select a digital test pattern and start modulating the carrier with it, using the configured modulation scheme.

If the current channel profile disables the transmitter (see "Transmitter" on page 137), you cannot carry out a P25 test.

Carrier Test

To test the base station's ability to transmit carrier, follow these steps.

1. Select Diagnose > RF Interface > Transmission Tests.
2. In the **Transmitter frequency** box, enter a frequency or use the arrows to increment or decrement the current frequency.

Do not select a prohibited frequency. For example, 406.0-406.100 MHz is reserved internationally for distress beacons.

3. In the **Power** box, specify the RF output power that the test will run at. The box to the right displays the equivalent power in dBm.

Check the transmit frequency and RF power output before beginning the test. In the TB9100, the transmission test does not default to the currently configured frequency and power. Make sure you do not inadvertently transmit on someone else's frequency.

4. Wait until the base station is not busy, to avoid interrupting a conversation, go to Standby mode, and then click **Start Test**.

   The PA outputs an RF signal on the RF Out N-connector. The **Transmitter output** area provides a graphical display of the forward and reverse power and the VSWR.

Tip: To check for intermodulation, simultaneously run a test to measure received signal levels across the band (Diagnose > RF Interface > Signal Level).

5. If desired, modulate the carrier using FM (see "FM Test" on page 224) or C4FM (see "P25 Test" on page 225).
6. Click **Stop Test** at any time to end the test.

FM Test

To test the base station's ability to transmit carrier modulated with analog FM, run a Carrier test, and then start an FM test to add analog FM modulation to the carrier. Follow these steps.

1. Under **Carrier**, start a Carrier test (see "Carrier Test" on page 224).
2. Under **FM**, configure FM modulation as follows.
   a. In the **Deviation** box, select a maximum transmit deviation.

If you select a deviation of 4 of 5 kHz (mid-band or wide band) for a transmit frequency in the 150-174 MHz or 421-470 MHz frequency bands and the base station does not have an Unrestricted Wideband feature license, it will not transmit.

If you attempt to start a transmission test after trying to transmit with a prohibited FM test configuration, the transmitter will not transmit. This is because the base station remembers the transmit test configuration as a whole (even though the CSS does not display it). Even if you request a carrier only transmission, the base station will attempt to carry out an FM test with the remembered configuration, and fail. To successfully carry out any transmit test, first run another FM test using narrowband deviation. You can now transmit carrier and then modify it in any permitted way.

   b. In the **Modulation level** box, specify what percentage of the maximum deviation the test tone will have.

   c. In the **Modulation frequency** box, specify the frequency of the tone that will modulate the test signal.

3. Under **FM**, click **Start Test**.

P25 Test

To have the base station transmit digitally modulated carrier, run a Carrier test, and then start a P25 test to modulate the carrier with a standard digital pattern. This pattern contains the default NAC.

This test can be used to verify the base station's modulation fidelity or for coverage mapping of a single transmitter (Tait SUs receiving this digital pattern can compute and display the BER as they move through the coverage area).

Follow these steps.

1. Prepare for the test by modifying the base station configuration. Unmodified configurations result in residual BER measurements.

   a. Make sure that status symbols are set correctly (in the current channel profile, General tab, set Status symbols to Channel).

   b. Set the number of microslots/slot to 1 (current channel profile, General tab).

2. Under **Carrier**, start a Carrier test (see "Carrier Test" on page 224).
3. Under **P25**, click **Conformance1011Hz** in the **Test pattern** box. This defines a fixed pattern of bits which are transmitted using the configured digital modulation type (for example, C4FM) and which result in a test tone of 1011 Hz at the receiver vocoder. The receiving radio must be configured for the default NAC (0x293).
4. Under **P25**, click **Start Test**.
5. When the test is completed, under P25, click Stop Test and then under Carrier, click Stop Test.
6. Revert the configuration to its previous settings.

Conformance Tests

To make test transmissions in order to test the base station's transmitter or another receiver for conformance to the P25 standard, follow the instructions for a P25 test ("P25 Test" on page 225), but select a different test pattern. The results obtained can be compared with the results on the factory test sheet.

The following test patterns are available:

Option	Description
V52BER	A standard transmitter test pattern used to check a receiver's BER.
ModulationFidelity	Standard Transmitter C4FM Modulation Fidelity Pattern. The transmitter output is sent directly to test equipment to check the accuracy of the base station's radio modem.
ConformanceSilence	Standard Silence Test Pattern. Used for testing a receiver. When this pattern is decoded, there should be no sound from the receiver.
Conformance1011Hz	Standard Tone Test Pattern. Presents a 1011Hz tone at the receiver vocoder. The default NAC is embedded in the test pattern so the receiver must be configured with this NAC.
StdDeviation	Transmits the dibits 11 and 01. The test is used to measure the bandwidth used when transmitting the dibits with the greatest frequency offset.
LowDeviation	Transmits the dibits 10 and 00. The test is used to measure the bandwidth used when transmitting the dibits with the least frequency offset. With this test pattern, a standard frequency counter can be used to measure the frequency of the transmitter's carrier.
SerialInput	Transmits the bit pattern received on the serial input.

For more details about these tests, see the Project 25 standards document TIA-102.CAAA-A.

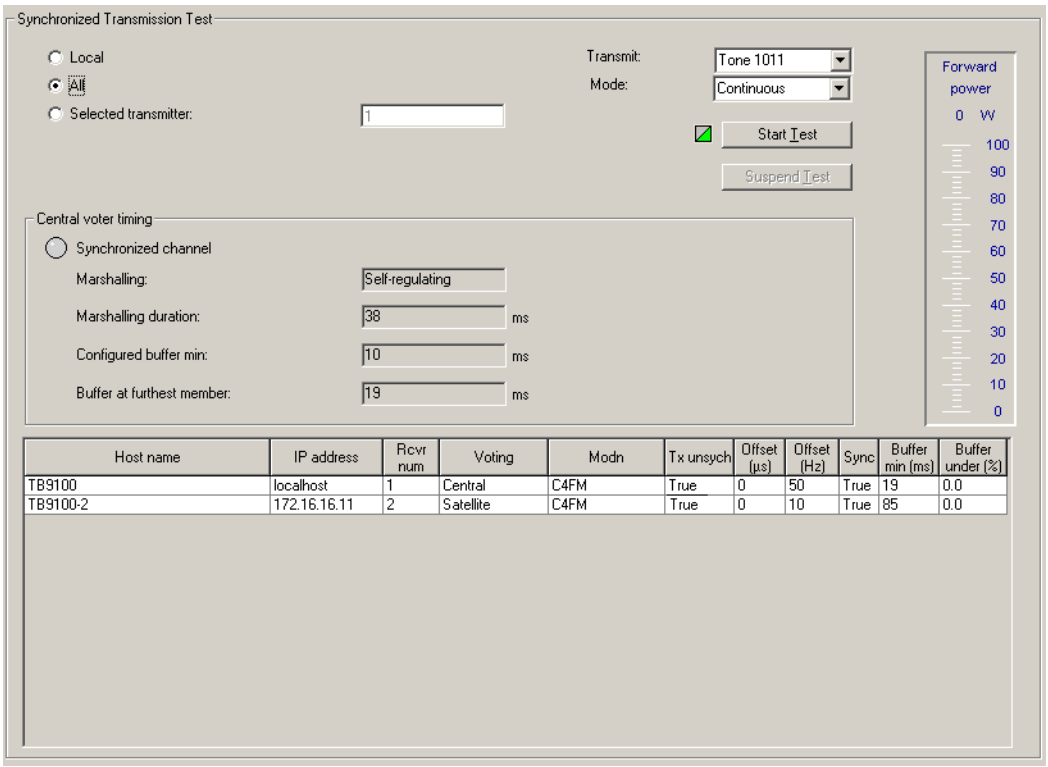
Providing Raw C4FM Data

In the Miscellaneous form, you can tell the base station to start providing output from the receiver as raw C4FM data.

1. Make sure that the current channel profile selects C4FM modulation.
2. Select Diagnose > RF Interface > Log C4FM.
3. In the Log box, specify whether the data is sent to a syslog collector (at severity level Trace) or to the serial port. The serial port baud rate is set to 19,200 for the duration of the logging, overriding the configured setting.
4. Click **Start log**.

Synchronized Transmission Test

Using the Synchronized Transmission Test form (Diagnose > RF Interface > Synchronized Transmit), you can test the simulcast operation of the channel group or of particular transmitters within it. In contrast to other TB9100 transmission tests, the synchronized transmission test can only be carried out in Run mode. You can also suspend the test, reverting to normal operation, and resume it when appropriate.



This test is useful during installation and commissioning for coverage verification by measuring the BER (or MER, for trunking control channels) at various points within the channel's coverage area.

The form monitors simulcast operation even when a test has not been initiated and is useful for checking the configured launch time offsets of channel group members.

When using this test to map channel group coverage, make sure that transmit buffer levels are high enough to ensure that network jitter does not result in buffer underflows. These will corrupt the transmitted signal. You may need to increase the minimum buffer level (Buffer min parameter) or marshalling duration defined in the central voter.

Carrying Out the Test

1. If carrying out a BER or MER test, prepare for the test by modifying the configuration of all base stations that will transmit during the test. Unmodified configurations result in residual BER measurements.
   a. Save to files the current configurations of all base stations that will participate in the test.
   b. Make sure that status symbols are set to indicate the state of the channel (current channel profile, General tab)

c. Set the number of microslots/slot to 1 (current channel profile, General tab)

d. Set the Transmit NAC to the default (0x293) (current signaling profile)

2. Connect to the central voter of the channel group.
3. Specify the scope of the test.
   - Select **Local** to test only the connected member.
   - Select **All** to test the whole channel group.

Tip: You can involve various combinations of members in the test. To exclude a member from the test, put it in Standby mode.

   - Select **Selected transmitter** and enter that member's receiver number in order to test only that member.
4. In the **Transmit** list, click **Tone 1011** for a 1011 Hz test tone or **Speech** for pre-recorded voice.
5. In the **Mode** list, click **Continuous** for continuous transmission or **Individual overs** for a series of regular calls.
6. Click **Start Test**. (Do not first go into Standby mode.) During the test, the network element you are connected to generates the signal for transmission. All base stations in the channel group that are in Run mode transmit the signal.
7. Monitor the displayed data. The Forward power gauge indicates whether the base station you are connected to is transmitting. The Central voter timing area only displays information if you are connected to the central voter (see "Monitoring Central Voter Timing" on page 229). The table at the bottom of the form displays information about the members of the channel group (see "Monitoring Channel Group Synchronization" on page 229).
8. If desired, click **Suspend** to suspend the test.

   The test ceases generating a signal but the network element continues to be in Run mode (is operating normally and is able to handle SU calls as if there was no diagnostic test running). While the test is suspended, you can disconnect the CSS.

Tip: Disconnecting the CSS does not affect the test. This allows you to leave the site to carry out measurements in the field.

9. Re-connect the CSS and click **Resume** to undo the suspension and resume the test.
10. When you are ready, click **Stop Test** to stop the test.
11. Restore the configurations of the channel group members to their previous states by programming the saved configurations back into them (see step 1). This returns the members to normal operation.

Remotely Controlling the Test

The synchronized transmit test can be remotely suspended by making a radio call using a pre-defined NAC. This may be useful in the following situations:

- You are the only person carrying out coverage tests.

- The network is being installed and the linking infrastructure is not yet in place. After setting up the test, you can suspend and resume it without needing to visit the site.

With more complex Task Manager programming, you could send pre-defined NACs to include or exclude individual transmitters from the test.

To remotely control the synchronized transmit test

1. Set up Task Manager programming (see "Sync Tx Test Actions" on page 270) and configure your radio with channels that use the desired NACs.
2. Start the test and then disconnect the CSS. The network element continues in Run mode.
3. Go into the field to carry out tests. Use your radio as needed to send the NACs that suspend and resume the test.
4. When you are finished, use the CSS to re-connect to the network element and stop the test.

Monitoring Central Voter Timing

If you are connected to the central voter during the synchronized transmission test, the Central voter timing area displays information relevant to the synchronization of the central voter. The area displays information whether or not you have started the test. For details about the information displayed, see "Central Voter Timing" on page 101.

Monitoring Channel Group Synchronization

The Synchronization Transmission Test form displays a table with a row of information about synchronization for each of the members of the channel group. If a test is in progress, only those members involved in the test are displayed.

Host name	The name of the channel group member.
IP address	The IP address of the channel group member.
Rcvr num	Displays the receiver number of the channel group member. Voice streams from members with a lower receiver number win the vote (or are selected) when other things are equal. Make sure that each channel group member has a unique number.
Voting	The type of voting taking place at each channel group member. One member should display 'central voter,' the others should display 'satellite' or 'Backup central.'
Modn	Indicates the current modulation scheme that the transmitter is using.
Tx unsynch	Indicates whether the base station is configured to transmit when it or the central voter is unsynchronized or the voice stream arrives late.
Offset (µs)	The configured local transmit offset in microseconds. A value of 1 microsecond means that the transmitter delays transmitting for 1 microsecond after the launch time provided by the central voter.

Offset (Hz)

The configured carrier offset in Hz. This adds a number of Hz to the transmit frequency.

Sync

Displays the synchronization status of the transmitter.

Display	Description
True	Simulcast is enabled and the transmitter is synchronized
False	The transmitter is not synchronized

Buffer min (ms)

Displays the lowest buffer size over the current or most recent voice over. If negative values are displayed, increase the central voter's Buffer min value (self-regulating marshalling), or marshalling duration (fixed marshalling).

Buffer under%

The percentage of packets during the last 15 minutes that arrived late enough to cause a buffer underflow. If this value is too high, increase the central voter's Buffer min value (self-regulating marshalling), or marshalling duration (fixed marshalling).

Line Interfaces

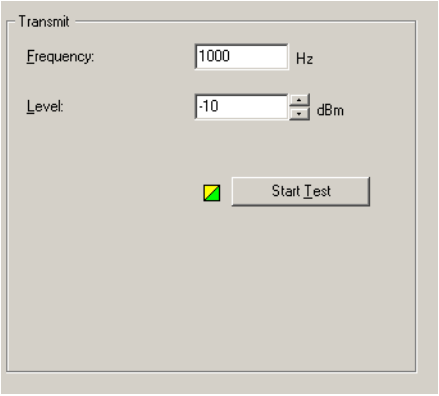
Using the CSS, you can carry out a range of tests on the analog line, the Ethernet interface, the digital inputs and output, the E & M lines, and the serial port.

Analog Line Tests

Using the CSS, you can carry out transmit and loopback tests on the analog line. You can also monitor line levels.

Sending a Test Tone

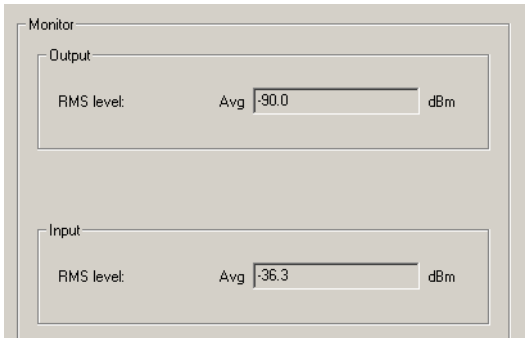
The channel module can output an audio test tone. Use this to test the channel module's ability to output audio on its analog line or to set up and configure the interface from external equipment to the network element.



1. Select Diagnose > Line Interfaces > Analog Line.
2. Under **Transmit**, enter the desired test tone frequency into the **Frequency** box.
3. In the **Level** box, enter a level in dBm.
4. Click **Start Test**.
5. View the **Monitor** area to verify that the network element is sending the test tone.
6. Adjust the external equipment as required.
7. Click **Stop Test** to end the test.

Monitoring Line Levels

The channel module can measure the mean levels of the current analog line input and output and display them on the CSS.



Use this diagnostic tool in the following situations:

- Troubleshooting: the measurement shows whether audio is arriving at the network element.
- Adjusting the audio output of other equipment such as a console.

To avoid transmitting the test audio input, put the base station into Standby mode.

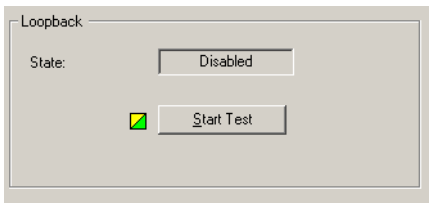
To monitor audio levels

1. Make sure that the analog line is connected.
2. Select Diagnose > Line Interfaces > Analog Line.

   The RMS level boxes display the average levels for audio that the network element sends and receives on the analog line. Levels are measured over a window of 500 ms and updated twice a second. The network element cannot actually measure values at the analog line interface: it measures them in the digital domain and compensates for calibration and line level adjustment effects.

Looping Back Audio

You can loop audio back on the analog line (this simply connects the audio in line to the audio out line). Once the audio is looped back, you can, from the dispatch console end of the audio line, check on line levels or check that the line works in both directions.



To loop back the analog line

1. Make sure that the analog line is connected.
2. Select Diagnose > Line Interfaces > Analog Line.
3. On the toolbar, click **Standby**.

4. In the Loopback area, click **Start test**. The **State** box now displays Enabled.
5. When you have finished testing the analog line, click **Stop test**. The **State** box now displays Disabled.

Testing Connections

The CSS can instruct the connected network element to test whether there is an IP connection (ping test) or to check on the operation of NTP.

Ping Test

The CSS supports the use of the ping command to test whether there is an IP connection to any entity with an IP address. In this way, you can test the IP/Ethernet links from the connected network element to routers and other network elements in the TaitNet P25 digital network. You can also obtain an estimate of link delays and use multicast IP addresses to check the membership of a channel group.

To carry out a ping test

1. Select Diagnose > Line Interfaces > Connections.
2. In the **Destination IP address** box, enter the IP address of the destination host. Use dotted decimal notation, for example 172.25.206.26.
3. Click **Ping**.

   The CSS instructs the network element to send a ping command to the IP address you entered. Responses are displayed in the large **Response** box and the number of responses in the small **Responses** box below.

The response time for a first ping may be long, if the network element needs to send an ARP request to obtain information about the destination IP address. A second ping carried out a short time later will give a more accurate estimate of the link delay, as the information will be cached.

Time Synch (NTP) Test

The CSS can carry out a time synch test to check how the NTP-based time synchronization is working. It instructs the network element to execute the `peers` command from the `ntpq` application. For more information, see www.ntp.org.

