

TaitNet T1541 Radio Network Installation Manual

MNA-00008-16 · Issue 16 · October 2017

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

All information contained in this manual is the property of Tait Limited. All rights reserved. This manual may not, in whole or in part, be copied, photocopied, reproduced, translated, stored, or reduced to any electronic medium or machine-readable form, without prior written permission from Tait Limited.

The words TAIT, TAITNET and the TAIT logo are registered trademarks of Tait Limited.

All trade names referenced are the service mark, trademark or registered trademark of the respective manufacturers.

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, NZ530819, NZ534475, NZ547713, NZ577009, NZ579051, NZ579364, NZ586889, NZ610563, NZ615954, NZ700387, NZ708662, NZ710766, NZ711325, NZ726313, NZ593887, AU2015215962, AU339127, AU339391, AU2016259281, AU2016902579, EU000915475-0001, EU000915475-0002, GB2532863, US14/834609 Div. no 1, US15/346518 Div.no 2, US15/350332, US15/387026 Div., US20150085799, US20160044572, US20160057051, US640974, US640977, US698339, US702666, US7758996, US8902804, US9107231, US9504034, US9559967.

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.

Preface

Scope of Manual


This T1541 Installation Manual provides installation and service information for a TaitNet wide area trunked network (running on TaitCentOS) when operating with the software identified as Q1541NC and Q1541NMT version 5.00. If the software version of Q1541NC and Q1541NMT is newer than 5.00, please consult the relevant software release notes to check whether this manual is still current.

For installation instructions for T1541 node controllers running on Solaris (prior to release 5.00), refer to issue 15 of this manual (MNA-00008-15).

Special Information

In this manual, icons together with special formatting draw attention to special information and indicate its nature and purpose.

Notice This alert is used to highlight information that is required to ensure procedures are performed correctly. Incorrectly performed procedures could result in equipment damage or malfunction.

 This icon is used to draw your attention to information that may improve your understanding of the equipment or procedure.

Typographical Conventions for the NMT

Select *File* > Configuration means “Select the File menu (for example by clicking on the menu name in the menu bar), then select Configuration from the list that appears.”

Select *Node* > Configure means “In the main window, click on the node you want to work with, then click the right-mouse button and select Configure from the pop-up menu that appears.”

Associated Documents

The System Manual (MNA-00019-xx) provides system-level descriptions of the network and general information to assist technicians in network installation and configuration.

The T1541 Operations Manual (MNA-00007-xx) describes how to configure and operate a TaitNet wide area trunked network.

Technical Notes are published from time to time on the Tait technical support web (password access only) to describe applications for Tait products, to provide technical details not included in manuals, and to offer solutions for any problems that arise.

Publication Record

Version	Publication date	Amended sections and pages
1.00	October 2002	First release
2.00	July 2003	Name changed from "TaitNet 5100 Installation Manual" (MN5100-00-00-315) Section added to Chapter 2 "Configuring the Second Ethernet Interface on a Sun Netra T1 or SunFire V120".
3.00	December 2003	Chapter 5 updated for installing T1541 NMT software version 3.x.x on Windows and Solaris.
3.11	April 2004	Chapter 11 added. Minor updates to "Email Format" and "NMT with Solaris".
MNA-00008-01	June 2005	Re-released and updated for version 4 software.
MNA-00008-02	October 2005	Updated for version 4.01 software.
MNA-00008-03	August 2006	Updated for version 4.02 software.
MNA-00008-04	February 2007	Information for installing Solaris 10 onto a Sun Netra-210 added
MNA-00008-05	June 2007	Updated for version 4.04 software.
MNA-00008-06	December 2007	Updated for version 4.04.02 software.
MNA-00008-07	August 2008	Updated diagrams
MNA-00008-08	November 2008	Updated for version 4.06 software: <ul style="list-style-type: none"> ■ DispatcherConsoleOverride added ■ Section 5.1 Configuration Procedure updated for Dispatcher Console Override configuration ■ Section 9.1 Software Installation updated ■ Section 10 NMT Upgrade Procedure updated
MNA-00008-09	June 2009	Updated for software version 4.07 and to include installation details for Solaris 10 on a Sun Netra X4200 M2 server: <ul style="list-style-type: none"> ■ Section 2.4 Solaris 10 on X4200 Installation Process added ■ Section 4 Install the Node Controller Software updated ■ Section 5.1 Configuration Procedure updated ■ DispatcherConsoleOverride updated ■ V110OverNpd added ■ Section 9.2 Setup for Multiple Users added ■ Section 11 High Availability Options added

Version	Publication date	Amended sections and pages
MNA-00008-10	December 2009	<p>Updated for software version 4.07.02:</p> <ul style="list-style-type: none"> ■ Section 2.3 Solaris 10 on Sparc Installation Process updated ■ Section 2.4 Solaris 10 on X4200 Installation Process updated ■ Section 4.1 Login as Root updated ■ Section 4.2 Mount the CD updated ■ Section 4.4 Install the Node Controller Software updated ■ "LogAgeLimit (Days to keep log files)" updated ■ Important notice added to Step 3 of Section 6 Node Upgrade Procedure ■ "Note About Versions Prior to 4.02.10" updated ■ System configuration details updated ■ Important notice updated in Section 9.2 Setup for Multiple Users ■ Data path name updates to Section 10 NMT Upgrade Procedure
MNA-00008-11	June 2010	<p>Updated for software version 4.08.00:</p> <ul style="list-style-type: none"> ■ Section 1.2.2 Backup Node Controller, ECC and Etherlite with Split Serial Ports (Option 2) added ■ Section 1.2.4 Geographically Diverse Nodes (Option 4) added ■ Section 4.5 Configuring SNMP (if required) added (TIMS 80017) ■ Section 5.1 Configuration Procedure updated ■ Section 5.3.1 Configuration Parameters updated ■ Section LogAgeLimit (Days to keep log files) added ■ Section 5.3.2 Additional Configuration Parameters added ■ Section 11 High Availability Options added
MNA-00008-12	March 2011	<p>Updated for software version 4.08.01:</p> <ul style="list-style-type: none"> ■ Section 2.4.2 Installing the Operating system updated ■ Section 5.2.5 Installing the Node Controller Software updated ■ Section 4.5 and Section 4.6 moved to Section 6.2.8 Configuring SNMP (if required) and Section 5.2.7 Installing the License File, respectively ■ Footnote added to "LogAgeLimit (Days to keep log files)" on page 44 ■ "NetworkCheckIPA NetworkCheckIPB" on page 48 updated ■ "CheckConflictingRegistrations" on page 49 updated ■ Site Link Parameters moved from Section 5.2.4 Configuration Parameters to Section 5.2.5 Additional Configuration Parameters on page 51 ■ Important note added to Section 6.2.8 Configuring SNMP (if required) ■ Section 5.2.8 Installing the run-active Script (optional) added ■ Section 6 Node Upgrade Procedure updated ■ "MonitorComPort" on page 49 updated ■ Note added to "DMM Parameters" table on page 53 ■ Section 5.2.6 Example node.cfg File updated ■ "Note About Versions Prior to 4.08.xx" on page 103 added

Version	Publication date	Amended sections and pages
.../ continued		<ul style="list-style-type: none"> ■ Note added to Section 7 Node Roll-back Procedure ■ Section 9.2.2 Logging on to the Node Controller as 'root' updated ■ Section 9.3 Additional taitnet commands added ■ Section 9.4 Advanced node commands added ■ Section 8.5 Directory Structure updated ■ "Recommended system configuration" on page 64 updated ■ Section 9.6 Porting an Existing NMT to a New PC added
MNA-00008-13	October 2011	<p>Updated for software version 4.09.00:</p> <ul style="list-style-type: none"> ■ Section 3.5 Installing Solaris 10 on X4250 added ■ Section 3 Configuring the Serial Port Server updated ■ Section 3.2 Digi EL Series Serial Port Server Configuration updated ■ Section 3.3 Digi TS Series Serial Port Server Configuration added ■ Section 3.4 Configuring a Digi TS Series Port for SMM Diagnostics added ■ Section Solaris 10 on X4250 updated ■ Section 5.2.2 Serial Device File Configuration added ■ GroupCallsOnHoldTimeoutForInactivity added to Section 5.2.5 Additional Configuration Parameters ■ Note added to Section 12.1
MNA-00008-14	September 2013	<p>Updated for software version 4.10.xx and later:</p> <ul style="list-style-type: none"> ■ Section 3.6 Installing Solaris 10 on X4270 added ■ "Solaris 10 on X4200/X4270" on page 72 updated ■ "Solaris 10 on X4250" on page 72 added ■ "Increasing the Memory Allocated to the NMT" on page 67 added
MNA-00008-15	November 2014	<p>Updated for software version 4.11.00 and later</p> <ul style="list-style-type: none"> ■ "DaysToKeepDatabases (Days to keep records and stats)" on page 44 updated ■ "NetworkCheckAttempts (Attempts before network failed)" on page 48 added ■ "Timeouts" on page 52 table updated ■ "Example node.cfg File" on page 53 updated ■ "taitnet print-checksums" on page 111 added ■ Section 9.2 Running the NMT on a Computer Without a Sound Card added ■ Section 9.7 Installing a Client NMT Without a License File added ■ Section 9.8 NMT Configuration Files added ■ Section 12.4 Full Alignment Method updated

Version	Publication date	Amended sections and pages
MNA-00008-16	October 2017	<p>Updated for software version 5.00 and later</p> <ul style="list-style-type: none"> ■ Installation instructions for CentOS servers added throughout the manual ■ Installation instructions for Solaris servers removed throughout the manual ■ Section 1.1 Overview updated ■ Section 1.2 High Availability footnote added ■ Section 2 Installing TaitCentOS added ■ Section 5.2.2 Mounting the USB Flash Drive added ■ Appendix 1: Transferring an ISO Image to a USB Flash Drive added