To carry out a time synch test

1. Select Diagnose > Line Interfaces > Connections.
2. Under Time synch (NTP) test, click **Start Test**.

   The CSS displays text like the following:

```
  remote           refid      st t when poll reach   delay    offset  jitter
*172.26.1.99    172.26.1.73      2 u   50   64  377   19.663    0.362   0.784
127.127.1.0     .LOCL.          13 l   59   64  377    0.000    0.000   0.244
```

System Interface Tests

The System Interface form (Diagnose > Line Interfaces > System Interface) displays the current state of all digital inputs and outputs. You can toggle the digital outputs and the M-wire output to help you test any equipment connected to them. This can be done on site or on the bench when the network element is connected to a CTU.

The **Digital inputs** area displays the current settings of digital inputs.

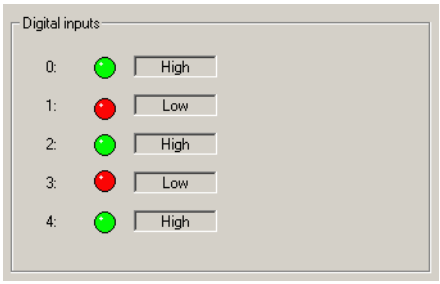
In the **Digital outputs** area, you can toggle the digital outputs. The pin number of each output is displayed.

The area below displays the current state of the E line and M line. You can toggle the M line output.

The **Computed input value** area displays the binary number that is currently set by the digital input lines. This value is used as a Task Manager input.

Testing Digital Inputs

The Digital inputs area displays the current state of all digital inputs to the channel module.



A digital input can be high (green LED) or low (red LED).

To test a digital input

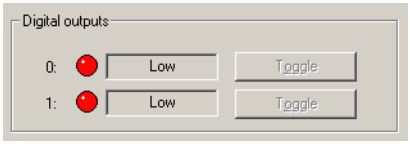
1. Select Diagnose > Line Interfaces > System Interface.
2. Using the equipment connected to the digital input, toggle the state of that input.

If digital input 4 is not available (through configuring pin 1 as an output), ignore its display.

3. In the **Digital inputs** area, check that the state of that input changed.

Testing Digital Outputs

If the system interface is configured to provide a digital output, you can toggle that output between high and low. Pin 9 can provide digital output 0 and pin 1 can provide digital output 1. Use this test to make sure that the output is working and to check that any equipment attached to that output responds as intended.



To test a digital output

1. Select Diagnose > Line Interfaces > System Interface.
2. Go into Standby mode. This is not necessary for the test, but it prevents Task Manager actions from interfering with the test.
3. Click **Start Test**. This enables the Toggle buttons in the **Digital outputs** area. It also sets both digital outputs to low.
4. Click the digital output's **Toggle** button to change its state.

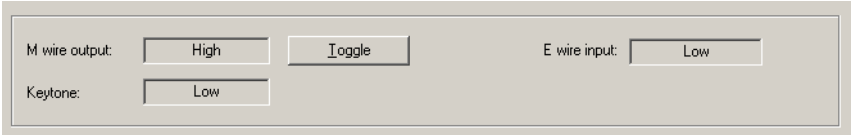
   When the output is high, its LED is green. When it is low, the LED is red.
5. Check the response of any attached equipment.
6. When you have finished testing the outputs, click **Stop Test**. This returns all digital outputs to the low state, irrespective of the state they were in before the test.
7. Return the network element to Run mode.

If you do not want a digital output to be low after this diagnostic test, create a Task Manager task like the following.

IF **Network Element in Run mode** THEN **Set digital output high (output 0)**

Testing the E & M Lines

The network element can be configured to use the E & M lines on the RJ45 connector to carry channel seize and analog valid signals (Configure > Network Element > System Interface).

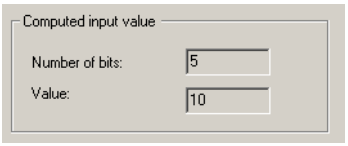


To test the E & M lines

1. Select Diagnose > Line Interfaces > System Interface.
2. Click **Start Test**.
3. Using the equipment (for example the Tait CTU) connected to the E line, toggle the state of that input.
4. In the **E wire input** box, check that the state of the E line changed.
5. Click the **Toggle** button alongside the M wire output box.
6. Check the equipment to verify that the state of the M line changed.

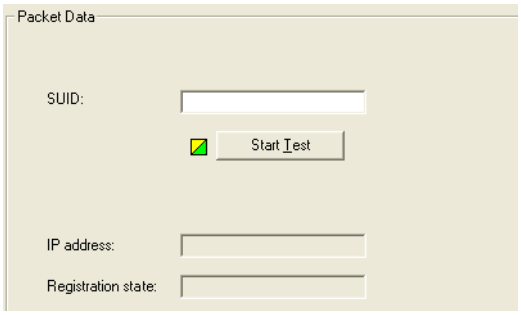
Viewing the Computed Input Value

The Computed input value area (Diagnose > Line Interfaces > System Interface) indicates the number of bits that the network element is using to compute its input value as well as the computed value itself. The former is a configurable item (Configure > Network Element > System Interface) and the latter can be used as a Task Manager input to trigger desired actions such as changing channel.



Packet Data Test

Using the CSS, you can check whether a radio is currently registered with the data gateway. Alternatively, you can step through the data gateway's list of registered radios.



To check a radio

1. Select Diagnose > Line Interfaces > Packet Data.
2. Enter the radio's SUID.
3. Click Start Test.

   If the radio is currently registered, or has ever been registered with the data gateway, its IP address is displayed.

   The Registration state box indicates the radio's status.

Display	Description
Out of range	The radio's SUID is not included in the data gateway's whitelist.
Offline	If an IP address is not displayed, the radio has never been registered with the data gateway. If an IP address is displayed, the radio has de-registered or its registration has expired.
Online	The radio is currently registered. Data can flow across the data gateway between it and a data server.

To step through the radios registered at the gateway

1. Select Diagnose > Line Interfaces > Packet Data.
2. Select the Next online check box.
3. Click Start Test.

   The IP address box shows the first IP address currently assigned to a radio and the SUID box displays the radio ID of that radio.

   The Registration state box indicates the status of the radio.

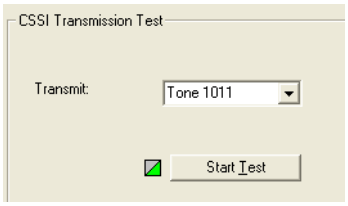
Display	Description
Offline	The radio has de-registered or its registration has expired.
Online	The radio is currently registered. Data can flow across the data gateway between it and a data server.

4. Click Start Test again. The page displays information for the next IP address. Repeat as needed.

CSSI Transmission Test

Using the CSS, you can initiate a transmission test from the trunked analog gateway. The gateway sends dispatcher voice or a test tone over the CSSI interface and the trunked network transmits it.

This test is particularly useful when setting audio levels during installation and commissioning.



To carry out a CSSI transmission test

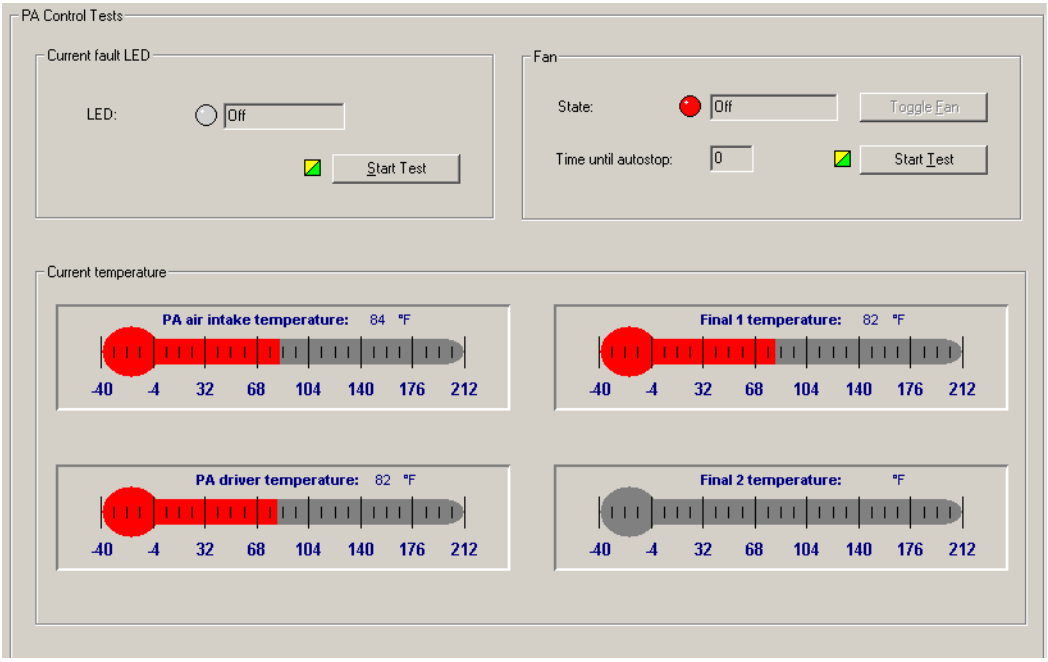
1. Connect the CSS to the trunked analog gateway and put it in Standby mode.
1. Select Diagnose > Line Interfaces > CSSI.
2. In the Transmit list, select Tone 1011 for a test tone or Speech to transmit speech.
3. Click Start Test.
4. Click Stop Test when you are finished.

Modules

Using the CSS, you can carry out various tests on network element modules. You can toggle fans, simulate a mains failure, and test the controls on the control panel.

PA Control Tests

In the PA Control Tests form (Diagnose > Modules > PA Control Tests), you can test the PA fan and front panel fault LED.



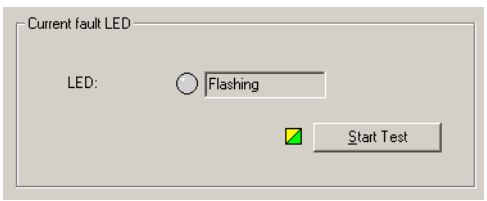
The PA Control Tests form provides information about the PA that is useful before you carry out any tests.

LED	Indicates whether the PA currently has any faults.
State	Indicates whether the fan is currently active.
Current temperature	The Current temperature area displays four thermometers that monitor the four PA temperature sensors.

Testing the PA Fault LED

You can test that the LED on the front of the PA is able to light up. (This LED is only visible when the front panel is removed.)

1. Select Diagnose > Modules > PA Control Tests.



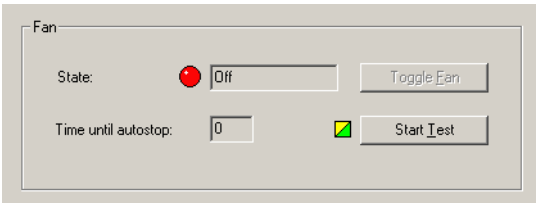
2. Click **Start Test**. This uncouples the fault LED from the PA's operational logic and flashes the LED on and off continuously.
3. Verify that the PA fault LED is in fact flashing.
4. Click **Stop Test** to end the test.

Testing the Fan

You can ask the base station to turn the PA fan on and off. This tests the fan and its control circuitry.

Test the fan after fixing a fan problem or fitting a new fan. When you fit a fan, use this test to verify that the fan is correctly connected, so that the PA (and not the PMU) activates it.

The base station can detect the motion of 3-wire fans and will raise an alarm if the fan does not operate.

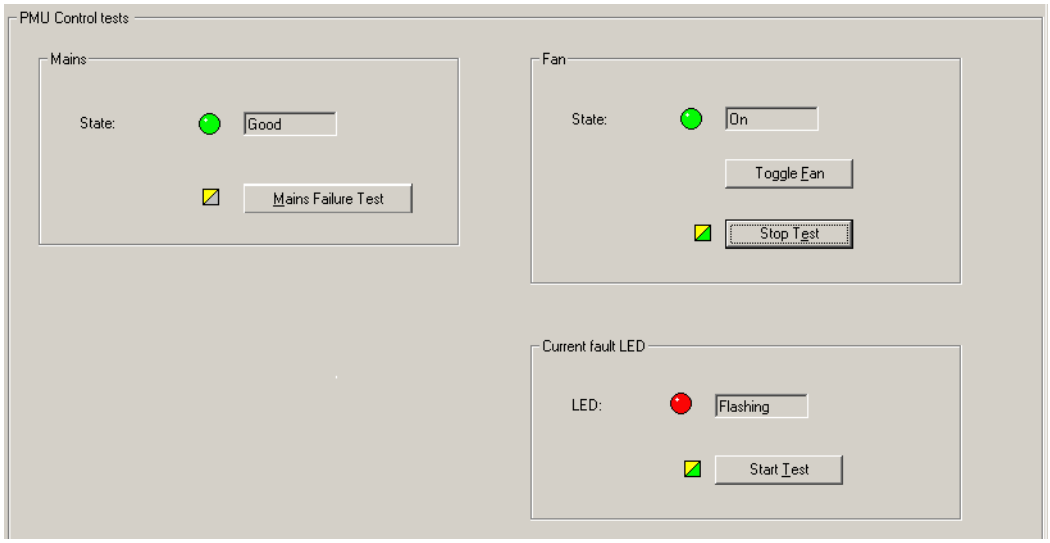


To test the fan

1. Select Diagnose > Modules > PA Control Tests.
2. Click **Start Test**. This uncouples the fan from the base station's control but leaves it in its current state.
3. Click **Toggle Fan**. If the fan was off, this should turn it on.
4. Check that the fan is operating. A 10-second timer counts down. When it expires, the test ends and control of the fan reverts to the base station.

PMU Control Tests

In the PMU Control Tests form, you can simulate a mains failure. You can also check that the fan and the fault LED are working.



Simulating Mains Failure

Simulating a mains failure tests the network element's battery backup and the PMU's DC-DC converter. The test can only be run if there is a DC power supply.

To simulate mains failure

1. On the toolbar, select Standby.
2. Select Diagnose > Modules > PMU Control Tests.
3. Click **Mains Failure Test**.

   The State LED should go off, indicating that mains power is no longer available to the network element.
4. Verify that the network element is still operating.
5. To end the test, click **End Test**.

Testing the Fan

You can ask the network element to turn the PMU fan on and off; this tests the fan and its control circuitry.

Test the fan after fixing a fan problem or fitting a new fan. When you fit a fan, use this test to verify that the fan is correctly connected, so that the PA and not the PMU activates it.

The network element can detect the motion of 3-wire fans and will raise an alarm if the fan does not operate.

To test the fan

1. Select Diagnose > Modules > PMU Control Tests.
2. Click **Start Test.**
3. Click **Toggle Fan**.
4. The State LED should change from On to Off, or from Off to On.

   After ten seconds, the test automatically ends and the network element takes back control of the fan.

Testing the PMU fault LED

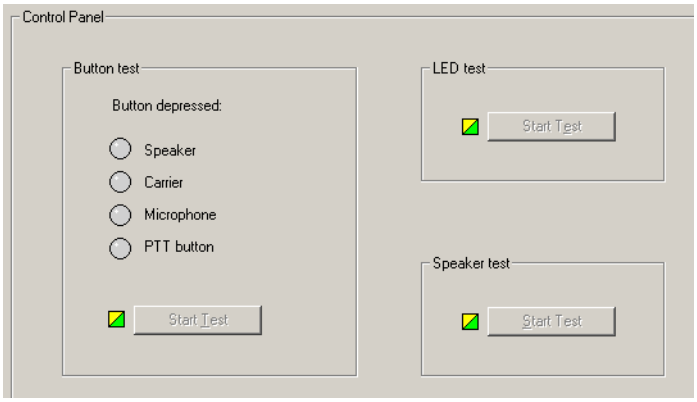
You can test that the fault LED on the front of the PMU is able to light up. (This LED is only visible when the front panel is removed.)

1. Select Diagnose > Modules > PMU Control Test.
2. Under Current fault LED, click **Start Test**. This uncouples the LED from the PMU's operational logic.
3. Check that the PMU LED flashes on and off. (The control panel LED should also light up, unless all PMU alarms are disabled.)
4. Click **Stop Test** to restore the LED's connection with the PMU.

Control Panel Tests

In the Control Panel form (Diagnose > Modules > Control Panel), you can carry out tests to verify that the controls on the front of the network element are working. You must be at the site.

Before starting a test, make sure that the CSS is connected to the same network element (channel) that the control panel currently selects. For example, if the channel button on the control panel has selected 1, you must be connected to reciter 1 or gateway module 1.



To test control panel buttons

1. Under **Button test**, click **Start Test**. This disables all control panel functions. The network element will now pass control panel inputs to the CSS.
2. Press a button on the control panel.
3. Check that the corresponding LED in the CSS form turns green.
4. Repeat steps 2 and 3 for each other button to be tested.
5. Click **Stop Test** to conclude the test.

To test the microphone's PTT button

1. Under **Button test**, click **Start Test**. This disables all control panel functions. The network element will now pass control panel inputs to the CSS.
2. Press the PTT button on the microphone.
3. Check that the PTT button LED in the CSS form turns green.
4. Click **Stop Test** to conclude the test.

To test the control panel LEDs

1. Under **LED test**, click **Start Test**.
2. Check that each of the control panel LEDs is going on and off in a recognizable sequence. (The Power LED is not affected by this test.)
3. Click **Stop Test** to conclude the test.

To test the speaker

1. Under **Speaker test**, click **Start Test**.
2. Turn up the volume and listen to confirm that a 700 Hz test tone at 0 dBm is coming from the speaker.
3. Click **Stop Test** to conclude the test.

Part H Task Manager

The CSS provides a window into Task Manager. You can view the list of tasks, create new tasks from the available list of inputs and actions, and create custom inputs and actions.

You can also monitor recent Task Manager actions and disable any tasks that may be causing problems.

Topics

Introduction to Task Manager

Task Manager operates like this. When the network element is in Run mode, Task Manager processes its task list every 10ms. If a task's input has become true, its action is calculated. Once Task Manager has completed processing its task list, it makes the results available to other firmware processes. When the next 10ms interval is reached, Task Manager begins again with the next processing cycle.

To change the way Task Manager works, you add new tasks or modify existing tasks, and then program the changes into the network element. In effect, you are creating scripts that make the network element perform simple actions. This customizes the way the network element operates without modifying its firmware. Task Manager can perform many functions that previously required expensive external equipment.

Task Manager Rules

Before writing your own sets of tasks, you need to know the following rules that define how Task Manager processes tasks.

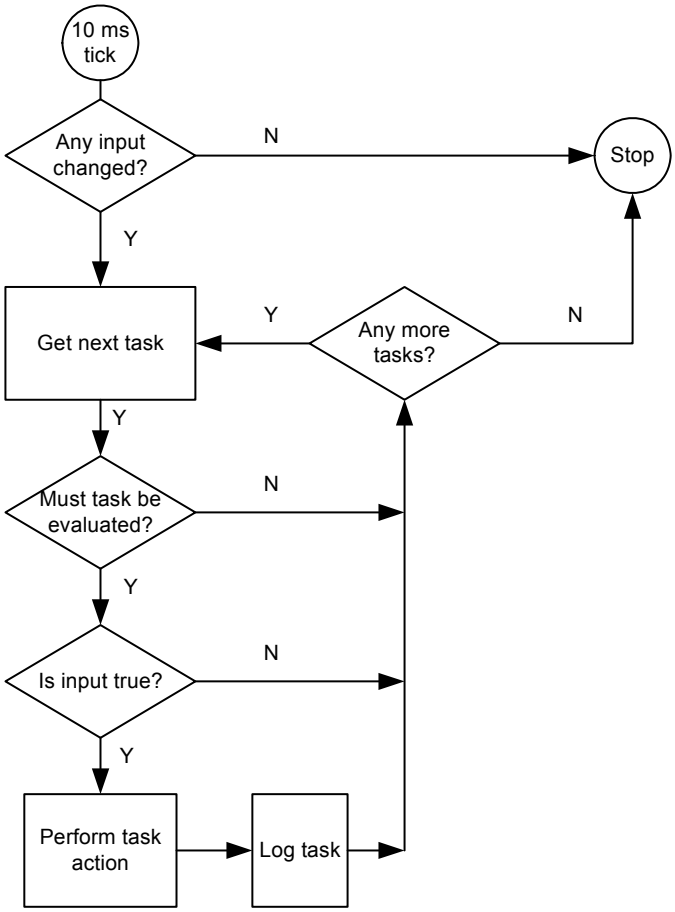
- A task is only carried out if its input changes. For example, when the network element is in Run mode, the task IF Network element in Run mode THEN Increment counter 1 is not carried out. Counter 1 only changes when the network element goes into Run mode, because it is only then that the input changes from false to true.
- Tasks often need to be created in pairs. For example, if you want to set the digital output high in response to an input, you also need to set it low when that input becomes false. Otherwise the output goes high and always stays high.

  IF **Analog received** THEN **Set digital output high**
  IF NOT **Analog received** THEN **Set digital output low**
- Tasks are evaluated in the order of the task list.
- External inputs (for example, alarms) never change in the middle of processing the task list. Changes to these inputs are queued until Task Manager finishes processing the task list. For example, if an alarm is triggered while Task Manager is in the middle of the task list, the equivalent alarm input does not change until the beginning of the next processing cycle.
- Internal inputs (for example, locks) can change in the middle of processing the task list. For example, if a task unlocks automatic CWID, a task later in the list with the input 'IF automatic CWID unlocked' will be processed in the same processing cycle.
- Tasks that are in the General folder are always processed if their input becomes true. Tasks that are in a channel profile or signaling profile folder are only processed if the current channel uses that profile.

Processing Cycle

To help reduce the amount of processing that Task Manager must do, the network element does some additional processing when an input is changed. All Task Manager tasks with that input are flagged "must be evaluated" and a flag "an input has changed" is set. This processing is done as soon as the input changes.

At the 10ms tick, Task Manager begins its processing cycle. First it checks the flag "an input has changed." If no input has changed, it stops and waits for the next 10ms tick. If at least one input has changed, it goes through the task list. First it checks whether a task has been flagged "must be evaluated." If it has, Task Manager processes that task, determining the action to be taken. This is made available to other software processes as soon as the whole task list has been processed.



Input Types

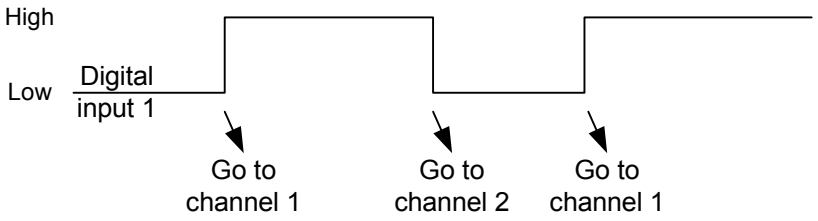
Task Manager inputs are of two fundamentally different types, 'state change' and 'event.' Tasks are triggered differently, depending on the type of input they have.

State change inputs

State change inputs trigger an action when a state changes.

For example.

IF **Digital input high (Input 1)** THEN **Go to Channel (Channel 001)**
IF NOT **Digital input high (Input 1)** THEN **Go to Channel (Channel 002)**



When the digital input goes high, it triggers any action with that input. Although the state of the digital input continues to be high, the action is not triggered again, because the input state has not changed. When the digital input goes low, any action with the IF NOT input becomes true, and that action is triggered. If the digital input goes high again, the action is triggered again.

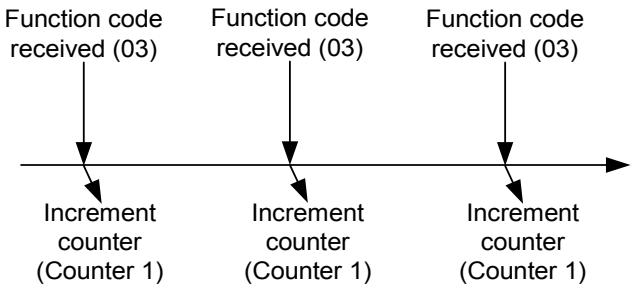
Most Task Manager inputs, including all alarms and digital inputs, are state change inputs.

Event inputs

Event inputs trigger an action whenever the event occurs.

For example.

IF **Function code received (03)** THEN **Increment counter (Counter 1)**



When a function code is received, any action with that input is triggered. If the same function code is received again, the action is triggered again. Task Manager does not maintain the state 'function code has been received.'

Do not use 'IF NOT' with an event input. Task Manager will never trigger such inputs.

The following Task Manager inputs are event inputs:

- Function code received
- Function code sent
- Channel changed
- Channel selected
- Tone remote detected
- Received NAC

Lock inputs

Lock inputs such as 'Receiver unlocked' can only become true through a Task Manager lock action. They are internal to Task Manager. Most become true automatically each time the network element enters Run mode.

Action Types

Task Manager actions are of two main types, 'lock' and 'do now'. These actions have different effects.

Lock actions

Lock actions lock, unlock or toggle a network element function. By default, functions are unlocked (except for the TM Tx key function). When Task Manager locks a function, that function cannot operate. The lock status of these functions is displayed in Monitor > Task Manager > Locks.

Task Manager tasks can have lock actions as an input. When Task Manager unlocks a function (for example automatic CWID), the equivalent input (in this case **Automatic CWID unlocked**) becomes true and any tasks with that input will be processed.

'Do now' actions

'Do now' actions issue a command to the network element to do something immediately, for example to change channel or send the alarm log. This is a one-off action which has no continuing effect on the network element's status. A 'do now' action cannot be re-triggered until the original action is completed. For example, Task Manager cannot carry out the action **Transmit CWID now** when the base station is still transmitting the CWID from a previous **Transmit CWID now** action.

Custom Inputs and Actions

A task can only have one input and one output. However, existing inputs or actions can be combined to form custom inputs or actions.

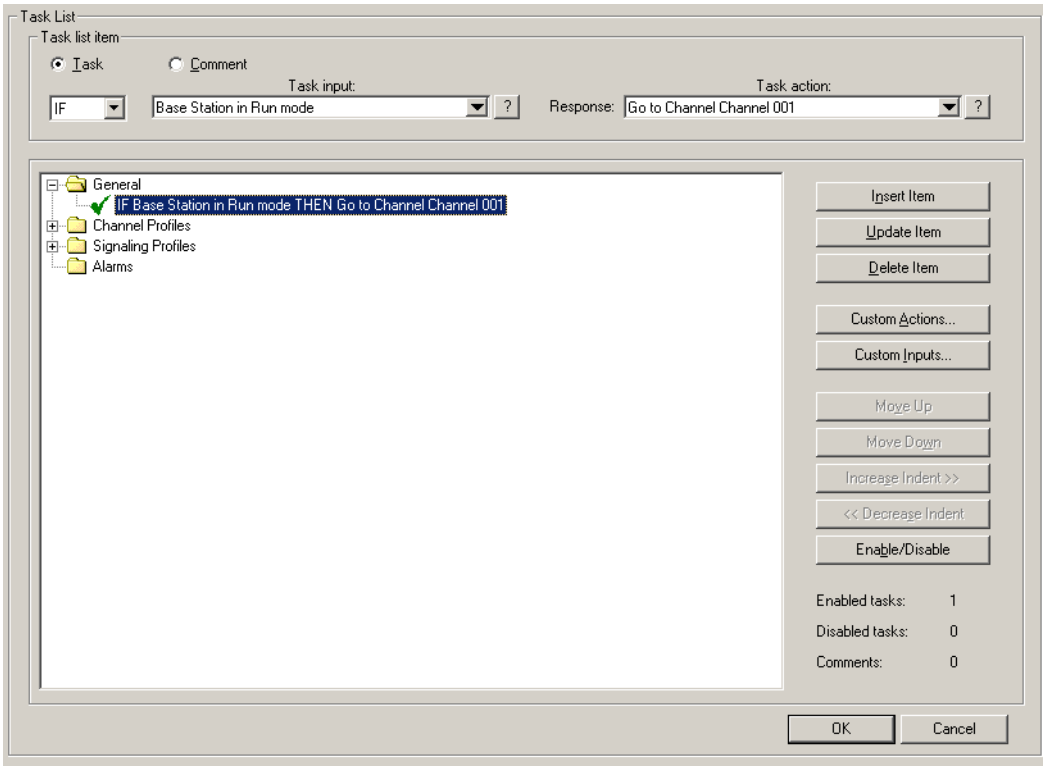
A custom input combines up to eight different inputs. It becomes true when the combination becomes true, according to the rules of the Boolean logic that you specify for the combination.

Similarly, a custom action can combine up to eight actions. When a task with a custom action is processed, all its constituent actions are carried out.

You can also use counters, timers, and your own flags when defining tasks.

Working With the Task List

The Task List form (Configure > Task Manager > Task List) displays the list of tasks that Task Manager processes. You can add new tasks, modify existing ones, and rearrange the order and structure of tasks. Generally, a set of tasks is headed by a comment indicating their nature and purpose. Comments have no effect on Task Manager processing.



In the **Task list item** area, you can create or edit tasks and comments. To edit an existing item, click it in the task list. Click one of the special Help icons to display information about the input or action currently displayed.

The task list displays tasks in folders. Double-click a folder (or click its +/- icon) to open or close it. An open folder displays the tasks and comments that belong to it. Tasks generally have a tick; this means that they are enabled; tasks with a cross have been disabled. Click an item to select it; it appears inside the Task List Item area.

The folders group related tasks. Tasks in a folder for a particular profile (for example, the default channel profile, or Signaling profile 1) are only processed if the current channel uses that profile.

Use the buttons to the right to maintain the tasks in the list. For example, you can insert a newly created item or delete the selected item.

Maintaining the Task List

In Task Manager forms, the buttons to the right of the task list help you maintain the task list. To use some buttons, you must first select a task list item by clicking it.

Update Item — Saves changes made to the selected item and updates the display in the Task List.

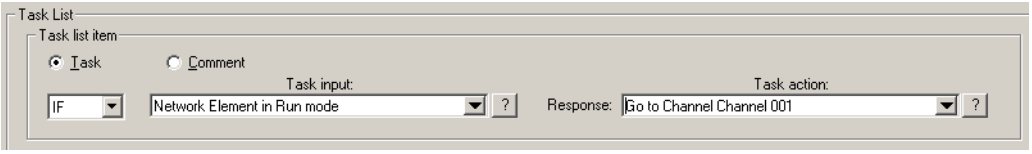
Insert Item	Inserts the task displayed in the Task list item area just below the selected item in the task list. See also "Adding a Task" on page 249.
Delete Item	The Delete button deletes the current task list item.
Custom Actions	Opens the Custom Actions form, where you can define a combination of existing actions.
Custom Inputs	Opens the Custom Inputs form, where you can define a combination of existing inputs.
Move Up / Move Down	Shift the selected item up or down one line. Use these buttons to rearrange the order of tasks and comments in the task list.
Increase Indent / Decrease Indent	Adds or removes an indent from a selected task. Indents have no effect on Task Manager processing; they help to make tasks easier to read and understand. You can only indent tasks that are under a comment.
Enable / Disable	By default, tasks are enabled; when an input condition becomes true, Task Manager processes the task. Use the Enable / Disable button to disable a task so that it has no effect, or toggle it between enabled and disabled.
Enabled tasks	Displays the total number of enabled Task Manager tasks. You can have up to 200 enabled tasks.
Disabled tasks	Displays the total number of disabled Task Manager tasks. The total number of tasks (enabled and disabled) must not exceed 400.
Comments	Displays the total number of Task Manager comments. The task list can have up to 100 comments.

Adding a Task

To make full use of the network element's capabilities, you need to add your own tasks to the list that Task Manager processes. This enables Task Manager to respond to events in a way that is tailored to the system. However, the set of actions must be well thought out to operate in exactly the way you want.

It is possible to create tasks that undermine the network element's ability to operate properly. Make sure that the choices made are appropriate. Be particularly careful with powerful actions such as Lock transmitter.

While Tait has carefully tested each input and each action, it is not possible to test the enormous number of possible combinations of inputs and actions. Thoroughly test any tasks before commissioning the network element. If you are uncertain about anything, refer to your supplier.



You can add a task anywhere in the task list. The order of tasks in the task list represents the order that they are processed in.

Tasks in a channel profile or a signaling profile folder will only be processed if the current channel has that profile assigned to it.

To define a task

1. Select Configure > Task Manager > Task List.
2. In the task list, click a task or comment below which you want to add the task. Alternatively, click a folder.
3. Select **Task** in the Task list item area.
4. In the drop-down text box, select IF.

   Alternatively, for the task to be processed when the input condition goes from true to false, select IF NOT. For example, tasks with the input 'IF NOT **Rx Gate valid**' will be processed when the base station stops receiving a RF signal that fulfils all the gating requirements.
5. Position the mouse cursor over the next drop-down box and click to open the list of available inputs.
6. Select an input from the list. It appears in the box.
7. In the same way, select an action from the drop-down list of the last drop-down text box.
8. Click **Insert Item**. The task appears in the task list.
9. If necessary, use the buttons on the right to move the task up or down, or to indent it.

Adding a Comment

When defining a set of tasks, you need to provide a comment that names them and indicates what they are for and how they work. You may also want to add further comments on individual tasks.

To add a comment

1. Select Configure > Task Manager > Task List.
2. In the task list, click the task above which you want to add the comment. Alternatively, click a folder.
3. In the Task list item area, select the **Comment** option.
4. Enter the text of the comment into the box below.
5. Click **Insert Item**. The comment appears in the task list.

6. If necessary, use the buttons on the right to move the comment up or down, or to indent tasks under it.
7. Click **OK** to confirm the changes and close the form.

Disabling a Task

You can disable any task in the task list. This is an easy way to stop Task Manager doing something. (When the network element is in Standby mode, Task Manager is disabled and no tasks are executed.)

To disable a task

1. In any Task Manager form, click a task.
2. Click **Enable/Disable**. The tick at the beginning of the task turns into a cross.

Tip: Disable a comment to disable all tasks indented under that comment.

Inputs

An input is anything that Task Manager monitors. When the state of that input changes from false to true, Task Manager executes tasks with that input. IF NOT tasks are executed when the state of the input changes from true to false.

To select an input

1. In the **Task list item** area, click in the **Task input** box. A menu with several submenus appears.
2. Click on an item in the menu or submenu.

To obtain Help on the input of a task

1. In the task list, click the task. The task appears in the **Task list item** area.
2. Click the Help button beside the **Task input** box.

Alarm Inputs

Any alarm can be a Task Manager input. This makes it possible to individually configure the network element's response to any alarm. For information about alarms, see "Monitoring Alarms" on page 199. All alarms are basic inputs. Even if an alarm is disabled in the Alarm Control form, tasks with that alarm as an input will be processed.

1 PPS absent

This input becomes true when the network element loses its 1 PPS input, triggering the 1 PPS pulse absent alarm. For information about this alarm, see "Absent" on page 207.

Battery protection mode on

This input becomes true when the PMU is operating in battery protection mode, triggering the 'Battery protection mode' alarm. For information about this alarm, see "Battery protection mode" on page 203.

Battery voltage high

This input becomes true when the 'Battery voltage high' alarm is triggered. For information about this alarm, see "Battery voltage high" on page 203.

Battery voltage low

This input becomes true when the 'Battery voltage low' alarm is triggered. For information about this alarm, see "Battery voltage low" on page 203.

Channel invalid

This input becomes true when the 'PA calibration invalid' alarm is triggered. For information about this alarm, see "Calibration invalid" on page 200.

External reference absent

This input becomes true when the 'External reference absent' alarm is triggered. For information about this alarm, see "External reference absent" on page 207.

External reference invalid

This input becomes true when the 'External reference invalid' alarm is triggered. For information about this alarm, see "External reference invalid" on page 207.

Fan failed

This input becomes true when the PA or PMU 'Fan failed' alarm is triggered. For information about these alarms, see "Fan failed" on page 200 for the PA or "Fan failed" on page 202 for the PMU.

Invalid channel selected

This input becomes true when the channel invalid alarm is triggered. For information about this alarm, see "Channel invalid" on page 204.

Network board alarm on

This input becomes true when any network board alarm is triggered.

Network board invalid calibration

This input becomes true when the Calibration invalid alarm is triggered. For more information, see "Digital board calibration invalid" on page 204.

Network board invalid configuration

This input becomes true when the Configuration invalid alarm is triggered. For more information, see "Digital board configuration invalid" on page 205.

Network board QoS Jitter

This input becomes true when the QoS jitter alarm is triggered. For more information, see "QoS jitter" on page 207.

Network board QoS lost packets

This input becomes true when the Lost packets alarm is triggered. For more information, see "QoS lost packets" on page 207.

Network element alarm on

This input becomes true when any alarm is triggered.

No PA detected

This input becomes true when the 'No PA detected' alarm is triggered. This occurs when the module fails or control bus communications are disrupted. For information about this alarm, see "No PA detected" on page 200.

No PMU detected

This input becomes true when the 'No PMU detected' alarm is triggered. This occurs when the module fails or control bus communications are disrupted. For information about this alarm, see "No PMU detected" on page 202.