Contents

Preface	3
Scope of Manual	3
Special Information	3
Notice Typographical Conventions for the NMT	3
Associated Documents	3
Publication Record	4
1 Introduction	11
1.1 Overview	11
1.1.1 T1541 Network Management Terminal (NMT)	11
1.1.2 T1541 Node	11
1.1.3 Site	13
1.1.4 Mobile and hand-portable radios	13
1.1.5 Dispatch consoles	13
1.2 High Availability	15
1.2.1 Backup Node Controller (Option 1)	16
1.2.2 Backup Node Controller, ECC and Split Port Etherlite (Option 2)	16
1.2.3 Backup Node Controller, EtherLite, ECC and SMM (Option 3)	17
1.2.4 Geographically Diverse Nodes (Option 4)	18
1.3 Overview of Installation Process	19
2 Installing TaitCentOS	20
2.1 Before You Start	20
2.1.1 Information Required	20
2.1.2 Equipment Required	20
2.2 Configuring BIOS Settings	20
2.3 Installing TaitCentOS 6.8 for the First Time	22
2.4 Changing the Default IP Address Using the Network Configuration Tool	23
3 Installing the Node Controller Software	25
3.1 CentOS Systems	25
3.1.1 Installing License Files	28
3.1.2 Obtaining the license.dat File	28
3.1.3 Installing the Node Controller's License File	28
4 Configuring the Serial Port Server	30
4.1 CentOS Systems	30
4.2 Digi EL Series Serial Port Server Configuration	31
4.2.1 Connecting to an SMM or DMM Site controller	33
4.3 Digi TS Series Serial Port Server Configuration	33
4.3.1 Configuring the TS as a RealPort device	34
4.3.2 Configuring the TS as a TCP Sockets device	34
4.3.3 Connecting to an SMM or DMM Site controller	36

4.4	Configuring a Digi TS Series Port for SMM Diagnostics	36
4.4.1	Connecting to a SMM Diagnostics Port	37
5	Configuring the Node Controller	38
5.1	CentOS Systems	38
5.1.1	Network Time Protocol (NTP)	38
5.1.2	SNMP	38
5.1.3	Syslog	39
5.1.4	Users	39
5.1.5	Centralized Authentication	39
5.1.6	Local Users	40
5.2	Node Configuration	40
5.2.1	Configuration Procedure	40
5.2.2	Serial Device File Configuration	41
5.2.3	Node Controller Parameter Definitions	42
5.2.4	Configuration Parameters	42
5.2.5	Additional Configuration Parameters	51
5.2.6	Example <code>tait_mptnc.cfg</code> File	55
5.2.7	Installing the run-active Script (optional)	57
6	Node Upgrade Procedure	58
6.1	Upgrading T1541 Firmware	58
6.2	Upgrading the Operating System	58
7	Node Roll-back Procedure	59
7.1	Recovering from a Failed Firmware Upgrade	59
8	Operating the Node Controller	60
8.1	Logging on to the Node Controller Using SSH	60
8.2	Logging on to the Node Controller as 'root'	60
8.3	Administration Application Backups	60
8.4	Advanced <code>taimnet.mptc</code> commands	61
8.5	Directory Structure	63
9	Installing the NMT Software	65
9.1	Installation Procedure	65
9.2	Running the NMT on a Computer Without a Sound Card	68
9.3	Increasing the Memory Allocated to the NMT	68
9.4	Setting up for Multiple Users	69
9.5	Configuring NTP for NMTs running Windows 2000	70
9.6	Porting an Existing NMT to a New PC	72
9.6.1	For the Server NMT:	72
9.6.2	For a Client NMT:	73
9.7	Installing a Client NMT Without a License File	74
9.8	NMT Configuration Files	75
9.8.1	Additional <code>NMT.cfg</code> Parameters	76

10	NMT Upgrade Procedure	79
11	High Availability Options	82
11.1	Option 1: Standby Node Only	82
11.1.1	Operation	82
11.1.2	Setup	83
11.2	Option 2: Standby Node/DAS with Split Serial Ports	86
11.2.1	Operation	86
11.2.2	Setup	86
11.3	Option 3: Standby Node/DAS and Site Management Modules	88
11.3.1	Operation	88
11.3.2	Setup	89
11.4	Option 4: Geographically Diverse Nodes	90
11.4.1	Operation	90
11.4.2	Setup	92
12	Adding or Replacing a High Availability Node Controller	94
12.1	Introduction	94
12.2	Preparing the System	94
12.3	Standard Alignment Method	95
12.4	Full Alignment Method	96
12.4.1	Determine Cause of Mismatched Checksums	96
12.4.2	Perform Full Alignment	96
	Appendix 1:Transferring an ISO Image to a USB Flash Drive	98
1.1	Using Rufus	98
1.2	Using Win32DiskImager	100
	Tait General Software Licence Agreement	104

1 Introduction

1.1 Overview

The TaitNet TN5100 multi-node or TN3100 single-node system is a network of interconnected sites that enable radios with trunking capability to communicate with each other. A system is made up of the following elements:

1.1.1 T1541 Network Management Terminal (NMT)

This is used for network and subscriber management. A single NMT server and a number of NMT clients can be installed. The NMT is connected to the nodes via a computer network.

1.1.2 T1541 Node

The TN3100 network supports a single node, the TN5100 network supports up to 32 nodes. On multi-node systems, the nodes are connected to each other via IP network. A node consists of three components:

- T1541 Node Controller - The node controller performs call control and network management functions. It handles inter-channel calls and connections to dispatch consoles and third party IP interfaces. The example below is a Kontron CG2300 server.



The following table lists the servers that can be used. Note that the shaded areas denote equipment that has reached end-of-life, and whilst currently supported, is no longer available.

Server	Operating System
Sun Netra X3-2	Unix - Solaris 10
Sun Netra X4200/X4250/X4270	Unix - Solaris 10
Kontron CG2300	Linux - CentOS

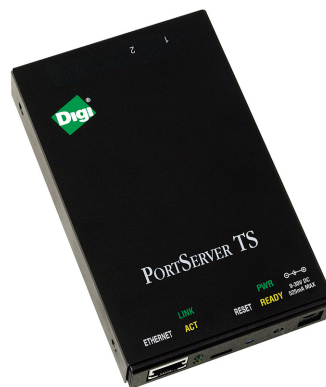
- Switching Ethernet Hub - This is used to connect the node to a computer network. This allows nodes to communicate with each other and allows the Network Management Terminal (NMT) to connect to the nodes. The hub is also used to connect the node controller to the serial port server.



- EtherLite Serial Port Server - This is used to connect sites to a node. The EtherLite has either 8 or 32 serial ports. Each serial port on the EtherLite can be used to connect one site to the node (up to a maximum of 30 sites).



- Digi ConnectPort TS 4x2 Serial Port Server - This is an alternative serial port server, for use as above



In addition, each node has a T1561 Digital Audio Switch (DAS). This is used to switch audio communications from node to node and between the node and a PABX/PSTN. The DAS is controlled by a T1561-15 Embedded Controller card (ECC).

1.1.3 Site

Up to 30 sites can be connected to each node. Each site can have up to 24 channels. One or two of these channels operate as control channels, the rest operate as traffic channels.

1.1.4 Mobile and hand-portable radios

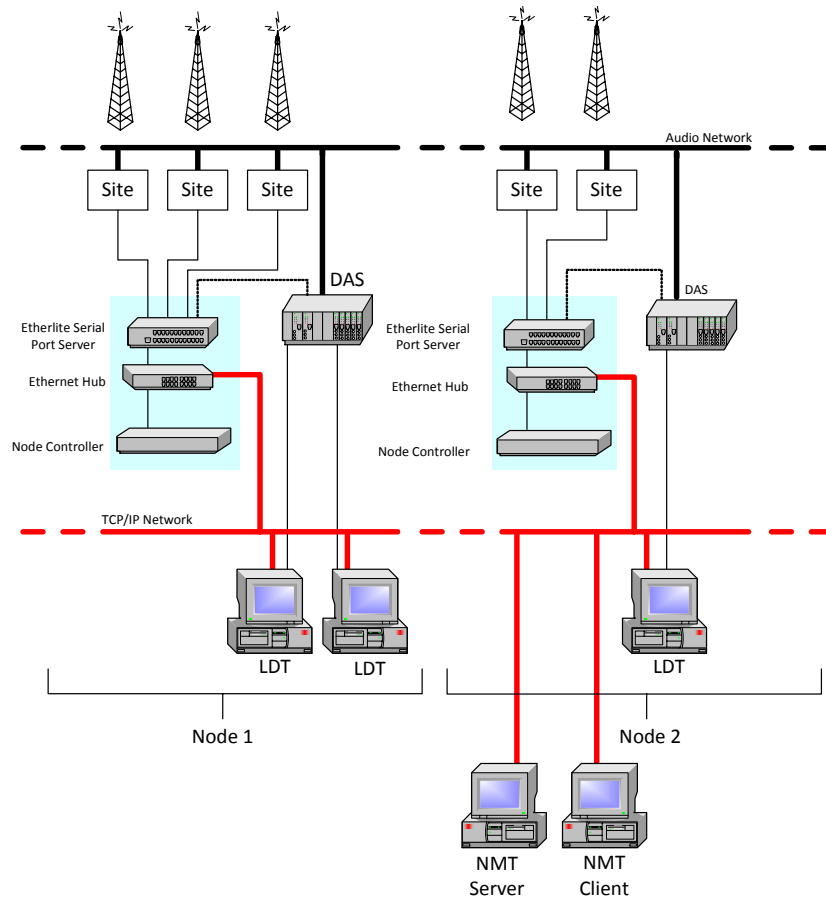
The network can support a large number of radios and groups (maximum number: 1,016,000). Radios communicate with each other via traffic channels. Radios register on a site and can call other radios on the same site (local calls) or at other sites (intersite calls) which may be connected to a different node (internode calls). Radios can register on different sites as they move around the network.

1.1.5 Dispatch consoles

The network can support one or more line-connected dispatch consoles, which facilitate communications and enables a central dispatcher to handle a large number of staff. It also provides special call handling options that are not available to other radios on the network.

The TaitNet Line Dispatcher Terminal (LDT) is connected to the Node Controller by TCP/IP and by audio lines connected to the DAS. From the node's perspective, each LDT is a radio with an audio connection to a particular DAS port. One LDT must be configured as a server that maintains talk group information for all the LDTs. If the LDTs are remotely located, they are connected to the node via routers. The number of LDTs that a node can have is, in practice, limited only by the conferencing capability of the DAS.