PA air intake temperature high

This input becomes true when the 'Air intake temperature high' alarm is triggered. For information about this alarm, see "Air intake temperature high" on page 206.

PA air intake temperature low

This input becomes true when the 'Air intake temperature low' alarm is triggered. For information about this alarm, see "Air intake temperature low" on page 206.

PA alarm on

This input becomes true when any PA alarm is triggered.

PA current fault

This input becomes true when any of the PA's current alarms are triggered. This happens if any part of the PA is drawing excessive current, or if one final stage uses significantly more current than the other. For information about these alarms, see "Current" on page 201.

PA forward power low

This input becomes true when the 'Forward power low' alarm is triggered. For information about this alarm, see "Forward power low" on page 200.

PA is shut down

This input becomes true when the PA's 'Shutdown' alarm is triggered. For information about this alarm, see "Shutdown" on page 201.

PA power foldback

This input becomes true when the PA's 'Power foldback' alarm is triggered. For information about this alarm, see "Power foldback" on page 201.

PA supply voltage fault

This input becomes true when one of the PA's power supply voltage alarms is triggered. This happens if the voltage is too high or too low. For more information, see "Supply voltage" on page 201.

PA temperature high

This input becomes true when the one or more of the PA's 'Temperature high' alarms is triggered. For information about this alarm, see "Temperature high" on page 202.

PMU alarm on

This input becomes true when any PMU alarm is triggered.

PMU mains supply failed

This input becomes true when the PMU's 'Mains supply failed' alarm is triggered. For information about this alarm, see "Mains supply failed" on page 203.

PMU output failed

This input becomes true when one of the PMU's output alarms is triggered, because the voltage is high or low or the current is high. For information about these alarms, see "Output" on page 203.

PMU power up fault

This input becomes true when the PMU's 'Power up fault' alarm is triggered. For information about this alarm, see "Power up fault" on page 203.

PMU shutdown imminent

This input becomes true when the PMU's 'Shutdown imminent' alarm is triggered. For information about this alarm, see "Shutdown imminent" on page 203.

PMU temperature high

This input becomes true when the PMU's 'Temperature high' alarm is triggered. For information about this alarm, see "Temperature high" on page 203.

Reciter alarm on

This input becomes true when any alarm in the channel module is triggered.

Reverse power high

This input becomes true when the 'Reverse power high' alarm is triggered. For information about this alarm, see "Reverse power high" on page 201.

Use the VSWR fault input instead of the Reverse power high input if the transmit power is set to less than 20 W or if the base station has a 5 W PA. The resolution of the reverse power measurement is 1 W; only a very serious antenna fault would trigger the reverse power high alarm if the power setting is low.

Simulcast unsynchronized

This input becomes true when the network element becomes unsynchronized, triggering the Simulcast unsynchronized alarm, for example because it lost its 1 PPS signal and the holdover timer has expired.

Synthesizer failed

This input becomes true when a synthesizer goes out of lock or the external frequency reference is invalid and the corresponding alarm is triggered. For information about these alarms, see "Synthesizer out of lock" on page 205 and "External reference invalid" on page 207.

Tx not ready

This input becomes true when the exciter begins training its VCXO, triggering the corresponding alarm. For information about this alarm, see "Tx not ready" on page 206.

VSWR fault

This input becomes true when the 'VSWR high' alarm is triggered. For information about this alarm, see "VSWR high" on page 201.

Analog Line Interface

Analog line inputs are concerned with the state of the analog line interface.

Channel seized

The Channel seized input becomes true when the analog interface receives a channel seize signal. This signal must be received by the means that the network element is configured to recognize (digital input, E & M, or tone remote).

Tone remote detected

The Tone remote detected (nnn) event input becomes true when the network element detects function tone number nnn on its analog line. To select this input, specify a frequency (Tone 1) for a single tone or a frequency pair (Tone 1 and Tone 2), depending on whether the analog line is configured for single tone or dual tone.

Do not use IF NOT with this input.

Channel

Task Manager has inputs that become true when a particular channel is selected or when the channel is changed.

Channel changed

The **Channel changed** event input becomes true when the network element changes from one channel to another.

Select channel

The **Channel (Channel name)** event input becomes true when the network element changes channel to the channel in the channel table with the specified channel name.

Digital fixed station interface

Task Manager can monitor the state of the DFSI interface.

DFSI connected

The **DFSI connected** input becomes true when a conventional DFSI connection is established.

Digital I/O

Digital I/O inputs are concerned with the state of the digital inputs and outputs.

Digital input (n) high

The **Digital input (n) high** input becomes true when digital input n goes high.

Pin 1 can be configured as digital input 4, as an antenna relay driver, or as digital output 1. The Task Manager input 'Digital input 4 high' reflects the state of pin 1, no matter how it is configured. It can therefore be used to modify base station operation depending on the state of the antenna relay driver.

Example

As the network element digital inputs float high, you probably want to create statements that trigger when the input is pulled low.

IF NOT **Digital input (2) high** THEN **Go to channel 2**

Digital input value

The **Digital input value nn** input becomes true when the setting of one or more digital inputs is changed so that the binary equivalent of those settings equals nn. Low is read as '0' and high as '1'.

Example

IF **Digital input value 3** THEN **Go to channel 3**

Digital output high

The **Digital output high (output n)** input becomes true when the network element sets digital output n high. This can only happen through the Task Manager actions **Set digital output high** and **Toggle digital output**.

Locks

Most locks are unlocked when the network element starts up. Unlock inputs only change through Task Manager lock actions. An unlock input become true when its function is unlocked after having been locked.

Analog line unlocked

The analog line is unlocked when the network element enters Run mode and when Task Manager unlocks the analog line after having previously locked it.

Automatic CWID unlocked

The automatic sending of a CWID is unlocked when the base station enters Run mode or when Task Manager unlocks the channel group after having previously locked it.

Auxiliary supply unlocked

The auxiliary supply unlocked input becomes true when the network element enters Run mode or when a Task Manager action unlocks the auxiliary supply. This only turns the auxiliary power output on if the Auxiliary power control box (Configure > Network Element > Miscellaneous) is set to Task Manager.

Channel group unlocked

The channel group is unlocked when the network element enters Run mode or when Task Manager unlocks the channel group after having previously locked it.

Receiver unlocked

The receiver is unlocked when the base station enters Run mode or when Task Manager unlocks the receiver after having previously locked it.

Subaudible encoding unlocked

The encoding of subaudible signaling is unlocked when the base station enters Run mode or when Task Manager unlocks this function after having previously locked it.

Subaudible/NAC decoding unlocked

The decoding of subaudible signaling and the NAC is unlocked when the base station enters Run mode or when Task Manager unlocks this function after having previously locked it.

Transmitter unlocked

The transmitter is unlocked when the base station enters Run mode or when Task Manager unlocks the transmitter after having previously locked it.

Network

Network inputs are concerned with network element functioning that affects the wider network.

Function code received

The **Function code received (nn)** input becomes true when the network element receives the function code nn from another channel group member. This input makes it possible for Task Manager to carry out an action on receiving a function code, which could for example be sent when a P25 console gateway receives a dispatcher wildcard command. See the TaitNet P25 Conventional System Manual for details.

Function codes are sent using UDP and can therefore be lost in transit across the network. Task Manager scripts need to be resilient enough to cope with such events. If reliability is important, this can be achieved by regularly sending the function code (heartbeat) or by implementing a request/acknowledge protocol. Flags can be used to represent states.

Do not use function codes for changing channel, for enabling/disabling RF repeat, or for monitor mode. Use collective channel control instead.

Example

IF **Function code received (02)** THEN **Lock transmitter**

Function code sent

The **Function code sent (nnn)** input becomes true when Task Manager instructs the network element to send function code nnn to the channel group.

Do not use function codes for changing channel or for enabling/disabling RF repeat or monitor mode. Use collective channel control instead.

Monitor on

The Monitor on input becomes true when the base station enters monitor mode. This disables the analog line's selective squelch and the receiver's filters for NAC, CTCSS and DCS. The receiver will unmute irrespective of the signal's NAC or analog subaudible signaling. However, the receiver still applies gating to analog FM calls based on RSSI and/or SINAD. Dispatcher commands can enable or disable monitor mode directly over the DFSI or indirectly over the analog line via function tones and suitable Task Manager tasks (see "Monitor actions" on page 267).

Vote won by Analog line

The **Vote won by Analog line** input becomes true when the network element's voter (switch) declares the signal on the analog line to be the best and the channel group repeats that signal.

Vote won by Digital line

The **Vote won by Digital line** input becomes true when the network element's voter (switch) declares the signal received on the digital line to be the best and the channel group repeats that signal.

Vote won by Control panel

The **Vote won by Control panel** input becomes true when the network element's voter (switch) declares the signal received from the control panel microphone to be the best and the channel group repeats that signal.

Vote won by RF

The **Vote won by RF** input becomes true when the base station's voter declares the signal received from the base station's own receiver to be the best and the channel group repeats that signal.

Network element in Run mode

The **Network element in Run mode** input becomes true when the network element goes into Run mode. This occurs on startup and when the CSS tells a network element in Standby mode to change to Run mode.

Use this input for tasks to be included in Task Manager's initialization routine, to start timers, and to lock functions that will only operate under particular circumstances.

The inverse of this input (IF NOT Network element in Run mode) must not be used; when the network element is not in Run mode, Task Manager is not operating.

Example

IF **Network element in Run mode** THEN **Lock transmitter**
IF **Network element in Run mode** THEN **Lock receiver**

This example could be used to configure a backup base station with everything locked but ready to go into operation when needed.

RF interface

RF interface inputs are concerned with the state of things at the base station's RF interface.

Analog received

The **Analog received** input becomes true when the base station starts receiving an analog FM signal on its RF interface.

Analog transmitted

The **Analog transmitted** input becomes true when the base station starts transmitting an analog FM signal on its RF interface.

APCO received

The **APCO received** input becomes true when the base station recognizes, through detecting frame synchronization, that it is receiving a digital P25 digital signal on its RF interface.

APCO transmitted

The **APCO transmitted** input becomes true when the base station begins transmitting a digital P25 signal on its RF interface.

PA carrier present

Whenever the reciter tells the PA to start transmitting, the **PA carrier present** input becomes true.

Received NAC

The **Received NAC nnn** event input becomes true when the base station begins receiving a digital transmission with a NAC of nnn.

This input is very useful as it enables an SU to control a base station. While the base station can only detect the subaudible signaling that it is configured for, it can detect any NAC. This means that you can set up a variety of tasks, each of which is triggered by receiving a particular NAC.

Example

IF **Received NAC (03)** THEN **Go to Channel (Channel 002)**

Do not use IF NOT with this input. The absence of a specific NAC cannot be used to trigger tasks. Instead, set up a task with a different NAC as its input. Then SU users can send the different NAC to reverse an action that has been triggered by sending the first NAC.

RF repeat

The **RF repeat** input becomes true when RF repeat is enabled in the base station. This can occur as a result of a dispatcher command (received via the DFSI gateway or implemented using the Task Manager action Enable/Disable/Toggle RF repeat). It can also occur when the base station changes channel or transitions to Run mode, if this enables RF repeat.

Rx Gate valid

The **Rx Gate valid** input becomes true when the criteria for unmuting the receiver are met. **Rx Gate valid** becomes true even if the receiver signal does not win the vote. **Rx Gate valid** becomes true for analog FM and for digital P25 signals.

Subaudible tone detected (Tone *n*)

The **Subaudible tone detected (Tone n)** input becomes true when the base station detects one of the CTCSS tones or DCS codes that are configured for the current signaling profile. Before creating a task with this input, configure the signaling profile with the subaudible signaling that you want to trigger the action.

Task Manager

Inputs under the Task Manager heading are concerned with special aspects of Task Manager: Custom inputs, flags, timers, and counters.

Counter at maximum

The **Counter at maximum (Countername)** input becomes true when the particular named counter reaches the maximum value set for it in Configure > Task Manager > Counters.

The counter value changes through Task Manager actions such as **Increment counter**. Counter values are read at the beginning of a processing cycle. If the counter value changes during the processing cycle, it is immediately available; any subsequent tasks will use the new input. When the network element enters Run mode, all counters are reset to 0.

Example

IF **Counter at maximum (LightTrigger)** THEN **Set digital output low**

Custom Inputs

The Custom Inputs submenu contains all the custom inputs that have been defined for the network element using Configure > Task Manager > Custom Inputs.

Flag set (flagname)

The **Flag set** (***flagname***) input becomes true when Task Manager sets the corresponding flag. *Flagname* represents any name that was assigned to the flag in Configure > Task Manager > Flags. The state of flags is read at the beginning of a processing cycle. If a flag state changes during the processing cycle, it is immediately available; any subsequent tasks will use the new input. When the network element enters Run mode, each flag is cleared, unless a Task Manager task explicitly sets it.

Timer expired

A timer can only be started by the Task Manager action **Start timer**. It expires when the timer's maximum time has elapsed. This time was entered in Configure > Task Manager > Timers.

Example

IF **Timer expired** (CWID timer) THEN **Transmit CWID now**

This input can be used to set up regular actions such as transmitting the CWID.

Trunking

Trunking inputs can be used when the base station is part of a trunking system and is connected to an external trunking site controller.

Control channel

The **Control channel** input becomes true when a TB9100 base station enters Run mode and is handled by the trunking controller as a control channel or when a TB9100 base station, operating as a traffic channel, takes over the control channel function when the previous control channel fails. This input makes it possible for Task Manager to modify base station operation to suit control channel operation.

The **Control channel** input becomes false when a traffic channel enters Run mode. The input IF NOT **Control channel** can be used to configure base station operation specifically for traffic channel operation.

Example

IF **Control channel** THEN **Go to channel 1**
IF NOT **Control channel** THEN **Go to channel 2**

Site controller present

The **Site controller present** input becomes true when a TB9100 base station enters Run mode and receives heartbeat messages from an external trunking site controller. This input makes it possible for Task Manager to modify base station operation to suit trunking operation.

The **Site controller present** input becomes false if the base station loses contact with its site controller. The input IF NOT **Site controller present** can be used to configure base station operation when site controller communications fail.

Actions

An action is something that Task Manager instructs the network element to do.

There is often a group of actions relating to a particular network element function. For example, Task Manager can lock, unlock, or toggle the automatic transmission of a network element identity, or set, clear, or toggle a flag.

To select an action

1. In the **Task list item** area, click in the **Task action** box. A menu with several submenus appears.
2. Click on an item in the menu or submenu.

To obtain Help on the output of a task

1. In the task list, click the task. The task appears in the **Task list item** area.
2. Click the Help button beside the **Task action** box.

Channel Actions

Channel actions make it possible to change the network element's current channel.

Go to channel

The **Go to channel** action instructs the network element to change channel and operate according to the configuration defined by the channel with the name specified in the action. It stays on that channel until another Task Manager action changes channel (for example following a reset).

The actual change of operating channel happens at the end of a processing cycle. This means, for example, that if the task list has a **Go to channel channel 005** action followed by a **Go to channel channel 006** action, the network element will only ever change to channel 006.

Make sure that Task Manager actions do not ask the network element to change channel more often than once every 500ms.

Go to next channel

The **Go to next channel** action instructs the network element to operate on the next valid channel in the channel table. If the network element was on Channel 001, it changes to Channel 002. It stays on that channel until a Task Manager action changes channel (for example following a reset).

The actual change of operating channel happens at the end of a processing cycle. This means, for example, that if the task list has two **Go to next channel** actions, the network element will move two channels down the channel table.

If the network element is already operating on the last channel in the channel table, the action takes it to the first channel.

Make sure that Task Manager actions do not ask the network element to change channel more often than once every 500ms.

Go to previous channel

The **Go to previous channel** action instructs the network element to operate on the previous valid channel in the channel table. If the network element was on Channel 002, it changes to Channel 001. It stays on that channel until a Task Manager action changes channel (for example following a reset).

In network elements with a complex set of Task Manager tasks, it is important to understand exactly how this action works. It is not a 'do now' action; the actual change of operating channel happens at the end of a processing cycle. This means, for example, that if the task list has two **Go to previous channel** actions, the network element will move two channels up the channel table.

If the network element is already operating on the first channel in the channel table, the action takes it to the last channel.

Make sure that Task Manager actions do not ask the network element to change channel more often than once every 500ms.

Profile actions

Task Manager profile actions can instruct the network element to use a particular named channel group, calling profile, or service profile, overriding the one specified by the channel table.

Go to call profile

The **Go to call profile** action instructs the network element to use the calling profile named in the action. This overrides the calling profile selected by the channel table and supersedes any calling profile selection by the dispatcher using function tones (see Configure > Analog Line > Tone Remote Mapping). A subsequent function tone selection of calling profile will supersede the Task Manager action.

Go to channel group

The **Go to channel group** action instructs the network element to become part of the channel group named in the action. This overrides the channel group selected by the channel table.

Go to RF service profile

The **Go to RF service profile** action instructs the network element's RF interface to use the service profile named in the action. This overrides the service profile selected by the channel table but does not affect the service profile selected by the calling profile for the analog line interface.

Digital output actions

Task Manager actions can set the digital outputs high or low or toggle them between the two states.

Set digital output high

The **Set digital output high** action sets the selected digital output line high.

The actual setting of the digital output doesn't happen till the end of a processing cycle. So the task list can set the digital output high or low many times, but the output line will only ever be set in the way that the last action in the task list specifies.

When you select this action, a dialog box pops up so that you can select the digital output line to use. The Task Manager action will only have an effect if the relevant system interface pin has been configured as a digital output.

Set digital output low

The **Set digital output low** action sets the selected digital output line low.

The actual setting of the digital output doesn't happen till the end of a processing cycle. So the task list can set the digital output high or low many times, but the output line will only ever be set in the way that the last action in the task list specifies.

When you select this action, a dialog box pops up so that you can select which digital output line to use. The Task Manager action will only have an effect if the relevant system interface pin has been configured as a digital output.

Example

IF **Counter at maximum (LightTrigger)** THEN **Set digital output low**

Toggle digital output

The **Toggle digital output** action changes the state of the selected digital output line. If it was low, it become high. If it was high, it becomes low.

The actual setting of the digital output doesn't happen till the end of a processing cycle. So the task list can change the state of the digital output many times, but the output line will only ever be set in the way that the last action in the task list specifies.

When you select this action, a dialog box pops up so that you can select the digital output line to use. The Task Manager action will only have an effect if the relevant system interface pin has been configured as a digital output.

Fan test now

The 'do now' action **Fan test now** instructs the network element to run the fans for 5 seconds, irrespective of the temperature. If the fans are already running, this has no effect.

Locks

Lock actions lock, unlock or toggle a network element function. By default, most functions are unlocked (except for TM Tx Key). When Task Manager locks a function, that function cannot operate. If Task Manager unlocks a function, it is free to operate. (However, for the function to actually operate, it may need to be licensed and to be enabled in configuration.)

Generally speaking, if you create a task that locks a function, you need to create at least one equivalent function that unlocks it again.

The current status of Task Manager locks is displayed in Monitor > Task Manager > Locks.

Each lock action has an equivalent lock input. When Task Manager unlocks a function (for example automatic CWID), the equivalent input (in this case **Automatic CWID unlocked**) becomes true and any tasks with that input will be processed.

Analog line lock

Task Manager can lock the analog line. This disconnects the dispatch console from the network element. No analog voice can pass between the console and the network element. Physical signaling on the E line is recognized, but the channel cannot be seized.

Automatic CWID lock

Task Manager can lock the automatic transmission of a CWID. This stops the base station from transmitting its CWID as configured in Configure > RF Interface > CWID. It does not affect the ability of Task Manager to send a CWID using the action **Transmit CWID now**.

Auxiliary supply lock

If the Auxiliary power control box (Configure > Network Element > Miscellaneous) is set to Task Manager, locking the auxiliary supply turns it off and unlocking it turns it back on again.

Example

IF **Network element in Run mode** THEN **Lock auxiliary supply**

This task turns the auxiliary output off whenever the network element enters Run mode.

Channel group lock

Task Manager can lock the current channel group. This disconnects the network element from its channel group so that it cannot receive a voice stream or function code from other channel group members.

Changing channel group (by changing channel) has no effect on the lock.

Remote locking and unlocking of a network element's channel group using function codes is not supported. While a function code can lock the channel group, it cannot subsequently unlock the channel group.

Example

IF **Tone remote detected (650)** THEN **Lock Channel Group**.
IF **Tone remote detected (850)** THEN **Unlock Channel Group**.

This pair of tasks makes it possible for the dispatcher to instruct a TB9100 base station to disconnect itself from the channel group, so that dispatcher communications only use that base station, and then to re-connect the base station, as needed.

Receiver lock

Task Manager can lock the receiver. This prevents the base station from receiving any RF signals.

Subaudible encode lock

Task Manager can lock the encoding of subaudible signaling. When encoding is locked, transmissions do not contain any subaudible signaling.

The transmission of the NAC cannot be locked, because it is not possible to send P25 digital transmissions without a NAC.

When decoding is unlocked, the transmitter behaves according to the current signaling profile.

Subaudible/NAC decode lock

Task Manager can lock the decoding of subaudible signaling and the NAC. When decoding is locked, the receiver unmutes irrespective of the subaudible signaling or the NAC that the received signal contains.

When decoding is unlocked, the receiver behaves according to the current signaling profile.

Transmitter lock

Task Manager can lock the transmitter. This prevents the base station from sending any RF signals.

Monitor actions

Task Manager can enable or disable the monitor function. Monitor mode disables the analog line's selective squelch and the receiver's filters for NAC, CTCSS and DCS. The receiver will unmute irrespective of the signal's NAC or analog subaudible signaling. However, the receiver still applies gating to analog FM calls based on RSSI and/or SINAD.

Monitor actions make it possible for the analog dispatch equipment to control monitor mode via function tones. Monitor commands can control the monitor mode of the whole channel group, if that control is set to collective in each member's channel group configuration.

Example

IF **Tone remote detected (550)** THEN **Enable monitor**

RF repeat actions

If the RF Repeat setting of the current channel (in the channel table) is set to DispatchControlled, Task Manager can enable, disable, or toggle the base station's RF repeat function. If the control of RF repeat is set to Collective (see "RF repeat" on page 160), this action will be passed on to the other members of the channel group.

You can create tasks with this action in the P25 console gateway, even though it has no RF capability. The action has no effect on the console gateway itself, but if collective channel control is enabled, the action is passed on to the other channel group members.

Example

IF **Tone remote detected (550)** THEN **Enable RF repeat**
IF **Tone remote detected (650)** THEN **Disable RF repeat**

Send function code

The **Send function code** action sends the defined function code over the digital line to all channel group members. This action can be used to propagate a dispatcher wildcard command to the channel group. See the TaitNet P25 Conventional System Manual for details. It can also be used in conjunction with timers to send heartbeat messages to standby base stations, which can enter service if they cease to receive the heartbeats.

Do not use function codes for changing channel, enabling/disabling RF repeat, or enabling/disabling monitor mode. Use collective channel control instead.

Caution is needed when using function codes. They are sent using UDP and can therefore be lost in transit across the network. Also, if a function code is followed by a second function code in less than 10ms, Task Manager is unable to process the first code. Intensive use of function codes (more than two per second per channel group) could degrade voice quality. Task Manager scripts need to be resilient enough to cope with such events. Using Task Manager flags to represent states can help.

Example

IF **Tone remote detected (550**) THEN **Send Function Code 5**

Statements of this type make it possible for wildcard commands received over the analog line to be relayed to other channel group members.

Task Manager

Outputs under the Task Manager heading are concerned with special aspects of Task Manager: counters, custom outputs, flags and timers.

Counter actions

Task Manager actions make it possible to increment or decrement a counter value, or to reset the value to 0. Before creating statements with these actions, set up one or more counters in Configure > Task Manager > Counters.

Increment counter

The **Increment counter (nn)** action adds one to counter nn. When a counter reaches its specified maximum, it triggers actions with the input **Counter at maximum (nn)**. Further Increment counter actions have no effect.

Decrement counter

The **Decrement counter** action subtracts one from the current value of the counter specified. If the counter is at 0, Decrement counter actions have no effect.

Reset counter

The Reset counter action sets the value of the counter specified to zero, so that it must begin counting anew.

Flag actions

Task Manager actions can set, clear, or toggle flags. Before creating statements with flag actions, name one or more flags in Configure > Task Manager > Flags.

Set flag

Task Manager can set or clear any of 16 numbered flags. A flag can only have one of two states: set or cleared. The state of a flag can be used as an input in other tasks.

Clear flag

Task Manager can set or clear any of 16 numbered flags. A flag can only have one of two states: set or cleared. The state of a flag can be used as an input in other tasks.

Toggle flag

Task Manager can set or clear any of 16 numbered flags. Toggling a set flag clears it. Toggling a cleared flag sets it. The state of a flag can be used as an input in other tasks.

Timer actions

Task Manager can start or stop timers. Before creating statements with timer actions, set up one or more timers in Configure > Task Manager > Timers.

Start timer

Task Manager can start or stop any of its 16 timers. When a timer is started, it is re-initialized, then it begins to count up from zero to the maximum set in Configure > Task Manager > Counters and Timers. When it has reached that maximum, it expires. You can create tasks that are executed when a timer expires.

Stop timer

Task Manager can start or stop any of its 16 timers. When a timer is stopped, it ceases to count up, so it does not expire. If it is re-started, it starts counting up again from 0. You can create tasks that are executed when a timer expires.

Custom alarm actions

Task Manager can raise or clear custom alarms. Before creating statements with custom alarm actions, give one or more custom alarms suitable names in Configure > Task Manager > Custom Alarms.

Raise custom alarm (nnnn)

The raise custom alarm action triggers the named alarm. Use this action to provide an alarm to a syslog collector when an external alarm activates a digital input. For more information, see "Working with Custom Alarms" on page 277.

Example

IF NOT **Digital input 01 high** THEN **Raise custom alarm (Custom Alarm 1)**

Clear custom alarm (nnnn)

Generally, each action that raises a custom alarm needs an equivalent action that clears it.

Example

IF **Digital input 01 high** THEN **Clear custom alarm (Custom Alarm 1)**

Transmit CWID now

The 'do now' action **Transmit CWID now** instructs the base station to immediately transmit the CWID message defined in the CWID form. This action enables you to configure CWID transmissions in a way that is not otherwise possible. For example, the CWID could be transmitted more than once a minute or at every transmit tail.

Transmit CWID now is not affected by the Task Manager Automatic CWID lock.

This action will transmit the CWID message regardless of whether the channel is currently being used for a call. To prevent CWID transmissions from interrupting voice, enable the automatic sending of CWIDs instead (see "Automatic CWID system" on page 153).

Sync Tx Test Actions

Task Manager can suspend or resume the Synchronized Transmission test. This enables a radio user to control the test over the air.

Suspend Sync Tx test

The Suspend Sync Tx test action suspends a synchronized transmit test. The network element stops generating test signal and behaves as if it were operating normally in Run mode, except that the test can be resumed.

Example

IF **Received NAC (296)** THEN **Suspend Sync Tx test**

Resume Sync Tx test

The Resume Sync Tx test action re-starts a synchronized transmit test that has been suspended. The network element generates the test signal and sends it to the channel group.

Example

IF **Received NAC (297)** THEN **Resume Sync Tx test**

TM Tx Key Actions

TM Tx key actions can key or unkey the transmitter. They work through a Task Manager lock which affects the TB9100 digital board's logic.

The operation of this pair of Task Manager actions can be monitored in Monitor > Task Manager > Locks. In Monitor > Interfaces > RF Interface, the transmitter status displays TM Tx Key when the base station is transmitting because of the Unlock TM Tx Key action.

Lock TM Tx Key

When the base station enters Run mode, Task Manager carries out the Lock TM Tx key action. This simply means that Task Manager does not trigger the transmitter. When the TM Tx key is locked after being unlocked, the transmitter stops transmitting, unless it has another reason for transmitting.

Example

This example gives a regular voting pulse for base stations. Timer 1 defines the interval between pulses and Timer 2 defines the length of the pulse.

IF **Network Element in Run mode** THEN **Start Timer (Timer 1)**
IF **Timer expired (Timer 1)** THEN **Unlock TM Tx Key**
IF **Timer expired (Timer 1)** THEN **Start Timer (Timer 2)**
If **Timer expired (Timer 2)** THEN **Lock TM Tx Key**
If **Timer expired (Timer 2)** THEN **Start Timer (Timer 1)**

Unlock TM Tx Key

The Unlock TM Tx key action is similar to the effect of asserting the Tx key line on a base station. It instructs the digital board to transmit, which it does as analog FM using the current signaling profile. Unlock TM Tx key cannot be used to tell the base station to transmit digital P25.

Example

This example gives a regular voting pulse for base stations. Timer 1 defines the interval between pulses and Timer 2 defines the length of the pulse.

IF **Network Element in Run mode** THEN **Start Timer (Timer 1)**
IF **Timer expired (Timer 1)** THEN **Unlock TM Tx Key**
IF **Timer expired (Timer 1)** THEN **Start Timer (Timer 2)**
If **Timer expired (Timer 2)** THEN **Lock TM Tx Key**
If **Timer expired (Timer 2)** THEN **Start Timer (Timer 1)**

Custom Actions

The Custom Actions submenu contains all the custom actions that have been defined for the network element using Configure > Task Manager > Custom Actions.

Task Manager Examples

Task Manager makes it possible for you to build complex functions into a TB9100 base station or gateway. Here are some examples, to give an idea of what can be done.

While Tait has carefully tested Task Manager, no guarantee can be given that these examples will work correctly for the system. Make sure that you thoroughly test any set of Task Manager tasks before commissioning the system.

Scanning Repeater

Task Manager makes it possible for a stand-alone TB9100 to function as a scanning repeater.

The set of Task Manager statements below works like this. When the TB9100 goes into Run mode, the ChangeChannel timer starts. When that timer stops, Task Manager instructs the TB9100 to go to the next channel in the channel table. If the TB9100 receives a call that wins the vote, it stops scanning. When the call ends, a second timer (OnChannel) is started. This timer stops the base station scanning long enough to give the called party time to respond.

IF **Network element in Run mode** THEN **Start timer (ChangeChannel)**
IF **Vote won by RF** THEN **Stop timer (ChangeChannel)**
IF **Vote won by RF** THEN **Stop timer (On Channel)**
IF NOT **Vote won by RF** THEN **Start timer (On Channel)**
IF **Timer expired (ChangeChannel)** THEN **Go to next channel**
IF **Timer expired (ChangeChannel)** THEN **Start timer (ChangeChannel)**
IF **Timer expired (On Channel)** THEN **Go to next channel**
IF **Timer expired (On Channel)** THEN **Start timer (ChangeChannel)**

Set the **ChangeChannel** timer to at least 350ms. Changing channels too quickly can put excess load on the firmware and cause it to miss its deadlines. The consequences could include the firmware protection mechanisms restarting the base station.

Give the On Channel timer a suitable value (for example, 5 seconds), to give the called party time to respond before the base station changes channel.

A small variation on this set of statements can make the base station stay on its home channel until an external signal triggers the scanning.

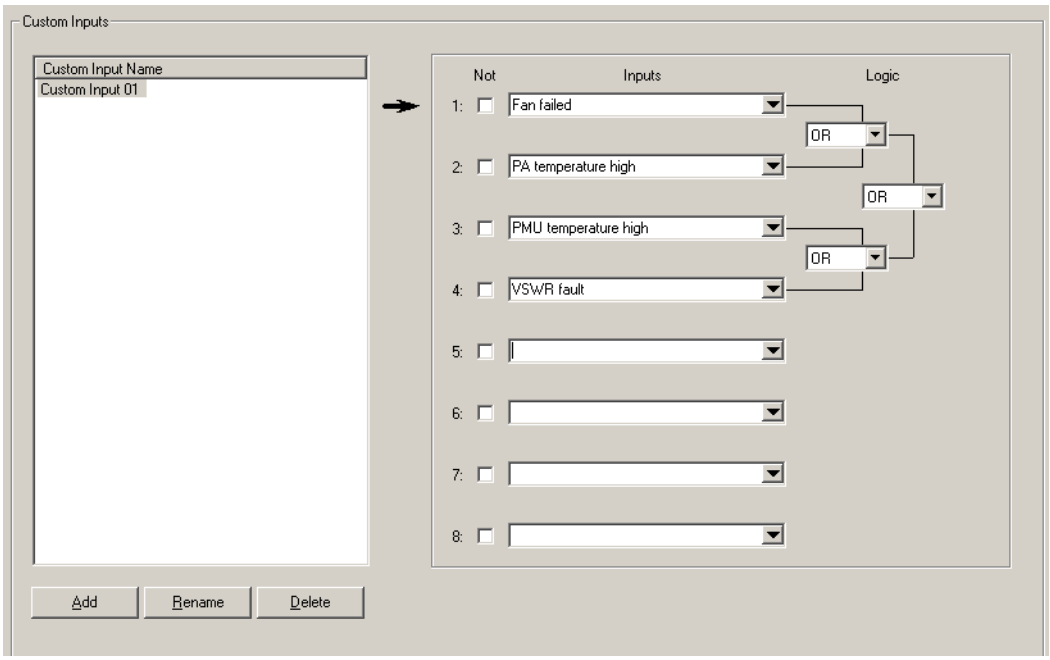
Customizing Task Manager

Customizing Task Manager adds to its power and flexibility. There are several options available. You can create custom inputs or actions and define timers, counters, and flags. You can then use them to create tasks that will be executed when the custom input becomes true, the timer expires, the counter reaches its maximum, or the flag is set.

Working With Custom Inputs

The Custom Inputs form (Configure > Task Manager > Custom Inputs) lists the existing custom inputs. Click an input to see what combination of standard inputs it consists of. You can also create new custom inputs and edit or rename existing ones.

A custom input is a user-defined Task Manager input that consists of a combination of standard inputs. Custom inputs make it possible to define tasks that will be processed when a combination of inputs becomes true. (A Task Manager task can only have one input.)



Viewing a Custom Input

1. Click an item in the Custom Input Name column.
2. View the display in the rest of the form. It shows the standard inputs used to create the custom input, whether they are negated, and the logic of their combination. The standard truth table determines the outcome for the different states of any pair. (See "Truth Table" on page 275.)

   The Logic column shows graphically how the standard inputs will be combined. First the input is negated, if its Not check box is selected. Then it is combined with the adjacent input to which it is joined by a line. The result of that combinatorial operation is combined with the input or result that it is joined to, and so on, until the final result is obtained. In this way,

up to eight standard inputs can be combined to produce an input that can only be true or false.

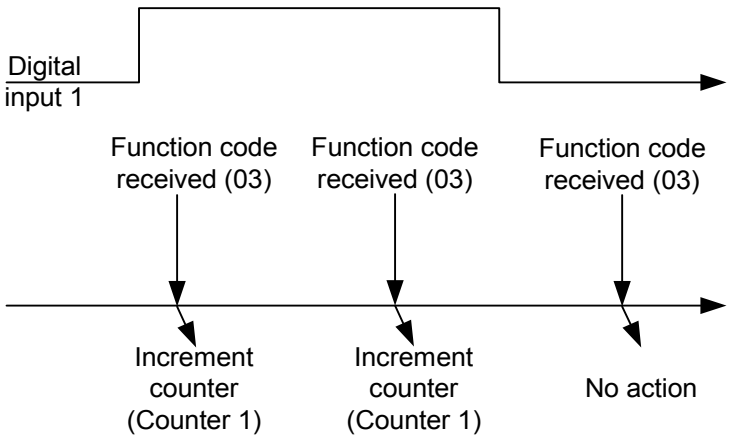
Defining a Custom Input

1. Click **Add**.
2. Edit the name that appears in the Custom Input Name column.
3. Click in an **Input** box and select an input from the list.
4. If you want the negative of the input to contribute to the custom input's logic, select the **Not** check box alongside.
5. Repeat steps 3 and 4 for all the standard inputs that will go to make up the custom input. The Input boxes that you choose will determine the order in which the standard inputs are combined.
6. Under the **Logic** heading, select the appropriate options in the drop-down boxes to give the desired logical combination of inputs. (For information about the effect of the different options, see "Truth Table" on page 275.)
7. Check that type of inputs that you are combining makes sense. For example, do not combine two event inputs with an AND. See "Combining Inputs in a Custom Input" on page 274.
8. Click **OK**.