A simple TN5100 network with two nodes is illustrated below. Three sites are connected to one node and two sites are connected to the other node. An NMT server and NMT client are used to manage the network. The components of the nodes are shown in the shaded regions.



The discreet parts that make up the nodes and sites are connected using a variety of cables and protocols but three main data highways are shown:

- A computer network

This is used to connect the nodes to each other and to connect the NMT(s) to the nodes. Line dispatchers (LDTs) are also connected to this network, which they use to communicate control data.

- An audio network

This can comprise many types of links, for example; 4-wire analog, or E1/T1 digital. The audio network is used to transmit audio (speech) data between the following:

- A site and the DAS at the node (for intersite speech calls)
- The DAS at the node and a telephone interface (PABX or PSTN)
- The DAS at one node and the DAS at another (for internode speech calls)

Non-Prescribed Data (NPD) is also carried over the audio network.

- The intersite control network

Each site is controlled by a T1722 Site Management Module (SMM). The control link is via a connection between the EtherLite at the node and the SMM at each site. The link can be either:

- An RS-232 link

This is usually used to connect a site that is geographically co-located with a node. This can also be used to connect sites to a

geographically remote node via an RF or microwave link. Baud rates up to 64k are supported.

- A Modem

1200, 2400 or 9600 baud serial links are supported, generally over a leased line.

1.2 High Availability

High availability provides quick system recovery in the event of a major component failure. The feature provides redundancy for the following hardware:

- T1541Node Controller
- Etherlite Serial Port Server
- T1561-15 Embedded Controller Card (ECC)
- T1722 Site Management Module (SMM)

Two of each component can be installed, a primary and a backup. The primary hardware is active with the backup operating in a standby mode. If a fault occurs on a primary component, the backup hardware takes over and becomes active.¹

This feature does not provide uninterrupted hand-over when switching to the backup equipment. Most active calls or those that are in the set-up process will be cleared (or may hang). This is especially so for intersite or internode calls.

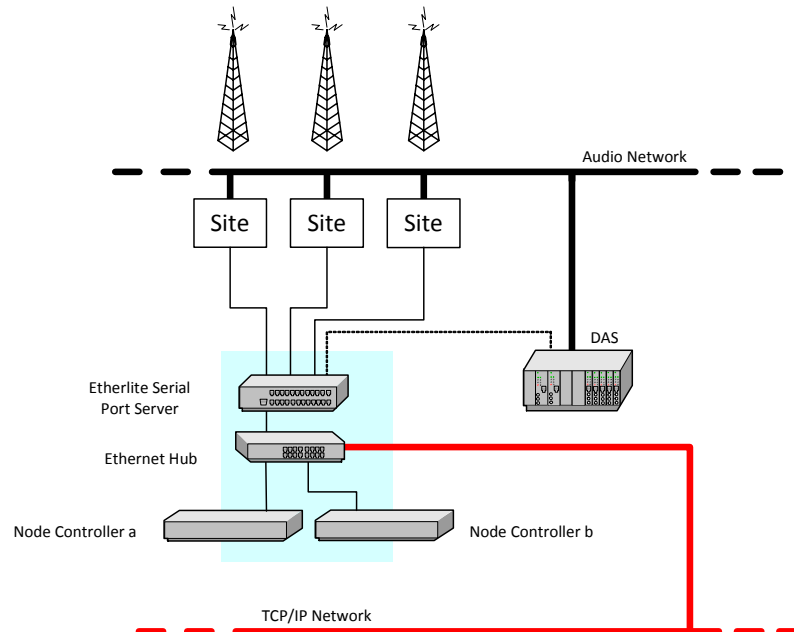
An additional software license is required to activate the high availability feature.

Four options, each with increasing levels of redundancy, are described in the following sections. Installation details for each option are described in [Section 11 High Availability Options](#).

1. The primary and backup nodes can consist of both a Solaris node and a CentOS node.

1.2.1 Backup Node Controller (Option 1)

This configuration provides the most basic and cost effective arrangement to secure the trunked radio system. Two node controllers are installed at the node, these are referred to as node a and node b. Node a operates as the primary node controller and node b operates as a backup in case the primary should fail. No other equipment is duplicated.



1.2.2 Backup Node Controller, ECC and Split Port Etherlite (Option 2)

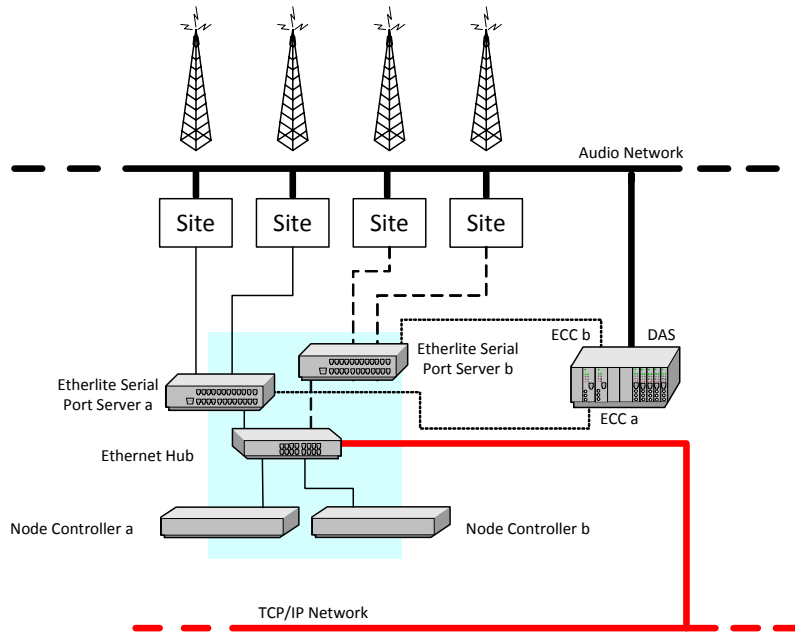
This configuration provides redundancy for critical components at the node. Two node controllers are installed at the node, these are referred to as node a and node b. Node a operates as the primary node and node b operates as a backup in case the primary should fail. The node controllers are connected to the same ethernet hub. (Note that the backup node controller must be configured with the same number as the primary node controller.)

Two Etherlite serial port servers are installed at the node, these are referred to as Etherlite a and Etherlite b. Etherlite a is connected to half of the site SMMs and Etherlite b is connected to the other site SMMs.

Each Etherlite is also connected to one of two embedded controller cards. These cards, referred to as ECC a and ECC b, are housed within the same DAS.

In this configuration, the network can withstand the failure of any one component in the node. However, in the event of an Etherlite failure, the

sites connected to that Etherlite lose intersite service until their connections are manually moved to the other Etherlite.



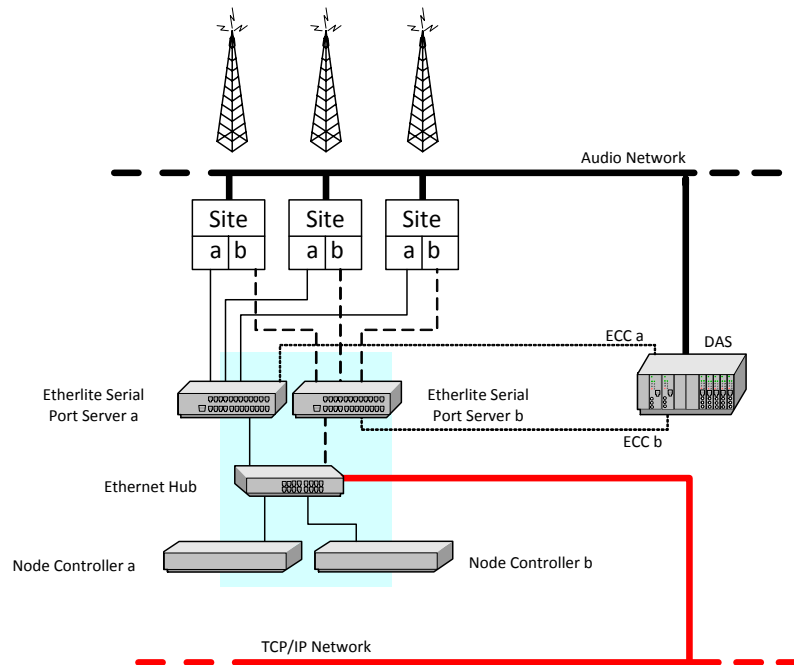
1.2.3 Backup Node Controller, EtherLite, ECC and SMM (Option 3)

This configuration provides redundancy for most critical components. Two node controllers are installed at the node, these are referred to as node a and node b. Node a operates as the primary node and node b operates as a backup in case the primary should fail. The node controllers are connected to the same ethernet hub. (Note that the backup node controller must be configured with the same number as the primary node controller.)

Two serial port servers are installed at the node, these are referred to as Etherlite a and Etherlite b. At each site there are two site management modules, referred to as SMM a and SMM b. Etherlite a is connected to the SMM a at each site and Etherlite b is connected to the SMM b at each site.

Each Etherlite is also connected to one of two embedded controller cards. These cards, referred to as ECC a and ECC b, are housed within the same DAS.

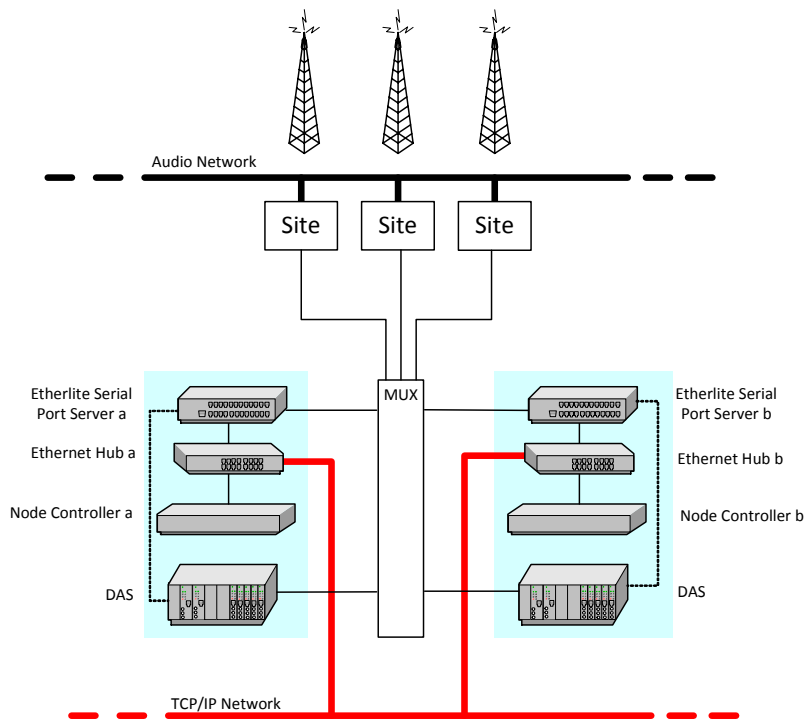
In this configuration, the network can withstand the failure of any one component.