Combining Inputs in a Custom Input

State input and event input

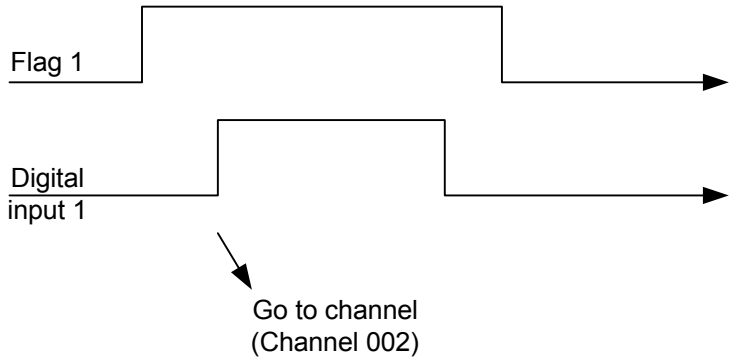
You can combine a state input with an event input using AND. The action will be triggered if the state input has the desired state when the event occurs. The following example shows what happens with a custom input that combines the state input **Digital input high** with the event input **Function code received**.



You can use IF NOT with the custom input, but not with its event input.

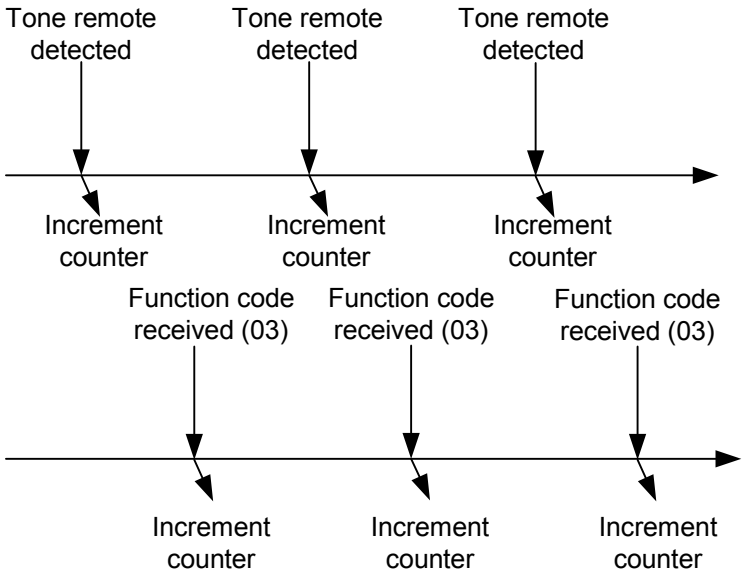
State input and state input

You can combine two state inputs using AND. The action will be triggered when one input has the desired state when the other input changes to the desired state. In the example below, Flag 1 is set, and the action is triggered when digital input 1 goes high.



Event input and event input

You can combine two event inputs using OR. The action will be triggered when either event input occurs. In the example below, a tone remote function tone or a function code triggers the action.



Truth Table

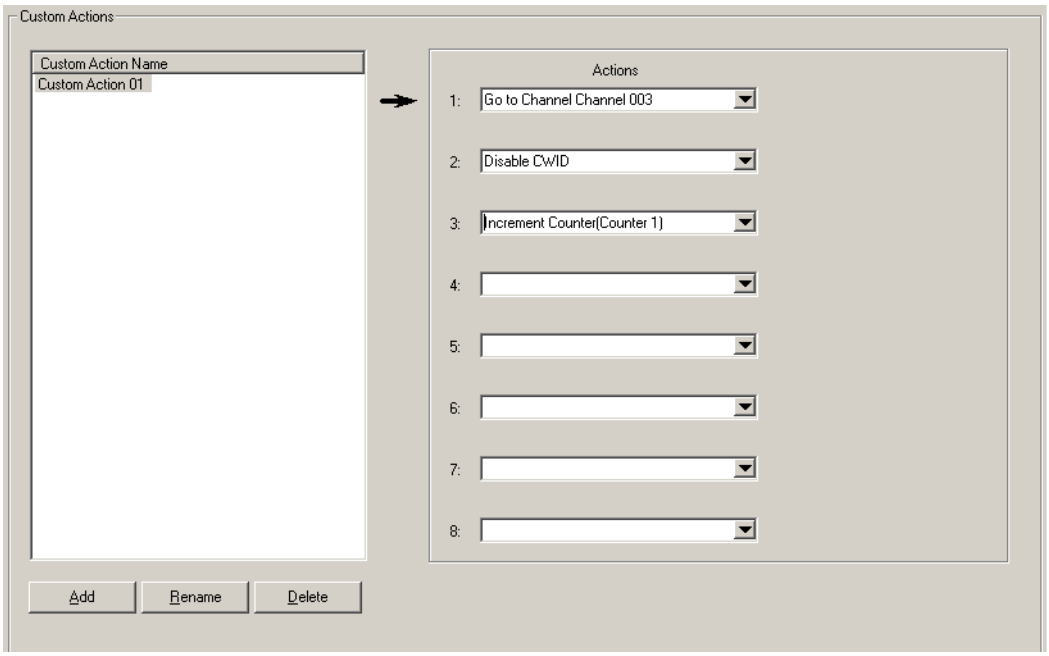
The truth table below displays the possible individual values for input A and input B, and the result when you combine those values using each of the six available logic operators. So, for example, if A is true and B is false and we combine A and B using XOR, the result is true.

A	B	AND	NAND	XOR	XNOR	OR	NOR
false	false	false	true	false	true	false	true
false	true	false	true	true	false	true	false
true	false	false	true	true	false	true	false
true	true	true	false	false	true	true	false

Working With Custom Actions

The Custom Actions form (Configure > Task Manager > Custom Actions) displays the list of existing custom actions. Click a custom action to see what combination of standard actions it consists of. You can also create new custom actions and edit or rename existing ones.

A custom action is a user-defined Task Manager action that consists of more than one standard action. It saves you writing several different tasks with the same input.



Viewing a Custom Action

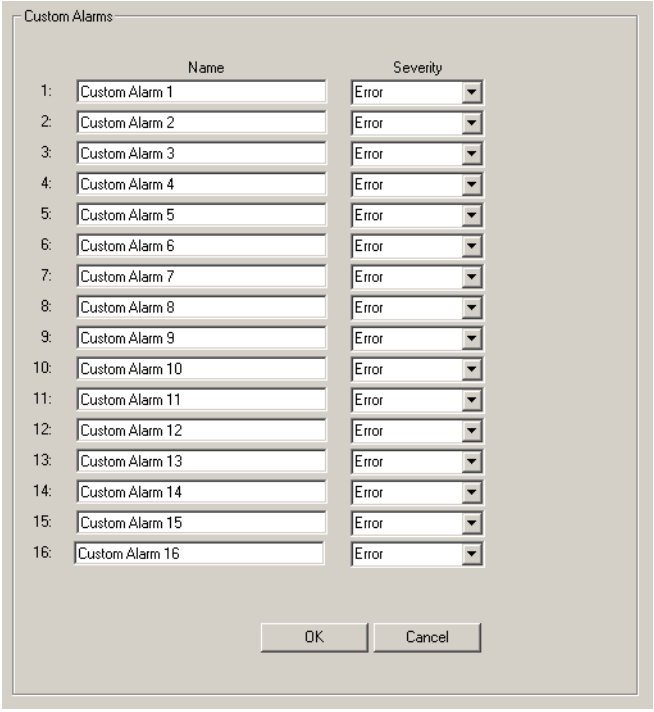
1. Click an item in the Custom Action Name column.
2. View the Actions column. It lists the standard actions that the custom action consists of.

Defining a Custom Action

1. Click **New**.
2. Edit the name that appears in the Custom Action Name column.
3. Click in the first row of the Actions column and select an action from the list.
4. Repeat step 3 for all the standard actions that will go to make up the custom action.
5. Click **OK**.

Working with Custom Alarms

The Custom Alarms form (Configure > Task Manager > Custom Alarms) displays the number, name, and severity level of the available custom alarms.



You can rename any of the available alarms to provide a more meaningful name such as 'Door open.' Assign a severity level appropriate to the alarm, making sure that it is higher than the logging level so that it will be sent to the syslog collector.

Custom alarms are needed to provide an alarm when an external event activates a digital input. They can be triggered by any event that changes a Task Manager input.

To set up a custom alarm, define a Task Manager task with any input and **Raise custom alarm** as the action. You probably also need to define another task with the action **Clear custom alarm**. When the input of the first task becomes true, the alarm is triggered. Custom alarms can be sent to a syslog collector. Unlike other alarms, they cannot be inputs to Task Manager and cannot be disabled. They do not cause the control panel alarm LED to flash.

Defining Counters, Timers, and Flags

Counters, timers, and flags make it possible for Task Manager to do such things as respond to three presses of PTT or to email a status message once a week.

Short timers may not be accurate. This is because it may take Task Manager longer than 10ms to process its tasks, causing it to miss the next instruction to go through its task list. We recommend that you avoid short timers (< 50ms) if the task list has more than 10 enabled tasks.

To define a counter

1. Select Configure > Task Manager > Counters.
2. If desired, enter a suitable name for the counter into the **Name** box.

3. In the **Maximum** box, enter the highest number that the counter can reach.

   When the counter reaches its maximum, the input **Counter at maximum** becomes true for that counter and any tasks containing it are processed.

To define a timer

1. Select Configure > Task Manager > Timers.
2. If desired, enter a suitable name for the timer into the **Name** box.
3. In the **Units** box, specify the unit of time for the entered number.

   When the timer reaches its maximum, the input Timer expired becomes true for that timer and any tasks containing it are processed.

To define a flag

1. Select Configure > Task Manager > Flags.
2. If desired, enter a suitable name for the flag into the **Name** box.
3. Click **OK**.

Monitoring Task Manager

The items under Monitor > Task Manager provide options for monitoring Task Manager. If the network element is behaving unexpectedly, check to see whether Task Manager has locked any functions. Alternatively, have a look at the system log; it records any actions that Task Manager carries out. You can also view the current state of timers, counter, and flags.

Viewing Locks

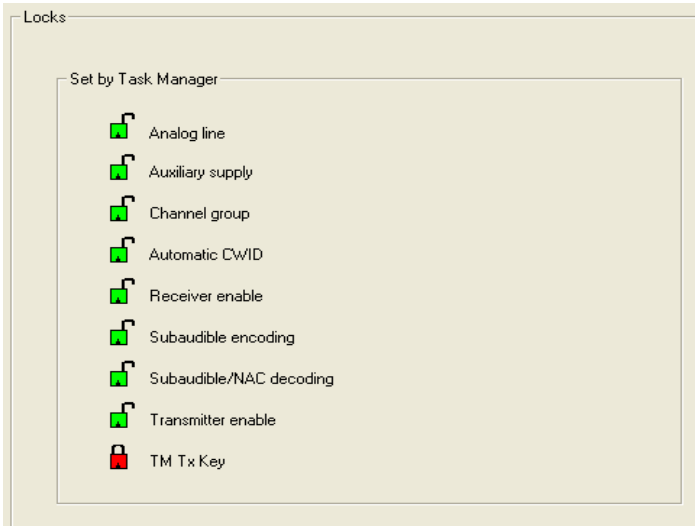
The Locks form (Monitor > Task Manager > Locks) shows whether Task Manager has locked any functions.

If the function is locked, the form displays a red locked padlock.

If the function is unlocked, the form displays a green open padlock.

When the network element enters or re-enters Run mode, all functions (except for TM Tx Key) are unlocked. A function can only be locked through Task Manager action.

The Locks form is an important place to check, if the network element is not behaving as expected.



Analog line — When the analog line is locked, the analog line cannot be used.

Auxiliary supply — Locking or unlocking the auxiliary supply only has an effect if the auxiliary supply is configured to be under the control of Task Manager (Configure > Network Element > Miscellaneous). In this case, when the auxiliary supply is locked, the auxiliary power output is turned off. When the auxiliary supply is unlocked, it is turned back on and supplies power.

Channel group — When the channel group is locked, the network element cannot input or output a voice stream over its digital line. It also cannot receive function codes.

Automatic CWID — When automatic CWID is locked, the base station cannot automatically transmit a continuous wave ID (Morse code). However, Task Manager can still initiate the sending of the CWID using the action **Transmit CWID now**.

Receiver enable	When the receiver is locked, it is unable to pass any received audio.
Subaudible encode	When the encoding of subaudible signaling is locked, subaudible signaling is not added to the transmitted signal. (The encoding of the NAC cannot be locked.)
Subaudible/NAC decode	When the decoding of subaudible signaling and the NAC is locked, subaudible signaling and the NAC are not decoded, which means that the receiver unmutes to any CTCSS tone, DCS code, or NAC.
Transmitter enable	When the transmitter is locked, it is unable to transmit.
TM Tx key	When Task Manager unlocks TM Tx key, it keys up the transmitter. When TM Tx key is locked, transmitter operation is normal.

Viewing Counters

The Counters form (Monitor > Task Manager > Counters) displays the current state of any counters configured for Task Manager.

The Name column lists the counters. A bar graph shows how far each counter has progressed towards its maximum value, which is displayed in the Maximum column.

Viewing Flag States

The Flags form (Monitor > Task Manager > Flags) displays the current state of any custom flags configured for Task Manager.

Each of the possible flags has an LED alongside it. A flashing red LED means that the flag is set. A green LED means that is is cleared.

Viewing Timers

The Timers form (Monitor > Task Manager > Timers) displays the current state of any timers configured for Task Manager.

The Name column lists the timers. A bar graph shows how far each timer has progressed towards its maximum value, which is displayed in the Maximum column.

Viewing Custom Alarms

The Custom Alarms form (Monitor > Task Manager > Custom Alarms) displays the current state of all custom alarms. If an alarm has been triggered, its LED turns green (not red as one might expect). If an alarm is cleared or not used, its LED is gray.

Glossary

This glossary contains an alphabetical list of terms and abbreviations related to the TaitNet P25 network, the CSS, the TB9100 base station, the console gateway, and the trunked analog gateway.

A

access code A password required to gain access to a set of privileges.

ADC Analog-to-Digital Converter. A device for converting an analog signal to a digital signal that represents the same information.

administrator A special type of access to CSS functions, used for activities such as changing passwords.

AES AES (Advanced Encryption Standard) is an encryption algorithm that uses keys of up to 256 bits.

AGC Automatic Gain Control. A device that optimizes signal level.

Algorithm ID The Algorithm ID is an identifier that specifies an encryption algorithm (for example, DES or AES).

analog FM Analog FM is a mode of operation in which the RF interface transmits and receives analog FM signal. The network element's channel group interface sends and receives the analog signal as G. 711 speech packets.

analog valid Analog valid is a signal that indicates that the TB9100 base station or gateway is presenting a valid output on the analog line. This output can originate from an analog FM or from a digital P25 call. The M-line carries the analog valid signal.

ANI Automatic Number Identification. A service that provides the receiver of a call with a numerical identifier or alphanumeric label of the caller.

antenna relay A DC-powered device that switches the antenna as needed between the base station's receiver and transmitter. With an antenna relay, a simplex base station only needs one antenna.

APCO The Association of Public Safety Communications Officials in the United States. The APCO Project 25 standards committee defined the P25 digital radio standard. The standard is often referred to as APCO or P25.

ARP ARP (Address Resolution Protocol) is a IP protocol used to map IP network addresses to the hardware addresses used by a data link protocol.

B

Base station A radio receiver and transmitter that is located in a specific place (at a site) that enables a two-way radio to communicate with a dispatcher or over a larger range with other two-way radios. Specifically, Tait TB9100 equipment in a subrack.

Battery protection mode A PMU enters battery protection mode when it has AC power but its DC power is below the configured power shutdown voltage. In battery protection mode, the PMU will shut down to protect the battery if it loses AC power.

BCD BCD (binary coded decimal) is a code in which a string of four binary digits represents a decimal number.

bearer network Telecom equipment that is used to carry user data.

BER Bit Error Rate. A measure of the quality of digital transmission, expressed as a percentage. The BER indicates the proportion of errors to correctly received digits in a received signal.

C

C4FM Compatible Four-level Frequency Modulation. A modulation scheme defined in the P25 CAI standard for 12.5 kHz bandwidth.

CAI Common Air Interface. The over-the-air data formats and protocols defined by the APCO P25 committee.

Calibration Software The Calibration Software is a utility for defining the switching ranges of the receiver and the exciter and for flattening the receiver response across its switching range. It can also be used to calibrate modules.

call A call is a complete exchange of information between two or more parties. A call requires a receive signal path and a transmit signal path. In trunked systems, a call may be a conversation, made up of a number of overs, but in conventional systems, a call is a single over.

calling profile A group of configuration settings that defines the properties of the TB9100 analog line, which can be regarded as equivalent to a SU on the network.

central voting Voting that is centralized at one member of the channel group.

channel A channel is: 1. A path through which signals can flow. 2. In the RF domain, a frequency pair (or just a single frequency in a simplex system). 3. A set of configuration information that defines the frequency pair and other related settings (a channel configuration). 'Channel' has this meaning in the CSS.

channel coordinator A software module within the reciter or gateway module that propagates dispatcher channel control commands to the channel group. The channel coordinator also ensures that all channel group members have consistent states so that they work together properly.

channel group A channel group is a single logical channel consisting of a set of base stations. P25 console gateways can also be members. The members of a channel group are linked by an IP network and share a common multicast IP address.

channel module Channel module is a common term used to refer to reciters and gateway modules. TB9100 base stations have reciters and gateways have gateway modules.

channel profile A channel profile is a named group of configuration settings that help to define the properties of a channel. Each channel in the channel table must have a channel profile assigned to it.

channel seize Channel seize is a signal received at the analog line interface, requesting the base station or gateway to accept the signal on the analog line as an input into the channel group. An asserted E-line, LLGT, or LLGT following MDC1200 signaling can function as a channel seize signal.

channel spacing Channel spacing is the bandwidth that a channel nominally occupies. If a TB9100 base station has a channel spacing of 12.5 kHz, there must be a separation of at least 12.5 kHz between its operating frequencies and those of any other equipment.

channel table The channel table is the base station's database of channel configurations.

circuit domain The part of the base station processing functionality that processes speech signal as a continuous stream of bits – a digital circuit. The opposite of packet domain.

CKR The CKR (common key reference) is a number used by the key fill device and by the CSS to indirectly refer to an encryption key without using its Key ID or Algorithm ID.

CODEC A device which combines analog-to-digital conversion (coding) and digital-to-analog conversion (decoding).

community repeater Repeater that is shared by several user groups.

configuration file A configuration file consists of all the configuration settings needed for a TB9100 base station or gateway, stored as a file in the configurations folder. Configuration files have the extension *.apc.

connection list A connection list contains the names and IP addresses of base stations and gateways that the CSS can connect to.

control bus The control bus is used for communications between modules in a subrack. It is an I2C bus, a bi-directional two-wire serial bus which is used to connect integrated circuits (ICs). I2C is a multi-master bus, which means that multiple chips can be connected to the same bus, and each one can act as a master by initiating a data transfer.

control panel The control panel is an area at the front of the base station or gateway with buttons, LEDs and other controls that let a maintainer interact with the network element.

conventional network Conventional networks are systems that do not have centralized management of channel access. System operation is entirely controlled by system end users.