1.2.4 Geographically Diverse Nodes (Option 4)

This configuration supports a system where a complete set of standby equipment may be installed in a separate location, far enough from the primary equipment so that external causes (power outage, lightning damage, fire, etc.) that have disabled the primary equipment have less chance to affect the backup as well.

There are several different levels of redundancy available with this option, but the key difference between this option and the other options is that the entire DAS is duplicated, not just the DAS Embedded Controller Card.



1.3 Overview of Installation Process

The installation process consists of the following steps:

1. Install TaitCentOS on the node controller.
2. Install the node controller software.
3. Configure the EtherLite serial port server.
4. Configure the node controller.
5. Install the Network Management Terminal software.

2 Installing TaitCentOS

The TaitCentOS node controller consists of a Kontron CG2300 server running the Tait CentOS operating system, the TaitNet Administration application and Tait network software.

2.1 Before You Start

Notice Only install the TaitCentOS version supplied by Tait, to ensure that the correct configuration settings are installed. This version of CentOS also includes the TaitNet Administration application.

2.1.1 Information Required

Ensure that you have the following information at hand before beginning the installation:

- host name of the node controller
- IP address of the node controller
- subnet mask to be used on the node controller, this is usually 255.255.0.0
- IP address of the router/gateway (this is optional)

2.1.2 Equipment Required

- IP-connected server with monitor, keyboard and mouse
- USB flash drive containing TaitCentOS
- USB flash drive containing T1541 node controller software

Notice Refer to [“Transferring an ISO Image to a USB Flash Drive” on page 98](#) for instructions on how to load TaitCentOS and the Node Controller software on to USB flash drives.

The following is a brief description of the installation process.

Notice In the following installation instructions, the use of the term ‘select’ means highlight the item and press `Enter`.

2.2 Configuring BIOS Settings

The intent of configuring the BIOS settings is for the following:

- The server will boot unattended and headless
- The server will power up automatically after a power failure
- The server is configured for performance rather than power saving
- Default users/passwords are configured

- Default remote login network settings are configured
- Booting from Network Interface Cards is disabled

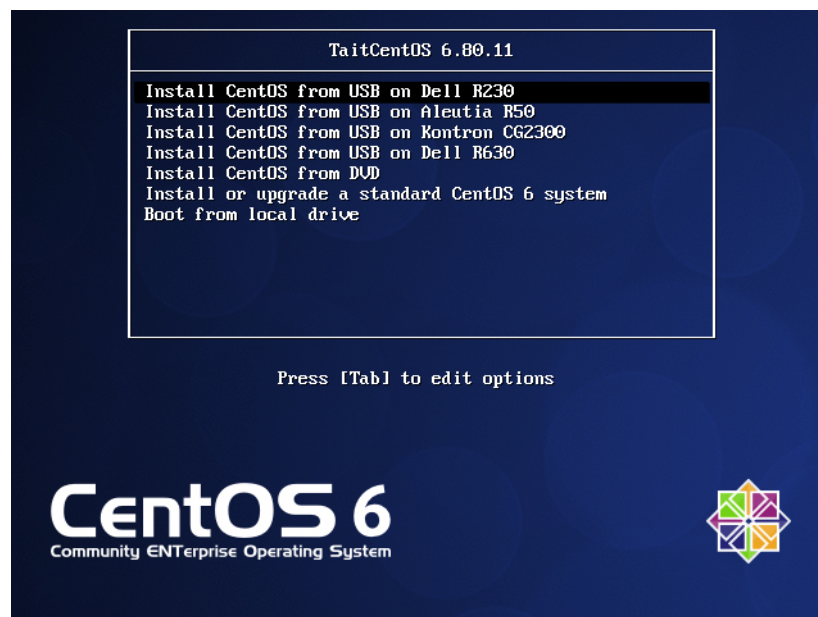
The following instructions are for configuring the BIOS settings in a Kontron CG2300.

1. Power on or reboot the server.
2. Wait for the RAID BIOS screen to finish initializing the drives and get ready to press F2 for the next step.
3. There will be a couple of quick screens with other text, then when the Intel Server Board color graphics screen appears, press F2 quickly. There is only a short time period of approximately 2 seconds for pressing the F2 key.
4. Select Setup Menu.
 - a. Select Main.
 - Select Post Error Pause.
 - Select Disabled.
 - Press Escape to return to Setup Menu.
 - b. Select Advanced.
 - Select Power & Performance.
 - Select CPU Power & Performance Policy.
 - Select Performance.
 - Press Escape to return to Advanced menu.
 - Select System Acoustic Performance Configuration.
 - Select Fan Profile.
 - Select Performance.
 - Press Escape to return to Advanced menu.
 - Press Escape to return to Setup Menu.
 - c. Select Server Management.
 - Select Resume on AC Power Loss.
 - Select Power On.
 - Scroll down the page to select BMC LAN Configuration .
 - Configure the dedicated management LAN settings for the remote server management:
 IP address: 172.29.0.121
 Subnet: 255.255.0.0
 Gateway: 172.29.0.254
 - Select User Configuration.
 - Scroll down to root user and set:
 Privilege to Administrator
 User Status to Enabled
 User Password to K1w1k1w1 (or whatever is appropriate).
 - Press Escape to return to BMC LAN Configuration.
 - Press Escape to return to Server Management.
 - Press Escape to return to Setup Menu.
 - d. Select Boot Maintenance Manager.

- Select Legacy Network Device Order.
 - Ensure all network devices are set to Disabled.
 - Select Save changes and exit this sub-menu.
 - Press Escape to return to Setup Menu.
- e. Press F10 to save the configuration.
- Press y to save and exit.
5. The server will now reboot.

2.3 Installing TaitCentOS 6.8 for the First Time

1. Insert the USB flash drive containing TaitCentOS.
2. To boot from the USB flash drive, perform the following:
 - a. Power on/reboot the server and wait for 4 options to appear in the top left of the screen. Select Boot Manager.
 - b. Wait for the Boot Manager WebUI to appear, then Select One-shot BIOS Boot Menu.
 - c. Select the USB flash drive.
3. The server will reboot, wait for the following window to be displayed:



4. Select the Install option for your server type with the Tab key and press Enter.
5. The install is automatic, and when it has finished the command prompt will be displayed. (A progress bar is displayed during the installation process.)

During the automatic install, the following default settings are applied:

- The firewall is set to disabled

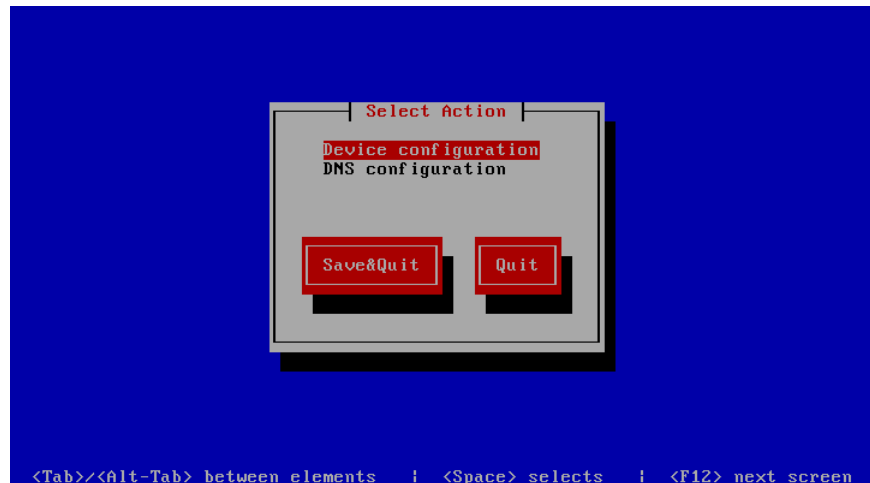
- The root user password is set to K1w1k1w1
 - The default network settings are set to:
 - IP: 172.29.0.101
 - Netmask: 255.255.255.0
 - Gateway: 172.29.0.254
 - Time zone and clock are set to UTC
6. When the installation is complete, click Reboot. When the device restarts, remove the USB flash drive quickly, before the boot sequence starts.

Notice Should there be any installation or upgrade failure, for example a power cut occurring during the procedure, then the node/channel controller will need to be re-installed. In this instance, re-install the firmware and, in the case of an upgrade, restore the latest backup.

2.4 Changing the Default IP Address Using the Network Configuration Tool

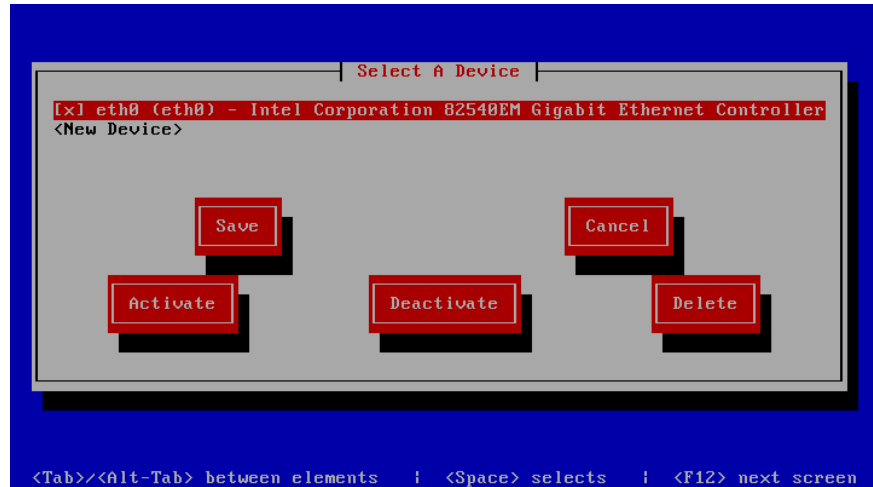
Notice You only need to use this method of changing the IP address if the TaitNet Administration application has not yet been installed, or if you are changing the IP address subnet.

1. From the keyboard attached to the controller, login in to the controller as the `taignet` user.
2. Enter `sudo system-config-network`. A text based screen will appear.

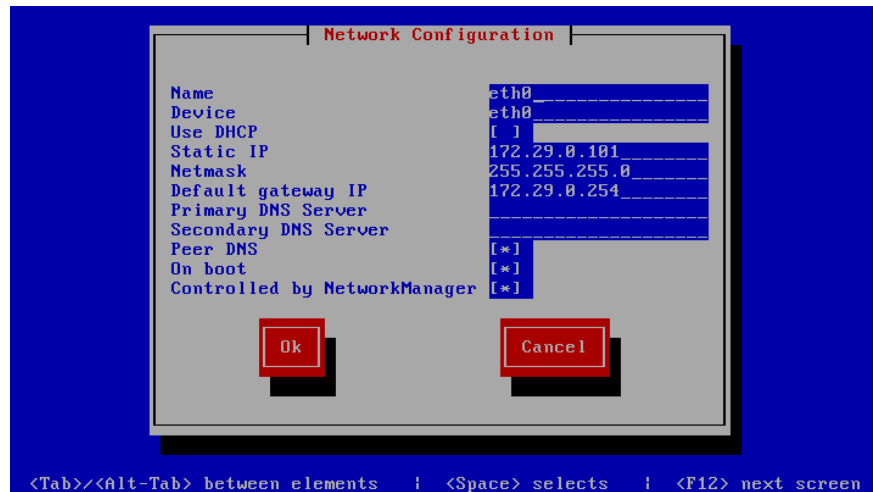


3. Select Device configuration.

- The Select A Device screen should appear.



- Select eth0 or em1 depending on your device name.
- A text based screen will appear.



- Update the Static IP, Netmask and Default gateway IP fields with the information obtained for [Section 2.1.1 Information Required](#). Use the Tab key or Up arrow and Down arrow keys to navigate from field to field. When your settings have been updated, select Ok.
- This will return to the Select A Device page in step 4.
- Select Save.
- Select Save&Quit. This will close the network configuration tool.

Enter **reboot** to restart the controller with the new network configuration settings.

3 Installing the Node Controller Software

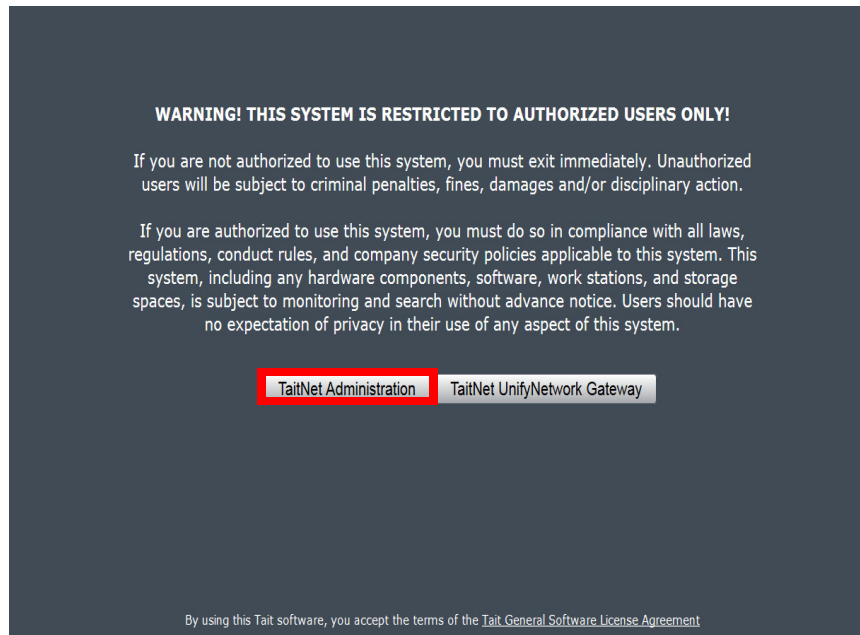
This section outlines the installation of the T1541 node controller software.

3.1 CentOS Systems

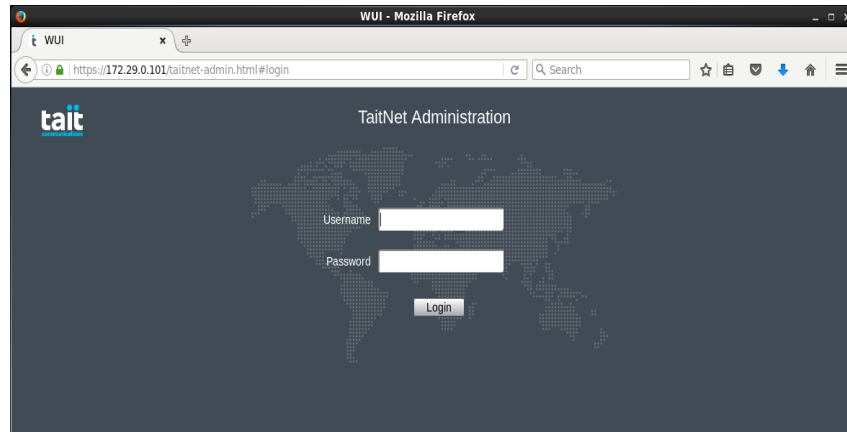
This is done from the TaitNet Administration application, using Q1541 Node Controller install/upgrade packages.

1. Save the received upgrade packages to a PC.
2. Open the PC browser and enter the IP address of the T1541 node controller and select the Administration application.

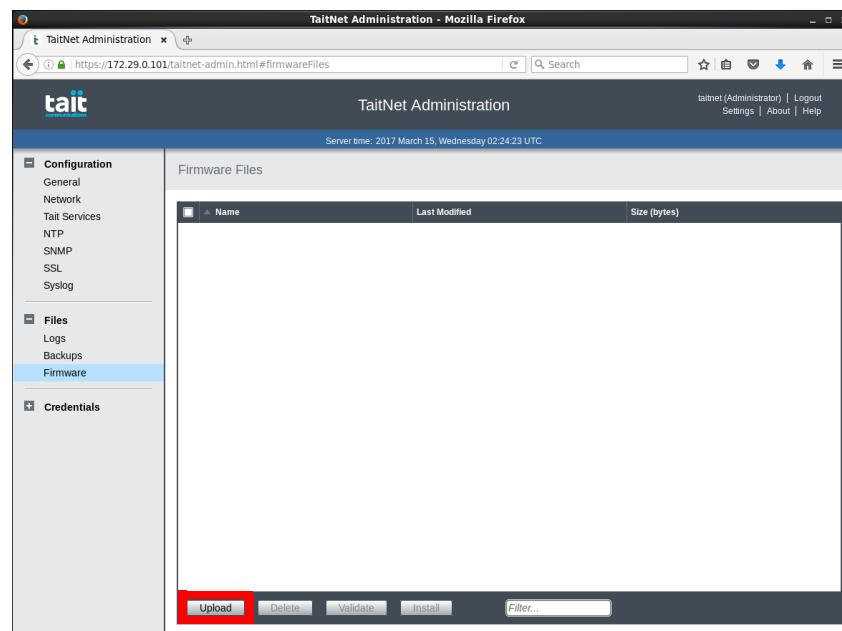
Notice The T1541 node controller uses secure HTTP by default (HTTPS). You may need to prepend your IP address with HTTPS:// in your browser to access the WebUI.



3. Log in with `taitnet` as the username and `taity` as the password.

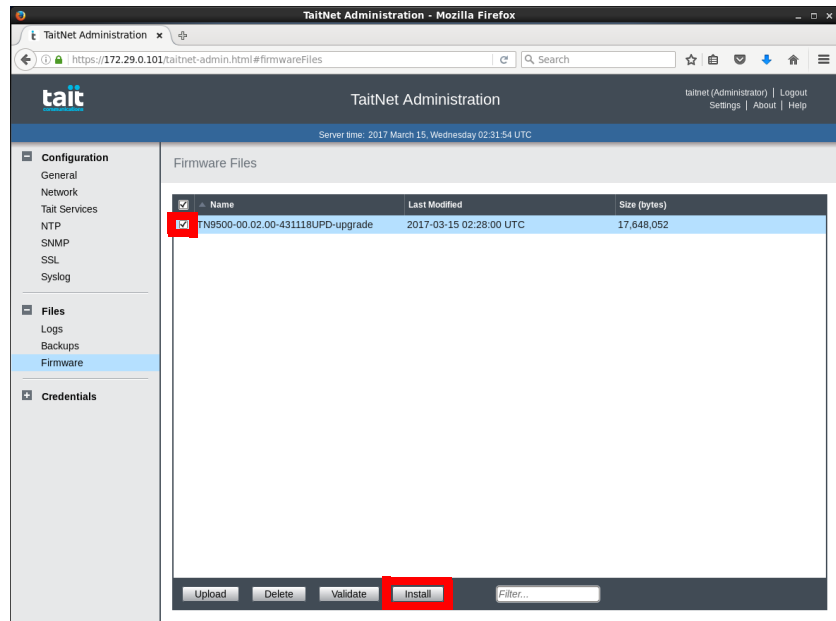


4. Select Files > Firmware from the left column menu.

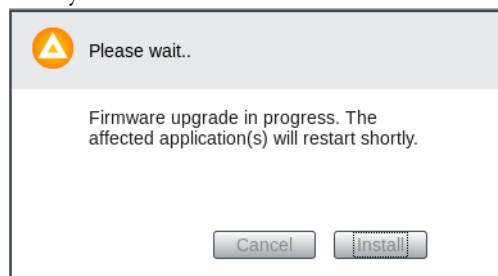


5. Click Upload, then click Choose file to select the T1541 Node Controller upgrade package for installation. Navigate to the location of the T1541 Node Controller firmware upgrade package and select the file. The T1541 Node Controller firmware package file name will be in the format: `Q1541NC-<version number>.rhel6`

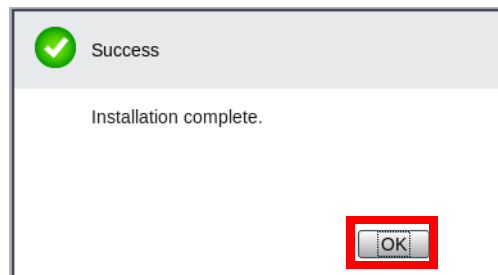
6. Select the upgrade package by clicking the box next to the name of the upgrade package, then click Install. (Ignore the filename in the following diagram, which is only an example of how to install a firmware file.)