CRTP Compressed RTP.

crypto module Module for securely storing encryption keys and for encrypting and decrypting signals.

CSM Constant-envelope Simulcast Modulation. A modulation scheme designed for simulcast that can be used by non-linear transmitters.

CSS Customer Service Software. Tait PC-based software for monitoring, configuring, and diagnosing a Tait TB9100 base station, P25 console gateway, or P25 trunked analog gateway.

CSSI interface The Console Subsystem Interface is a P25 standard interface that connects dispatch equipment to a trunked network.

CTCSS CTCSS (continuous tone controlled squelch system), also known as PL (private line) is a type of signaling that uses subaudible tones to segregate groups of users.

custom action A custom action is a user-defined Task Manager action that consists of more than one pre-defined action.

custom input A custom input is a user-defined Task Manager input that consists of a set of pre-defined inputs that are combined using Boolean logic.

CWID CWID (Continuous Wave IDentification) is a method of automatically identifying the base station using a Morse code. Continuous wave means transmission of a signal with a single frequency that is either on or off, as opposed to a modulated carrier.

D

DAC Digital-to-Analog Converter. A device for converting a digital signal to an analog signal that represents the same information.

data gateway In a P25 conventional network, a data gateway provides a data connection between applications running on the customer's IP network and mobile data applications.

DCS DCS (digital coded squelch), also known as DPL (digital private line), is a type of subaudible signaling used for segregating groups of users. DCS codes are identified by a three-digit octal number, which forms part of the continuously repeating codeword. When assigning DCS signaling for a channel, you specify the three-digit code.

DDC Digital Down Converter. A device which converts the digitized IF signal of the receiver down to a lower frequency (complex baseband) to suit the DSP.

de-emphasis De-emphasis is a process in the receiver that restores pre-emphasized audio to its original relative proportions.

DES DES (Data Encryption Standard) is an encryption algorithm selected by the P25 standard.

DFSI The Digital Fixed Station Interface connects digital dispatch equipment with a channel group or base station. It is defined in the Project 25 TIA standard.

digital input value A value that the TB9100 base station computes from the state of a configured number of digital inputs. The digital input value is an input into Task Manager.

digital P25 Digital P25 is a mode of operation in which the RF interface transmits and receives digital signal as defined by the APCO P25 CAI. The digital line sends and receives IMBE speech packets.

dispatcher A dispatcher is a person who gives official instructions by radio to one or more SU users.

distributed voting Voting for the best RF signal that is carried out separately by each channel group member using the same voting algorithm. It is not supported and only occurs if a central voter is not available.

dotted quad A method for writing IPv4 addresses. The form is DDD.DDD.DDD.DDD where DDD is an 8-bit decimal number.

downlink The transmission path from fixed equipment to SUs.

DSCP Differentiated Services Code Point. A field in the header of IP packets that is used to indicate to routers and switches the quality of service that should be provided.

DSP Digital Signal Processor.

dual mode The ability to operate as a transceiver in two different ways: analog FM and P25 digital. Dual mode equipment can be configured to support either mode or to switch between modes from one over to another.

duplex Providing transmission and reception in both directions simultaneously.

duty cycle Duty cycle is used in relation to the PA. It is the proportion of time (expressed as a percentage) during which the PA is transmitting.

E

E & M A pair of wires used for DC signaling. For example, the signal to set up a call is often sent from the 'M' (mouth) end of a wire to the other 'E' (ear) end by grounding the wire.

EIA Electronic Industries Alliance. Accredited by the American National Standards Institute (ANSI) and responsible for developing telecommunications and electronics standards in the USA.

EMC Electromagnetic Compatibility. The ability of equipment to operate in its electromagnetic environment without creating interference with other devices.

encryption The coding of voice (or data) into unintelligible forms for secure transmission.

ETSI European Telecommunications Standards Institute. The non-profit organization responsible for producing European telecommunications standards.

F

failsoft mode Failsoft mode is an optional operational mode in trunked networks. It comes into effect when the channel group loses all connection to the trunking site controller.

FCC Federal Communications Commission. The FCC is an independent United States government agency that regulates interstate and international radio communications.

Feature Code Code that identifies a software feature license that can be enabled or disabled using the Software Feature Enabler.

Feature Code Sequence Number Number that indicates how many times a software feature license has been enabled or disabled.

Feature license key A set of digits purchased from Tait that is required to enable a software feature license.

FEC Forward Error Correction. A method of encoding data so that the receiving end is able to correct transmission errors.

FFSK Fast Frequency Shift Keying. A modem encoding scheme for carrying data on FM radios.

fill-in receiver An additional receiver placed within the coverage area of a TB9100 base station to receive SU transmissions that are too weak to be received by that base station.

flag A flag is a programming term for a "yes/no" indicator used to represent the current status of something. The network element has a set of flags that Task Manager can set and clear.

FLASH Electrically block erasable and programmable read-only memory.

FM Frequency Modulation. Often used as an adjective to denote analog radio transmission.

frequency band The range of frequencies that the equipment is capable of operating on.

front panel The cover over the front of the TB9100 base station containing fans for the PA and PMU.

FSH Fixed Station Host.

function code A value that Task Manager can send to the channel group that can serve as an input to Task Manager actions at other channel group members.

G

G. 711 The name of the ITU standard that defines how speech is digitally encoded (64 kbit, A-law or u-law). When the TB9100 base station is in analog FM mode, G. 711 speech is sent and received on the channel group interface.

gating Gating is the process of opening and closing the receiver gate. When a valid signal is received, the receiver gate opens, letting the signal through.

group call A group call is a call that is sent to more than one SUs simultaneously.

H

heartbeat message A message whose purpose is to indicate to the receiver that the sender is operational.

hiccup mode Many power supplies switch off in the event of a short-circuit and try to start again after a short time (usually after a few seconds). This "hiccup"-type of switching off and on is repeated until the problem is eliminated.

HLGT High level guard tone. A tone that announces the beginning of tone remote signaling.

holdover mode A simulcast base station can enter holdover mode when it loses its 1?PPS pulse. Holdover mode temporarily maintains synchronization by phase-locking the transmit clock to the external frequency reference.

hostname The unique name by which a network element is known on the network.

hub A unit for connecting hosts together. It sends all incoming Ethernet packets to all the other hosts.

hysteresis Hysteresis is the difference between the upper and lower trigger points. For example, the receiver unmutes when the upper trigger point is reached, but will mute again until the level falls to the lower trigger point. An adequate hysteresis prevents the receiver gate from repeatedly muting and unmuting when the level varies around the trigger point.

I

IMBE Improved Multiband Excitation. A voice compression technology patented by Digital Voice Systems, Inc and used in the vocoders of P25 radios.

IMG ISSI Media Gateway.

impairment A measure of signal quality used in channel group voting. Impairment is inversely related to signal quality. The lowest impairment (0) indicates the highest signal quality. The highest impairment (15) indicates the worst signal quality.

inbound Inbound describes the direction of a signal: from a subscriber unit over the air interface to the fixed station.

inhibit A control command that can be sent across the CAI to inhibit a SU. An inhibited SU appears to the user as if it is powered off.

IP Internet Protocol. IP is a protocol for sending data packets between hosts.

isolator An isolator is a passive two-port device which transmits power in one direction, and absorbs power in the other direction. It is used in a PA to prevent damage to the RF circuitry from high reverse power.

K

kernel The kernel is the core executable of an operating system.

key fill device A device such as a Motorola KVL3000+ for defining encryption keys and transferring them into P25 equipment.

key ID The Key ID is the identifier for an encryption key variable.

key variable The key variable is a parameter used by the encryption algorithm to encrypt or decrypt a message.

keytone A signaling tone that accompanies voice on the analog line and is used to key the transmitter. Also referred to as LLGT.

L

LAN Local Area Network

LDU Link Data Unit. Voice calls are sent over the CAI as a series of LDUs.

LED Light Emitting Diode. Also the screen representation of a physical LED.

LLGT Low level guard tone. One of a set of tones used to remotely control base stations.

M

marshalling duration The marshalling duration is the length of time that the voice stream needs to travel from the central voter to the furthest channel group member. The fixed marshalling duration parameter includes the time needed to fill the transmit buffer to the required level.

master The channel group master is the member with the control connection to the trunking site controller.

MDC1200 MDC1200 is a proprietary signaling protocol developed by Motorola and used in analog PMR to provide subscriber signaling.

MER Message Error Rate. MER is used to measure the quality of the signal received from trunked control channels. It is the percentage of TSBKs that cannot be decoded.

Mobile IP Mobile IP is a standard communications protocol that enables mobile devices to communicate using the same home IP address, while roaming around the Internet.

monitor function The Monitor function unmutes the receiver, so that the user can hear all traffic on a channel.

multicast group The group of hosts associated with a specific IP multicast address.

multicast IP address An IP address that refers to a group of hosts rather than a single host. These hosts will all accept packets with this IP address.

mute A mute prevents audio from being passed to the radio's speaker.

N

NAC Network Access Code. The 12 most significant bits of the network identifier information that precedes every packet sent on the CAI. The NAC identifies which network the data belongs to, allowing base stations and mobiles to ignore packets belonging to interfering networks.

NAT NAT (network address translation) allows the use of a single IP address for a whole network of computers. A NAT sits between the public Internet and the network it serves, and works by rewriting IP addresses and port numbers in IP headers on the fly so the packets all appear to be coming from (or going to) the single public IP address of the NAT device instead of the actual source or destination.

navigation pane The navigation pane is the left-hand pane of the CSS application window. It displays a hierarchical list of items. When you click an item, the main pane displays the corresponding form.

network element A network element is any device that is network-connected. A TaitNet digital network consists of a number of network elements. The TB9100 base station, the console gateway, and the trunked analog gateway are network elements designed and manufactured by Tait.

Non-DLI OTAR OTAR messaging is of two types: DLI OTAR and non-DLI OTAR (non-data link independent OTAR). The data gateway uses non-DLI OTAR over the CAI. Non-DLI OTAR communicates using the data link layer (layer 2). It does not use IP to address OTAR messages.

normal squelch A type of squelch operation in which the receiver unmutes on any signal with the correct NAC (digital P25) or subaudible signaling (analog FM).

O

octet A set of 8 bits.

OTAR Over-the-air rekeying. The protocol used by KMF and by radios for encryption key management.

outbound Outbound describes the direction of a signal: from a fixed station over the air interface to a SU.

P

P25 Project 25. A suite of standards and requirements endorsed by the TIA and intended for digital public safety radio communications systems.

P25 console gateway A Tait network element that acts as a gateway between an analog dispatch console and a channel group.

PA The PA (power amplifier) is a TB9100 base station module that boosts the exciter output to the required transmit level.

packet domain The speech processing area that deals with speech data that has been collected up into a packet. IP networks convey packets. The opposite of circuit domain.

PCB Printed Circuit Board

PMU The PMU (power management unit) is a module in the TB9100 base station that provides power to the subrack and monitors power conditions. Gateways can also have a PMU.

preamble The preamble is a well-defined signal that is transmitted at the beginning of digital P25 calls to facilitate downlink voting and to allow the transmit buffer to fill.

pre-emphasis Pre-emphasis is a process in the transmitter that boosts higher audio frequencies to improve the audio quality.

privileged RFSS A privileged RFSS is one to which the trunked analog gateway interfaces using the Airbus DS proprietary protocols GCT and RVP alongside a subset of the standard CSSI interface. In a privileged RFSS, group calls use a multicast IP address for distributing the voice stream.

privileges A set of access rights to CSS functions. There are Guest, Maintainer, and Administrator privileges.

program The act of sending a configuration data set from the CSS to the TB9100 base station or gateway.

Project 25 A project set up by APCO (the Association of Public Safety Communications Officials International), together with other US governmental organizations, to develop standards for interoperable digital radios to meet the needs of public safety users.

PSTN Public Switched Telephone Network: The public telephone network.

PTT Push To Talk. The button on a SU that keys the transmitter.

Q

QoS Quality Of Service. A router feature that gives real-time data such as voice calls priority over other data.

R

receiver number A unique number assigned to the members of a channel group and used by the DFSI interface.

reciter The reciter is a module of a TB9100 base station that provides both receiver and exciter functionality.

repeater talkaround Repeater talkaround allows the SU user to bypass repeater operation and so communicate directly with other SUs. While repeater talkaround is active, all transmissions are made on the receive frequency programmed for the channel.

reverse tone burst Reverse tone bursts can be used with CTCSS. When reverse tone bursts are enabled, the phase of the generated tones is reversed for a number of cycles just before transmission ceases. If the receiver is configured for reverse tone burst, it responds by closing its gate.

RFSS controller An RFSS controller is an application running on a Sun NETRA computer that provides the overall control of a Tait P25 trunked network.

RISC Reduced instruction set computer. A type of microprocessor that recognizes a relatively limited number of instructions. The reciter's digital board and network board both have RISC microprocessors.

router A router is an internetwork packet switch that switches data packets from an input interface to an output interface. The interfaces can be of different types.

RS-232 A protocol for serial communications between DTE (data terminal equipment) and DCE (data communications equipment).

RSSI RSSI (Received Signal Strength Indicator) is a level that indicates the strength of the received signal.

RTP RTP (Real Time Protocol) is an Internet protocol that supports the real-time transmission of voice and data.

Run mode Run mode is the normal operating mode of the TB9100 base station or gateway.

RVP RFSS Voice Protocol. A proprietary protocol that uses multicast IP to send digitized voice to the FNE destinations within the network.

Rx Receiver.

S

SAP Service Access Point. In packet data, the SAP is a number that tells the SU which application the data is intended for. The SAP and the SUID are the CAI equivalent of the port number and IP address in IP data.

satellite voter A channel group member that has delegated voting activity to a central voter.

SAW filter Surface Acoustic Wave filter. A band pass filter that can be used to filter both RF and IF frequencies. A SAW filter uses the piezoelectric effect to turn the input signal into vibrations that are turned back into electrical signals in the desired frequency range.

selective squelch A type of squelch operation in which the receiver unmutes only on signals that are explicitly addressed to that receiver. This can be done through a talk group ID or unit ID (digital P25) or through MDC1200 signaling (analog FM).

selectivity The ability of a radio receiver to select the wanted signal and reject unwanted signals on adjacent channels (expressed as a ratio).

sensitivity The sensitivity of a radio receiver is the minimum input signal strength required to provide a usable signal.

signaling profile A signaling profile is a named set of configuration items related to signaling that can be applied to any channel. Items include subaudible signaling and transmit timers.

simplex Able to provide transmission and reception only in one direction at a time.

simulcast Simulcast is the simultaneous broadcast by more than one transmitter of the same signal on the same frequency.

SINAD SINAD (Signal plus Noise and Distortion) is a measure of signal quality. It is the ratio of (signal + noise + distortion) to (noise + distortion). A SINAD of 12 dB corresponds to a signal to noise ratio of 4:1.

site 1. The base station equipment at a particular location. This includes power supplies, transmitters, receivers, network interfaces and controllers. 2. The location of that equipment.

site controller Equipment in a trunked network that controls the base stations belonging to a site.

skew

Skew is a measure used in centrally voted channel groups. If a voice stream arrives at the central voter 20?ms later than the first voice stream from the same SU, it is said to have a skew of 20?ms.

SMR

Specialized Mobile Radio. A communications system used by police, ambulances, taxis, trucks and other delivery vehicles.

SNMP

Simple Network Management Protocol. A protocol used (for example) by the trunking site controller to monitor the status of the channel group and its members.

squelch

Squelch is a feature of radio equipment. It ensures that the speaker only unmutes when a valid signal is received. To be valid, it must, for example, have the correct NAC.

SSRC

Synchronization source. The SSRC is a large number specified by the trunking controller in its connection message. It uniquely identifies voice streams sent from the master base station.

Standby mode

Standby mode is a mode of operation in which active service is suspended so that special operations can be carried out, such as programming in a new configuration or carrying out invasive diagnostic tests.

SU

Abbreviation for subscriber unit. This is the term used in the APCO P25 standard documents for a two-way radio (generally a mobile or a portable radio) conforming to the CAI specifications.

subaudible signaling

Subaudible signaling is signaling that is at the bottom end of the range of audible frequencies. The TB9100 base station supports CTCSS and DCS subaudible signaling.

subtone

A subtone (subaudible signaling tone) is a CTCSS tone or a DCS code.

supplementary service

A term used in the P25 standards. It refers to a group of services that is additional to the basic service that a telecommunications network provides. Examples include encryption and SU monitoring.

switching range

The switching range is the range of frequencies (about 10 MHz) that the radio equipment is tuned to operate on. This is a subset of the equipment's frequency band.

syslog collector

A program that can receive, display, and log syslog messages from many devices.

syslog protocol

syslog is a standard protocol used for the transmission of event notification messages across IP networks. TB9100 base stations and gateways can send messages such as alarms to an IP address on the TaitNet P25 digital network. Their logs store messages in the syslog format.

T

TaitNet — TaitNet is the brand name for any PMR network designed and manufactured by Tait.

TaitNet P25 network — A set of Tait base stations interconnected by an IP network that can carry voice and data traffic.

Task action — A task action is the second part of a Task Manager task. It specifies what the network element must do when the first part (the input) becomes true.

Task input — A task input is the first part of a Task Manager task. It specifies what must become true before the network element carries out the second part.

Task Manager — Task Manager is a part of the network element firmware that carries out tasks in response to inputs. These tasks are formulated using the CSS.

TB9100 base station — A P25-compliant base station consisting of the equipment necessary to receive and transmit on one channel. Generally, this means a reciter, a PA, and a PMU. Often abbreviated to TB9100 or base station.

TCCP — Trunking Channel Control Protocol. A proprietary protocol operating over IP for the exchange of channel control messages between a TB9100 base station and a trunking site controller.

TCP — Transmission Control Protocol. A complex protocol on top of IP for sending reliable streams of data with flow control.

TELCO — Telephone company.

TIA — Telecommunications Industry Association

toggle — The term toggle is used to describe the switching between two states. If something is on, toggling it turns it off. If it is off, toggling it turns it on.

tone — A tone is a sound wave of a particular frequency.

tone remote function tone — An audio tone used for signaling to a TB9100 base station or gateway on the analog line.

trunking site controller — Equipment that controls the base stations belonging to a site.