7. A confirmation box will appear. Click Install to continue. The installation may take several minutes while the software is installing.



8. A dialog box will appear when the installation has finished and will indicate if the installation was successful or not. Click OK to finish the installation.



- To confirm a successful installation, select Configuration > Tait Services from the menu in the left hand column. There should be at least 3 services listed with them all showing a service status of Running.

Tait Services						
Product Name	Version	Size (kB)	RAM (%)	CPU (%)	State	
<input type="checkbox"/> TaitNet Administration	01.02.03.441187-REL	8,396	0.1	0.2	Running	
<input type="checkbox"/> TaitNet E1/T1 Gateway	01.04.01.445684-UPD	0	0	0	Running	
<input type="checkbox"/> TaitNet UnifyNetwork Gateway	01.04.02.446248-mod542	0	0	0	Running	
<input type="checkbox"/> TaitNet Transcoder	01.02.02.445686-UPD	0	0	0	Running	

Stop Start

3.1.1 Installing License Files

A node controller must have a valid license file installed before it can operate.

License files can only be generated by Tait and each node controller must have its own unique license. If the node controller has been set up by Tait then an appropriate license file will have been installed.

Obtaining the Hostid The hostid can be found on the Configuration > General page in the Administration application WebUI.

3.1.2 Obtaining the license.dat File

Once you have provided the hostid and required features to Tait, you will be provided a license file called `T1541-00_XXXXX_YYYY.lic` for the node controller.

If you are getting multiple licenses, you may combine the license files into one file that can be installed on all the node controller. Because the license file is a text file, you can easily combine the information, but each line must be the full text from the original file. Each node controller will only use the line in the license information that matches its hostid.

3.1.3 Installing the Node Controller's License File

- Rename the supplied license file (`T1541-00_XXXXX_YYYY.lic`) as `license.dat`
- Manually copy the license file to the node application directory on the node controller (`/home/taitnet/mptnc`) by using SCP.

3. You will need to restart the node controller via the administration application or by entering the command:
service tait_mptnc restart

4 Configuring the Serial Port Server

4.1 CentOS Systems

The DigiPort software is installed as part of the node controller software package.

The following steps should be taken to configure the serial port server.

1. Use an SSH terminal application to connect to the IP address of the node controller.
2. Log on using **taitnet** for the username and **tait** for the password.
3. At the prompt enter:

```
su -
```

4. You will be prompted for the root password. The default is K1w1k1w1.
5. Enter a command in the following format to add the serial port server:

```
dgrp_cfg_node init <id> <serial port server IP address> <number of ports>
```

e.g. entering

```
dgrp_cfg_node init a 172.29.1.250 32
```


will create serial port devices named /dev/ttya00 to /dev/ttya31 for the 32-port etherlite at 172.29.1.250

6. To add additional serial port devices use a different id.

e.g. entering

```
dgrp_cfg_node init b 172.29.1.251 16
```

will create serial port devices named /dev/ttyb00 to /dev/ttyb15 for the 16-port etherlite at 172.29.1.251.

 The `serial.cfg` template files that are installed in the `/home/taitnet/mptnc` folder have default mappings for device ids a and b. These files will need to be edited if more combinations are required, to enable the addition of more serial port devices.

7. Change to the application folder, `/home/taitnet/mptnc` by entering:

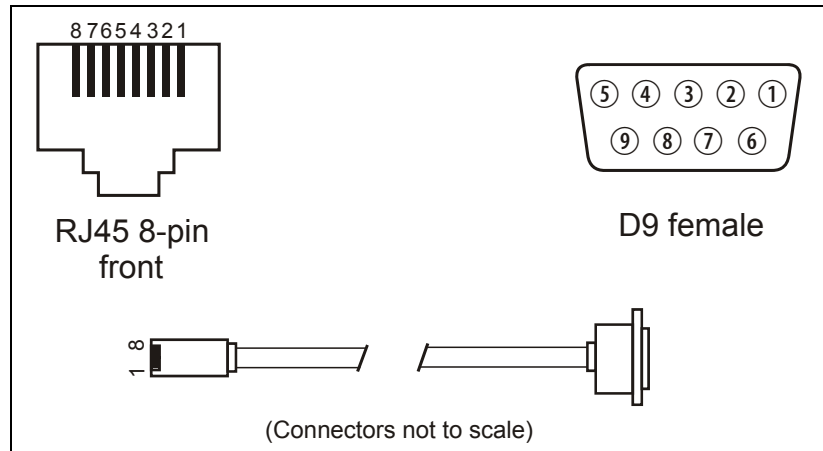
```
cd mptnc
```
8. To confirm that the node is configured to use the correct serial port server, enter

```
./config
```

This will list the `ta1t_mptnc.cfg` file, which will contain a line such as `import : serial.cfg.e132` for a 32-port server. Edit the line as required.

4.2 Digi EL Series Serial Port Server Configuration

To program the Digi EL you will need to connect it to a PC with a serial cable. The pin-outs for this cable are shown in the table below:



RJ-45 pin	Signal	Direction	DB-9 pin	Signal
4	RxD	←	3	TxD
5	TxD	→	2	RxD
7	DTR	→	6/1	DSR/DCD
6	SG	↔	5	SG
1	RTS	→	8	CTS
8	CTS	←	7	RTS
3	DCD	←	4	DTR

The DB-9 connector should be connected to a serial port on the PC. The RJ-45 connector should be connected to port 1 on the Digi EL.

To communicate with the Digi EL, you will need a terminal program (for example; HyperTerm) on the PC. Set the serial port to operate at 19,200 baud, 8 data bits, 1 stop bit, no parity and no hardware flow-control.

You will also need the following:

- The MAC address of the Digi EL (look for the label on the underside of the Digi EL)
- The IP address that you wish to assign to the Digi EL

- The IP address of the default gateway on your network
- The sub-net mask to be used on your network

Procedure

1. Remove the Ethernet cable and power cable from the Digi EL.
2. Connect the PC to the Digi EL using the serial cable and start the Terminal program.
3. Turn on the Digi EL by re-connecting the power cable.
4. Repeatedly depress the # key at the terminal until you get a console prompt. It should only take three keystrokes. A prompt will appear with the model number and the firmware version. For example:

```
--EL-32 V6.8--  
?
```
5. Enter the IP address with the command:

```
ip x.x.x.x
```

You can also store the default gateway (gw) and sub-net mask (sm) by entering:

```
gw x.x.x.x  
sm x.x.x.x
```

Where x.x.x.x are the actual numerical IP addresses.
6. Enter the command:

```
store
```

This command stores the IP address in flash memory.
7. Reboot the Digi EL module by unplugging, and then reconnecting the power cable.

You can test the IP address by powering on the Digi EL, and trying to ping it from the node controller.

You should attach a label to the Digi EL, showing the IP address stored in the unit.

4.2.1 Connecting to an SMM or DMM Site controller

Only three wires are connected, as shown in the table, other wires are cut at the SMM/DMM end of the cable.

Digi EL series				SMM or DMM		
RJ45 pin	Color ¹	Signal		Signal	Color	RJ45 pin
1	blue	RTS		n/c	n/c	1
2	orange	DSR		n/c	n/c	2
3	black	DCD		n/c	n/c	3
4	red	RXD		GND	yellow	4
5	green	TXD		RXD	green	5
6	yellow	GND/SG		TXD	red	6
7	brown	DTR		n/c	n/c	7
8	white	CTS		n/c	n/c	8

1. Colors may differ, depending on the cable used.


4.3 Digi TS Series Serial Port Server Configuration

The MAC address of the device is printed on the device label. You will need it to configure the device.


Procedure

1. Link the device to a PC using a standard Ethernet cable.
2. Load the Software and Documentation CD supplied with the device.
3. Click `setup.exe`. This launches a setup Wizard. It will detect and list the MAC address of all Digi TS devices on the network.
4. Select the device, click next.
5. Use the Wizard to configure the IP address, the default gateway, and subnet mask.
6. Configuring DNS parameters is optional. If preferred, these may be configured once the device is operational.
7. It is not necessary to configure the ports at this stage.

Notice The MAC addresses of all Digi TS devices on the network, configured or otherwise, will be displayed by the Wizard. It is essential to choose the correct device to configure. There is nothing to prevent you from reconfiguring an installed and operational TS device – and taking down part of your network as the result. You may wish to configure the device IP address before the device is installed to prevent any chance of this mistake. Refer to the following Note.

 It is not necessary to have the device installed in the network to configure its IP address. If there is a firewall installed on the network, you will not be able to do this, anyway. Instead, disconnect your PC from the network, and use your network cable to link to the device. Configure the device as above using the Wizard, but note that at the end of the configuration procedure, when the Wizard attempts to connect to the network, it will fail, and will report an error. Ignore the error, disconnect the device from your PC, and install it in the network.

8. Once the Digi TS is installed, link to it by putting its IP address in your web browser. Enter the login name **root** and password **dbps** and then use the web interface to configure the Digi ports. If you want to configure DNS settings at this stage, select Configuration > Network, and click DNS Settings. Enter the details as required and click Apply.

 The TS device web server is relatively slow to respond. Be patient. It works at “dial-up” speed.

4.3.1 Configuring the TS as a RealPort device

Procedure

1. Using the web interface, select Configuration > Serial Ports.
2. Enter the login name and password if requested, then click on the port you want to configure.
3. The Select Port Profile window displays. Select RealPort and click Apply.
4. The Serial Port Configuration window displays. Select Basic Serial Settings.
5. When the window displays, enter a suitable port description. Click Apply.
6. Click Return to Serial Ports, and repeat the procedure for other ports.
7. When all ports are configured, you must reboot the TS for your changes to take effect. Select Administration > Reboot. When the Reboot window displays, click Reboot. Rebooting the device takes about one minute to complete.

4.3.2 Configuring the TS as a TCP Sockets device

To use TCP Sockets requires Node Controller software Q1541NC v4.09.00 or later. Earlier Node Controller software allows only RealPort connections.

Procedure

1. Using the web interface, select Configuration > Serial Ports.
2. Enter the login name and password if requested, then click on the port you want to configure.

3. The Select Port Profile window displays. Select TCP Sockets and click Apply.
4. The Serial Port Configuration window displays. Do not select Automatically establish TCP connections.
5. Select Basic Serial Settings. When the window displays, enter a suitable port description.
6. These do not change: Baud Rate: 9600, Data Bits: 8, Parity: None, Stop Bits: 1.
7. Select Flow Control > None. Click Apply.
8. Select Advanced Serial Settings. When the window displays:
 - a. Select Allow multiple systems to simultaneously connect
 - b. Connections: 2
 - c. Control: select Exclusive
 - d. Select Enable connection timeout
 - e. 5000 msAll other Advanced Serial Settings fields retain their default settings. Click Apply
9. Click Return to Serial Ports, and repeat the procedure for other ports.



The changes made to the TCP sockets Advanced Serial Settings are essential for High Availability node operation. Without these changes, HA switchover will not occur.

10. When all ports are configured, you must reboot the TS for your changes to take effect. Select Administration > Reboot. When the Reboot window displays, click Reboot. Rebooting the device takes about one minute to complete.

4.3.3 Connecting to an SMM or DMM Site controller

Only three wires are connected, as shown in the table, other wires are cut at the SMM/DMM end of the cable.

Digi TS series				SMM or DMM		
RJ-45 pin	Color ¹	Signal		Signal	Color	RJ-45 pin
1	blue	DSR/DCD			n/c	1
2	orange	RTS			n/c	2
3	black	GND			n/c	3
4	red	TXD	←	GND	black	4
5	green	RXD	←	RXD	red	5
6	yellow	SG	←	TXD	green	6
7	brown	CTS			n/c	7
8	white	DTR			n/c	8

1. Colors may differ, depending on the cable used.

4.4 Configuring a Digi TS Series Port for SMM Diagnostics

- Procedure**
- Using the web interface, select Configuration > Serial Ports.
 - Enter the login name and password if requested, then click on the port you want to configure.
 - The Select Port Profile window displays. Select Console Management and click Apply.
 - Select Basic Serial Settings. When the window displays, enter a suitable port description.
 - Select Baud Rate: 115200
These do not change: Data Bits: 8, Parity: None, Stop Bits: 1.
 - Select Flow Control > None. Click Apply.

4.4.1 Connecting to a SMM Diagnostics Port

Only five wires are connected, as shown in the table, other wires are cut at the SMM end of the cable.

Digi TS series				SMM or DMM		
RJ-45 pin	Color ¹	Signal		Signal	Color	RJ-45 pin
1	blue	DSR/DCD			n/c	1
2	orange	RTS			n/c	2
3	black	GND			n/c	3
4	red	TXD	↘	GND	black	4
5	green	RXD	↙	RXD	red	5
6	yellow	SG	↘	TXD	green	6
7	brown	CTS	↙	CTS	orange	7
8	white	DTR	↘	RTS	brown	8

1. Colors may differ, depending on the cable used.

5 Configuring the Node Controller

5.1 CentOS Systems

The following basic configuration procedures are done from the TaitNet Administration application, and are indispensable to successful server and application operations.

5.1.1 Network Time Protocol (NTP)

1. Using a web browser, login to the Administration application.
2. Select Configuration > NTP.
3. Select Edit.
4. Enter the IP addresses of up to three NTP servers.
5. Press Save.
6. Press Start to begin the NTP daemon service.
7. Pressing Synchronize will check the status of the synchronization of this server with at least one of the NTP servers specified.
8. Use the status area to monitor the state of the NTP service.

5.1.2 SNMP

The T1541 can be monitored via its own MIBs and the server in general can be monitored using the standard UCD-SNMP-MIB (CPU, memory and disk statistics and system uptime).

1. Using a web browser, login to the Administration application.
2. Select Configuration > SNMP.
3. Select Edit.
4. Add or change the Read-only community string and enter up to two IP addresses to which SNMP traps will be sent.
5. Click Save.
6. Click Start to begin the SNMP daemon on this server.
7. Use the status area to monitor the state of the SNMP service.

5.1.3 Syslog


1. Using a web browser, login to the Administration application.
2. Select Configuration > Syslog.
3. Click Edit.
4. Enter the IP addresses of up to two external syslog collectors.
5. Select the protocol to use for the formatting of the syslog messages.
6. Select the level of information required for syslog collection. Use the check box to enable the collection of audit trails. Use the Internal logs dropdown menu to select the level of logs to be collected, if any.

 The levels above the one selected are also included (e.g. selecting Critical will also include logs from the Alert and Emergency levels).

7. Click Save.

5.1.4 Users


The Administration application is used to configure centralized authentication, where required, and to create local user login entries.

 It is recommended that local users should not be created if centralized authentication is used on your server.

5.1.5 Centralized Authentication

Connections to the server can be authenticated by a remote (i.e. centralized) service. Two remote authentication protocols are supported: LDAP and RADIUS.

Changes here should only be made by people experienced with the AAA architecture and authentication protocols.

 Any changes made to the authentication settings will result in all currently logged on remotely-authenticated users being logged out.

1. Log on to the Administration application.
2. Select Credentials > Authentication and click Edit.
3. Select LDAP or RADIUS as required from the Remote drop down menu.
4. Enter LDAP or RADIUS server details as required.
5. Click Save.

5.1.6 Local Users

1. Log on to the Administration application.
2. Select Credentials > Users and click Add. (To add a user you must have the Administrator access level.)
3. Enter a name into the Username box. This is the name that the user must enter to log in. A user name can be up to 140 characters long, spaces are permitted, but the following characters are illegal: * ' " \ () & | ! = ~ < > , ;
4. Enter the user's full name into the Name box. Control characters are illegal (ASCII 0-31 and 127). When the user logs in to the server, it will display this name at the top of the page.
5. Optionally enter a comment.
6. Select the appropriate access level for the user.

5.2 Node Configuration

To configure the Node Controller, use the `config` script.

- Log in as `root` and enter the following commands:

```
cd /home/taitnet/mptnc
service tait_mptnc stop
./config
```

You can also run `config` when logged in as `taignet` but you will not be allowed to configure the serial port.

Usage

You will be asked a series of questions. The range of acceptable values will appear in brackets. A default value may be shown within square brackets. If you are happy with the default response, just hit enter. For example:

```
Is this correct (y/n) [y] ?
```

The two valid responses are shown in brackets (y/n). The default response is shown in square brackets [y].

5.2.1 Configuration Procedure

The `config` utility is designed to be self explanatory. It is called explicitly at the prompt. It is designed to be called by `root` by entering `/home/taignet/mptnc/config` but can be called by the `taignet` user entering `config`.

Some configuration can be performed only by `root`, so if the `config` utility is called by the `taignet` user, the following section is skipped:

- configuring the serial port device

When the utility starts, a welcome banner is displayed and the existing `tait_mptnc.cfg` file (if any) is read and processed (this may take a few seconds). The user is then prompted to answer a series of questions.

For each group of parameters, the current parameter settings are displayed and the user is asked:

```
Is this correct (y/n) [y] ?
```

To accept the prompted `[y]` press Enter. Otherwise type `n` and press Enter.

If `n` is entered, each parameter in the group is displayed in turn and the user prompted to either accept the value or enter a new value. If there are minimum and/or maximum values for a numerical parameter, these are displayed in parentheses, with the minimum value first, then a dash, followed by the maximum value, for example: `(5-180)`. To accept the prompted value, press Enter, otherwise type the new value and press Enter.

The parameter settings are then displayed again and the user is asked:

```
Is this correct (y/n) [y] ?
```

To accept the prompted `[y]` press Enter. Otherwise type `n` and press Enter to accept or modify each parameter value again.

Not every parameter value is displayed. Parameters that are irrelevant to the specific installation are skipped. For example, if the user chooses a `standalone` node, high availability node parameters are not displayed. Likewise, when the user selects a numbering mode, only parameters relevant to that numbering mode are then displayed.

When the `config` utility completes, the new `tait_mptnc.cfg` parameter file is written and a goodbye banner is displayed.

For additional information about each parameter, please refer to [Section 5.2.4 Configuration Parameters on page 42](#). The parameters are listed in the same order as the user is expected to encounter them in the `config` utility.

5.2.2 Serial Device File Configuration

The information in this section relates to the serial device file chosen during the configuration procedure. During node installation the following device files are installed in the `taidnet` directory:

- `tait_mptnc.cfg.e132`
- `tait_mptnc.cfg.e116`
- `tait_mptnc.cfg.e18`
- `tait_mptnc.cfg.ts2`

Assuming you are executing the configuration utility as `root`, you have the opportunity to select or modify which serial device file is used by this node. You are asked: Enter the number of EtherLite or TS serial ports

(2, 8, 16 or 32). The number you enter in response to this question is used to select the device file from the above list.

Each device file maps the allocation of COM ports to real devices in `/dev/ttya`. You can view this allocation by displaying the contents of the file (using `cat` or `more`).

In exceptional circumstances it may be necessary to edit a serial device file to create the mapping required for your installation, but this should be done only after first consulting Tait support.

- ① Serial device file configuration is required only if you are using the serial port server as a RealPort device. If you are using the serial port server as a TCP Sockets device, the Serial device file is ignored. Refer to [Section 4 Configuring the Serial Port Server](#) for further information.

5.2.3 Node Controller Parameter Definitions

The node controller is configured through the use of control parameters. The values of these parameters are held in the following file:

```
/home/taitnet/mptnc/tait_mptnc.cfg
```

The node configuration file is generated automatically during the installation process. To re-configure the node controller, or to activate certain special features, you can use the `config` script, as described in [Section 5.2.1 Configuration Procedure on page 40](#).