TSBK — A TSBK (trunking signaling block) is an over-the-air message format used in digital P25 mode for setting up trunked calls and for supplementary services such as messaging and status updates.

Tx — Transmitter.

U

UDP User Datagram Protocol. A simple protocol on top of IP for sending streams of data.

uninhibit A control command that can be sent across the CAI to restore an inhibited SU to normal functioning.

uplink The transmission path from SUs to fixed equipment.

UTC Coordinated Universal Time (word order from French). An international time standard that has replaced Greenwich Mean Time.

V

valid signal A valid signal is a signal that the receiver unmutes to. A signal is valid, for example, when it is strong enough to be decoded and when it has the specified NAC.

vocoder Voice encoder/decoder. A processing element that compresses/decompresses the digital voice signal.

voice over A voice over is a single transmission, which begins when a user presses PTT and ends when the user stops pressing.

voice stream A digitized voice signal that passes through the main switch.

VoIP Voice over IP. The name for the technology that puts speech signals in packets and then routes them over an IP backbone network.

voting Voting is the systematic sampling of a group of channels for the channel with the greatest signal strength. Voting provides wide-area coverage and ensures that as the user moves throughout the coverage area the strongest channel is always available for a call.

VPN Virtual private network. A private communications network used to communicate confidentially over a non-private network.

VSWR Voltage Standing Wave Ratio (VSWR) is the ratio of the maximum peak voltage anywhere on the transmission line to the minimum value anywhere on the transmission line. A perfectly matched line has a VSWR of 1:1. A high ratio indicates that the antenna subsystem is poorly matched.

W

watchdog A watchdog circuit checks that the system is still responding. If the system does not respond (because the firmware has locked up), the circuit generally resets the system.

whitelist In conventional packet data, the whitelist indicates which SUs are permitted to access packet data services. An SU that is not on the whitelist is not allowed to register with a data gateway.

Z

zeroize To zeroize one or more encryption keys is to render them useless by overwriting the key data with zeros.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Tait General Software Licence Agreement

This Software License Agreement ("Agreement") is between you (“Licensee”) and Tait Limited (“Tait").
By using any of the Software items embedded and pre-loaded in the related Tait Designated Product, included on CD, downloaded from the Tait website, or provided in any other form, you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, do not install or use any of the Software. If you install or use any of the Software, that will be deemed to be acceptance of the terms of this Agreement.
For good and valuable consideration, the parties agree as follows:

Section 1 DEFINITIONS

“Confidential Information” means all or any information supplied to or received by Licensee from Tait, whether before or after installation or use and whether directly or indirectly pertaining to the Software and Documentation supplied by Tait, including without limitation all information relating to the Designated Products, hardware, software; copyright, design registrations, trademarks; operations, processes, and related business affairs of Tait; and including any other goods or property supplied by Tait to Licensee pursuant to the terms of this Agreement.
“Designated Products” means products provided by Tait to Licensee with which or for which the Software and Documentation is licensed for use.
“Documentation” means product and software documentation that specifies technical and performance features and capabilities; user, operation, and training manuals for the Software; and all physical or electronic media upon which such information is provided.
“Executable Code” means Software in a form that can be run in a computer and typically refers to machine language, which is comprised of native instructions the computer carries out in hardware. Executable code may also refer to programs written in interpreted languages that require additional software to actually execute.
“Intellectual Property Rights” and **“Intellectual Property”** mean the following or their substantial equivalents or counterparts, recognized by or through action before any governmental authority in any jurisdiction throughout the world and including, but not limited to all rights in patents, patent applications, inventions, copyrights, trademarks, trade secrets, trade names, and other proprietary rights in or relating to the Software and Documentation; including any adaptations, corrections, de-compilations, disassemblies, emulations, enhancements fixes, modifications, translations and updates to or derivative works from, the Software or Documentation, whether made by Tait or another party, or any improvements that result from Tait processes or, provision of information services.
“Licensee” means any individual or entity that has accepted the terms of this License.
“Open Source Software” means software with freely obtainable source code and license for modification, or permission for free distribution.
“Open Source Software License” means the terms or conditions under which the Open Source Software is licensed.
“Person” means any individual, partnership, corporation, association, joint stock company, trust, joint venture, limited liability company, governmental authority, sole proprietorship, or other form of legal entity recognized by a governmental authority.
“Security Vulnerability” means any flaw or weakness in system security procedures, design, implementation, or internal controls that if exercised (accidentally triggered or intentionally exploited) could result in a security breach such that data is compromised, manipulated, or stolen, or a system is damaged.
“Software” (i) means proprietary software in executable code format, and adaptations, translations, de-compilations, disassemblies, emulations, or derivative works of such software; (ii) means any modifications, enhancements, new versions and new releases of the software provided by Tait; and (iii) may contain one or more items of software owned by a third-party supplier. The term "Software" does not include any third-party software provided under separate license or not licensable under the terms of this Agreement.
“Source Code” means software expressed in human readable language necessary for understanding, maintaining, modifying, correcting, and enhancing any software referred to in this Agreement and includes all states of that software prior to its compilation into an executable programme.
“Tait” means Tait Limited and includes its Affiliates.

Section 2 SCOPE

This Agreement contains the terms and conditions of the license Tait is providing to Licensee, and of Licensee’s use of the Software and Documentation. Tait and Licensee enter into this Agreement in connection with Tait delivery of certain proprietary Software and/or products containing embedded or pre-loaded proprietary Software.

Section 3 GRANT OF LICENSE

3.1. Subject to the provisions of this Agreement and the payment of applicable license fees, Tait grants to Licensee a personal, limited, non-transferable (except as permitted in Section 7), and non-exclusive license to use the Software in executable code form, and the Documentation, solely in connection with Licensee's use of the Designated Products for the useful life of the Designated Products. This Agreement does not

grant any rights to source code.
3.2. If the Software licensed under this Agreement contains or is derived from Open Source Software, the terms and conditions governing the use of such Open Source Software are in the Open Source Software Licenses of the copyright owner and not in this Agreement. If there is a conflict between the terms and conditions of this Agreement and the terms and conditions of the any applicable Open Source Software Licenses, the terms and conditions of the Open Source Software Licenses will take precedence. For information about Open Source Components contained in Tait products and the related Open Source licenses, see:
http://support.taitradio.com/go/opensource

Section 4 LIMITATIONS ON USE

4.1. Licensee may use the Software only for Licensee's internal business purposes and only in accordance with the Documentation. Any other use of the Software is strictly prohibited. Without limiting the general nature of these restrictions, Licensee will not make the Software available for use by third parties on a "time sharing," "application service provider," "service bureau" basis, or for any other similar commercial rental or sharing arrangement.
4.2. Licensee will not, and will not directly or indirectly allow or enable any third party to: (i) reverse engineer, disassemble, extract components, decompile, reprogram, or otherwise reduce the Software or any portion thereof to a human perceptible form or otherwise attempt to recreate the source code; (ii) modify, adapt, create derivative works of, or merge the Software; (iii) copy, reproduce, distribute, lend, or lease the Software or Documentation to any third party; (iv) grant any sublicense or other rights in the Software or Documentation to any third party; (v) take any action that would cause the Software or Documentation to be placed in the public domain; (vi) remove, or in any way alter or obscure any copyright notice or other notice of Tait or third-party licensor's proprietary rights; (vii) provide, copy, transmit, disclose, divulge or make the Software or Documentation available to, or permit the use of the Software by, any third party or on any machine except as expressly authorized by this Agreement; or (viii) use, or permit the use of, the Software in a manner that would result in the production of a copy of the Software by any means whatsoever other than what is permitted in this Agreement. Licensee may make one copy of the Software to be used solely for archival, back-up, or disaster recovery purposes; provided that Licensee may not operate that copy of the Software at the same time as the original Software is being operated. Licensee may make as many copies of the Documentation as it may reasonably require for the internal use of the Software.
4.3. Unless otherwise authorized by Tait in writing, Licensee will not, and will not enable or allow any third party to: (i) install a copy of the Software on more than one unit of a Designated Product; or (ii) copy or transfer Software installed on one unit of a Designated Product to any other device. Licensee may temporarily transfer Software installed on a Designated Product to another device if the Designated Product is inoperable or malfunctioning. Temporary transfer of the Software to another device must be discontinued when the original Designated Product is returned to operation and the Software must be removed from the other device.
4.4. Licensee will maintain, during the term of this Agreement and for a period of two years thereafter, accurate records relating to this license grant to verify compliance with this Agreement. Tait, or a third party nominated by Tait, may inspect Licensee's premises, books and records, upon reasonable prior notice to Licensee, during Licensee's normal business hours and subject to Licensee's facility and security regulations. Tait is responsible for the payment of all expenses and costs of the inspection, provided that Licensee shall indemnify Tait for all costs (including audit costs and legal costs on a solicitor client basis) if Licensee has breached the terms of this Agreement. Any information obtained by Tait during the course of the inspection will be kept in strict confidence by Tait and used solely for the purpose of verifying Licensee's compliance with the terms of this Agreement.

Section 5 OWNERSHIP AND TITLE

Tait, its licensors, and its suppliers retain all of their Intellectual Property Rights in and to the Software and Documentation, in any form. No rights are granted to Licensee under this Agreement by implication, estoppel or otherwise, except for those rights which are expressly granted to Licensee in this Agreement. All Intellectual Property developed, originated, or prepared by Tait in connection with providing the Software, Designated Products, Documentation, or related services, remains vested exclusively in Tait, and Licensee will not have any shared development or other Intellectual Property Rights.

Section 6 LIMITED WARRANTY; DISCLAIMER OF WARRANTY

6.1. The commencement date and the term of the Software warranty will be a period of one (1) year from Tait shipment of the Software. If Licensee is not in breach of any obligations under this Agreement, Tait warrants that the unmodified Software, when used properly and in accordance with the Documentation and this Agreement, will be free from a reproducible defect that eliminates the functionality or successful operation of a feature critical to the primary functionality or successful operation of the Software. Whether a defect has occurred will be determined solely by Tait. Tait does not warrant that Licensee's use of the Software or the Designated Products will be uninterrupted, error-free, completely free of Security Vulnerabilities, or that the Software or the Designated Products will meet Licensee's particular requirements. Tait makes no representations or warranties with respect to any third-party software included in the Software.
6.2 Tait sole obligation to Licensee, and Licen-

see's exclusive remedy under this warranty, is to use reasonable efforts to remedy any material Software defect covered by this warranty. These efforts will involve either replacing the media or attempting to correct significant, demonstrable program or documentation errors or Security Vulnerabilities. If Tait cannot correct the defect within a reasonable time, then at Tait option, Tait will replace the defective Software with functionally equivalent Software, license to Licensee substitute Software which will accomplish the same objective, or terminate the license and refund Licensee's paid license fee. If Tait investigation of the perceived defect reveals that no such defect in fact exists, Tait may recover its costs in respect of such investigation from Licensee.

6.3. Tait disclaims any and all other warranties relating to the Software or Documentation other than the express warranties set forth in this Section 6. Warranties in Section 6 are in lieu of all other warranties whether express or implied, oral or written, and including without limitation any and all implied warranties of condition, title, non-infringement, merchantability, or fitness for a particular purpose or use by Licensee (whether Tait knows, has reason to know, has been advised of, or is otherwise aware of any such purpose or use), whether arising by law, by reason of custom or usage of trade, or by course of dealing. In addition, Tait disclaims any warranty to any person other than Licensee with respect to the Software or Documentation.

Section 7 TRANSFERS

7.1. Licensee will not transfer the Software or Documentation to any third party without specific prior written consent from Tait. Tait may withhold such consent or at its own discretion make the consent conditional upon the transferee paying applicable license fees and agreeing to be bound by this Agreement.

7.2. In the case of a value-added reseller or distributor of Tait Designated Products, the consent referred to in Section 7.1 may be contained in a Tait Reseller or Tait Distributor Agreement.

7.3. If the Designated Products are Tait vehicle-mounted mobile products or hand-carried portable radio products and Licensee transfers ownership of the Tait mobile or portable radio products to a third party, Licensee may assign its right to use the Software which is embedded in or furnished for use with the radio products and the related Documentation; provided that Licensee transfers all copies of the Software and Documentation to the transferee.

7.4. For the avoidance of any doubt, Section 7.3 excludes TaitNet Infrastructure, or the products listed at any time under network products at: http://www.taitradio.com.

7.5. If Licensee, as a contractor or subcontractor (integrator), is purchasing Tait Designated Products and licensing Software not for its own internal use but for end use only by a Customer, the Licensee may transfer such Software, but only if a) Licensee transfers all copies of such Software and the related Documentation to the transferee and b) Licensee has first obtained from its Customer (and, if Licensee is acting as a subcontractor, from the interim transferee(s) and from the ultimate end user sub license) an enforceable sublicense agreement that prohibits any other transfer and that contains restrictions substantially identical to the terms set forth in this Software License Agreement. Except as stated in the foregoing, Licensee and any transferee(s) authorised by this Section may not otherwise transfer or make available any Tait Software to any third party nor permit any party to do so. Licensee will, on request, make available evidence reasonably satisfactory to Tait demonstrating compliance with all the foregoing.

Section 8 TERM AND TERMINATION

8.1. Licensee's right to use the Software and Documentation will commence when the Designated Products are supplied by Tait to Licensee and will continue for the life of the Designated Products with which or for which the Software and Documentation are supplied, unless Licensee breaches this Agreement, in which case this Agreement and Licensee's right to use the Software and Documentation may be terminated immediately upon notice by Tait.

8.2. Within thirty (30) days after termination of this Agreement, Licensee must certify in writing to Tait that all copies of the Software have been removed or deleted from the Designated Products and that all copies of the Software and Documentation have been returned to Tait or destroyed by Licensee and are no longer in use by Licensee.

8.3. Licensee acknowledges that Tait made a considerable investment of resources in the development, marketing, and distribution of the Software and Documentation and that Licensee's breach of this Agreement will result in irreparable harm to Tait for which monetary damages would be inadequate. If Licensee breaches this Agreement, Tait may terminate this Agreement and be entitled to all available remedies at law or in equity including immediate injunctive relief and repossession of all non-embedded Software and associated Documentation. Licensee shall pay all Tait costs (on an indemnity basis) for the enforcement of the terms of this Agreement.

Section 9 CONFIDENTIALITY

Licensee acknowledges that the Software and Documentation contain proprietary and Confidential Information valuable to Tait and are Tait trade secrets, and Licensee agrees to respect the confidentiality of the information contained in the Software and Documentation.

Section 10 LIMITATION OF LIABILITY

10.1. In no circumstances shall Tait be under any liability to Licensee, or any other person whatsoever, whether in Tort (including negligence), Contract (except as expressly provided in this Agreement), Equity, under any Statute, or otherwise at law for any losses or damages whether general, special, exemplary, punitive, direct, indirect, or consequential arising out of or in connection with any use or inability of using the Software.

10.2. Licensee's sole remedy against Tait will be

limited to breach of contract and Tait sole and total liability for any such claim shall be limited at the option of Tait to the repair or replacement of the Software or the refund of the purchase price of the Software.

Section 11 GENERAL

11.1. COPYRIGHT NOTICES. The existence of a copyright notice on the Software will not be construed as an admission or presumption of publication of the Software or public disclosure of any trade secrets associated with the Software.

11.2. COMPLIANCE WITH LAWS. Licensee acknowledges that the Software may be subject to the laws and regulations of the jurisdiction covering the supply of the Designated Products and will comply with all applicable laws and regulations, including export laws and regulations, of that country.

11.3. ASSIGNMENTS AND SUBCONTRACTING. Tait may assign its rights or subcontract its obligations under this Agreement, or encumber or sell its rights in any Software, without prior notice to, or consent of, Licensee.

11.4. GOVERNING LAW. This Agreement shall be subject to and construed in accordance with New Zealand law and disputes between the parties concerning the provisions hereof shall be determined by the New Zealand Courts of Law. Provided however Tait may at its election bring proceedings for breach of the terms hereof or for the enforcement of any judgment in relation to a breach of the terms hereof in any jurisdiction Tait considers fit for the purpose of ensuring compliance with the terms hereof or obtaining relief for breach of the terms hereof.

11.5. THIRD-PARTY BENEFICIARIES. This Agreement is entered into solely for the benefit of Tait and Licensee. No third party has the right to make any claim or assert any right under this Agreement, and no third party is deemed a beneficiary of this Agreement. Notwithstanding the foregoing, any licensor or supplier of third-party software included in the Software will be a direct and intended third-party beneficiary of this Agreement.

11.6. SURVIVAL. Sections 4, 5, 6.3, 7, 8, 9, 10, and 11 survive the termination of this Agreement.

11.7. ORDER OF PRECEDENCE. In the event of inconsistencies between this Agreement and any other Agreement between the parties, the parties agree that, with respect to the specific subject matter of this Agreement, this Agreement prevails.

11.8. SECURITY. Tait uses reasonable means in the design and writing of its own Software and the acquisition of third-party Software in order to limit Security Vulnerabilities. While no software can be guaranteed to be free from Security Vulnerabilities, if a Security Vulnerability is discovered, Tait will take the steps specified in Section 6 of this Agreement.

11.9. EXPORT. Licensee will not transfer, directly or indirectly, any Designated Product, Documentation or Software furnished hereunder or the direct product of such Documentation or Software to any country for which New Zealand or any other applicable country requires an export license or other governmental approval without first obtaining such license or approval.

11.10. SEVERABILITY. In the event that any part or parts of this Agreement shall be held illegal or null and void by any court or administrative body of competent jurisdiction, such determination shall not affect the remaining terms which shall remain in full force and effect as if such part or parts held to be illegal or void had not been included in this Agreement. Tait may replace the invalid or unenforceable provision with a valid and enforceable provision that achieves the original intent and economic effect of this Agreement.

11.11. CONSUMER GUARANTEES. Licensee acknowledges that the licenses supplied in terms of this agreement are supplied to Licensee in business, and that the guarantees and other provisions of prevailing consumer protection legislation shall not apply.

11.12. WHOLE AGREEMENT. Licensee acknowledges that it has read this Agreement, understands it and agrees to be bound by its terms and conditions. Licensee also agrees that, subject only to the express terms of any other agreement between Tait and Licensee to the contrary, this is the complete and exclusive statement of the Agreement between it and Tait in relation to the Software. This Agreement supersedes any proposal or prior agreement, oral or written, and any other communications between Licensee and Tait relating to the Software and the Designated Products.