Alternatively, you may edit the file by hand. Each line of the file contains either:

- A control parameter and its value
- A comment, these lines begin with the `!` character
- Nothing, i.e. a blank line

- ① The configuration parameters described in this section are designed to be used with Q1541NC v5.00 or later. If using earlier software, some of the parameters may not be available.

5.2.4 Configuration Parameters

Each line in the configuration file contains a parameter-value pair. Parameters and values are separated by the colon (`:`) character. Where the name used to describe the parameter in the `config` utility is significantly different to the name given to the parameter in `taait_mptnc.cfg`, the name used in the `config` utility has been added in *italics* to assist the user.

The meaning of each parameter is outlined below:

Node.Number

This parameter is used to specify the node number. Each node on a network has a unique identifying number in the range 0 - 31.

PrimaryNode

This parameter need only be specified if the node controller is one of a high-availability pair. It is used to specify whether the node controller is the primary or the backup. Set it to either:

- 1 - this is the primary node controller
- 0 - this is the backup node controller

ActiveNodeIP

This parameter need only be specified if the node controller is one of a high-availability pair. It is used to set the IP address, sub-net mask and gateway address that the node controller will adopt when it is operating in the active state. Set it to the following:

<IP address> <sub-net mask> <gateway IP address>

For example:

ActiveNodeIP: 172.27.1.48 255.255.255.0 172.27.1.255



In the config utility the ActiveNodeIP parameter is generated from the replies to three questions:

Enter the active node IP:

Enter the active node netmask:

Enter the active node gateway:

PeerNodeIP

This parameter need only be specified if the node controller is one of a high-availability pair. This is used to set the IP address of the other member of the pair.

HA.SeparateDasBins

If enabled (1), a node controller in standby mode will attempt to activate and monitor its DAS. If successful, this DAS is in an active but idle state. It is not performing any call functions, but it is actively monitoring its DAS ports. This parameter must be enabled only in High Availability nodes with full duplicated DAS (not one DAS with two Embedded Controller Cards). High Availability nodes with full duplicated DAS are known as 'Option 4' High Availability nodes.

RestartSerialPortDriver

This parameter need only be specified if the node controller is one of a high-availability pair. If this is set to the default of 1 (recommended), the EtherLite drivers will be restarted when the node controller becomes active. Set this to 0 to disable this feature.

NumberingMode

This parameter is used to specify the numbering scheme to be used on the network. The numbering scheme defines how radios are addresses on the network. This parameter can be set to one of the following values:

- 0 - MPT1343
- 1 - ANN
- 2 - CPSx

NumberingMode.CPS.L

NumberingMode.CPS.M

NumberingMode.CPS.S

These parameters need only be specified if the numbering mode is set to 2 (CPSx). They are used to define the values of the parameters L, M and S.

- L can take any value in the range 0 to 10
- M can take any value in the range 0 to 10, where $M \geq L$ and $M \leq S$
- S can take any value in the range 0 to 10, where $S \geq M$

NumberingMode.ANN.FPP

NumberingMode.ANN.MEP

These parameter need only be specified if the numbering mode is set to 1 (ANN). They are used to define the default values of the parameters FPP and MEP.

- FPP can take any value in the range 0 to 10
- MEP can take any value in the range 0 to $(10 - FPP)$

These values will apply over all prefixes except for up to seven user defined prefixes as defined using the following parameters:

NumberingMode.ANN.0.PFIX

NumberingMode.ANN.0.FPP

NumberingMode.ANN.0.MEP

These parameters can (optionally) be specified if the numbering mode is set to 1 (ANN). They are used to specify values of FPP and MEP that differ from the default values. These values apply in the specified prefix.

You can specify FPP, MEP values for up to 7 specific prefixes. They are specified as follows:

```
NumberingMode.ANN.n.PFIX: <prefix>  
NumberingMode.ANN.n.FPP: <fpp>  
NumberingMode.ANN.n.MEP: <mep>
```

Where:

- n is a number in the range 0 to 6
- <prefix> is the prefix, a value in the range 0 - 127
- <fpp> Can be any value in the range 0 to 10
- <mep> Can be any value in the range 0 to (10 - FPP)

import

This parameter is used to specify the file that contains the settings for the serial port server. Set this to the name of the file, can be one of four values:

- serial.ts2 for a 2-port Digi ConnectPort TS
- serial.e18 for an 8-port EtherLite or Digi ConnectPort TS
- serial.e116 for a 16-port EtherLite or Digi ConnectPort TS
- serial.e132 for a 32-port EtherLite or Digi ConnectPort TS

LinkErrorAlarms (*Send alarm on link error*)

This parameter is used to specify whether a site-link error results in an alarm being generated. It can have one of two values, 0 or 1:

- 0 - Alarms are not generated (default).
- 1 - Alarms are generated.

Note that a site-link error indicates corrupt data on the intersite link. It is not the same as a site-link failure.

Node.DiskSpace.Min (*Send alarm on disk space below*)

This parameter is used to specify an amount (in MB) of free disk space that should be available on the node controller. Below this value the node controller will send an alarm to the NMT.

Set this parameter to an integer value. Default is 500 Mb, minimum is 50 Mb, maximum is 5000 Mb.

Node.DiskSpace.Die (*Kill node on disk space below*)

This parameter is used to specify a minimum amount (in MB) of free disk space that should be available on the node controller. Below this value the node controller will shutdown.

Set this parameter to an integer value. Default is 10 Mb, minimum is 1 Mb, maximum is 100 Mb.

DaysToKeepDatabases (*Days to keep records and stats*)

This parameter is used to specify the number of days that call records and the site and DAS statistics should be stored. After this the data will be deleted.

Set this parameter to an integer value. Default is 30 days, minimum is 10 days, maximum is 90 days.

As the information stored in the Site and DAS statistics databases is viewed using the NMT, it is wise to use the same value in the NMT. So, if you change this parameter from its default value of 30, you should make the same change to the NMT configuration. Use a text editor, e.g. NotePad, to add the following line to %userprofile%\My Documents\Tait Applications\TaitNet NMT\config\NMT.cfg¹ and insert the changed value after the =.

```
Statistics.DaysToStore=
```

Save the change and restart the NMT.

LogAgeLimit (*Days to keep log files*)²

This parameter is used to specify the number of days that log files are stored on disk.

Set this parameter to an integer value (minimum is 5, maximum is 50). Default is 10 days.

LogSizeLimit (*Maximum size of log files*)

This parameter is used to specify the maximum size, in Mb³, of log files.

Set this parameter to an integer value (minimum is 5, maximum is 2000). Default is 100 Mb.

LogNumLimit (*Maximum log files per day*)

This parameter specifies the maximum number of log files that can be stored in a single 24 hour day. If set to a value greater than 1 (which is the default), each file will have the characters -xx appended to the file name, where xx is a 2 digit number starting from 00, used to identify the specific file. If the amount of logging generated exceeds this limit, then the most recent log file is deleted and overwritten. Maximum value is 99.

-
1. %userprofile% is a system defined path, often C:\Users*<username>*\
 2. With node version 4.07.xx or earlier, LogAgeLimit must be entered in seconds (not days). There are 86400 seconds in a day, so the time limits are minimum 432000, maximum 4320000.
 3. With node version Q1541NC 4.07.xx or earlier, LogSizeLimit must be entered in bytes (not Mb).

Notice The product $\text{LogAgeLimit} \times \text{LogSizeLimit} \times \text{LogNumLimit}$ must never exceed the amount of disk space available to store the logs. If the node computer runs out of disk space, the node software will crash and will not be able to be restarted until an operator deletes some of the log files.

The suggested log file size limit on the Kontron CG2300 is 50 Gb.

When using the config script to modify `tait_mptnc.cfg`, the product $\text{LogAgeLimit} \times \text{LogSizeLimit} \times \text{LogNumLimit}$ is displayed to the user.

DispatcherConsoleOverride

If enabled both here and in the DAS ECC, this parameter allows a dispatcher console to override a group call. When the E-line on a T1561-08 Conventional Interface card is asserted, all inputs into the DCC (digital conference controller), other than dispatcher inputs, are suppressed. The effect is similar to that of a broadcast call from the dispatcher.

Console override also enables loopback on all ECC ports⁴ except ports attached to a T1561-08 Conventional Interface card and set to Conventional mode. Also, console override enables two or more dispatcher consoles to override the same call, and to still hear each other's speech.

Dispatcher console override is not enabled by default.

i In the DAS, this feature significantly increases the number of calls routed via the DCC. If enabled, all voice calls are connected using the DCC. If disabled, the node connects 2-party calls using the DCS (digital crosspoint switch), and uses the DCC only for calls between 3 or more parties.

Notice Console override requires Q1561ECC firmware version 4.08 or later. If console override is required, this parameter must be enabled both here and in the DAS ECC (by enabling Advanced Options > Console Override active and by setting the Port Parameter for each port to which a dispatcher console is connected to 'FB'. All other ports should be set to 'FF').

i Networks with this feature enabled will usually also enable the feature 'Dispatcher can force clear group calls', which is set by a check-box in the NMT's *Node* > Configuration window.

V110OverNpd

This configuration parameter only applies if the DispatcherConsoleOverride parameter is set to y (yes).

-
4. Enabling console override automatically forces all ECC ports (except ports attached to a T1561-08 Conventional Interface card and set to Conventional mode) into loopback mode.

If V110OverNPD is enabled, this forces two party NPD calls to be routed via the DCS (Digital Crosspoint Switch), which will override the effect of DispatcherConsoleOverride.

Enable this parameter if either:

1. V110 is the protocol used during NPD calls
(e.g. -35 card in Async Data mode is connected to CMM at site)

or

2. TDP is the protocol, and radio to Dispatcher or Dispatcher to radio NPD calls should be supported
(e.g. -35 card in Modem mode is used by Dispatcher)

This restricts the behaviour of group NPD calls - see below.

Notice Enabling V110OverNPD restricts group NPD calls using TDP from working when only two ports are used. Specifically, radios on the same site as the transmitting radio will not receive NPD data.

SendNotHomeOnNotRegistered

If a caller dials what could be a valid radio address, but the address does not represent a radio present in the system database, the caller is sent ACKX qual 0 - this is usually displayed on the caller's radio as "Invalid Call".

If, however, the line: `SendNotHomeOnNotRegistered: 1` is added to the `tait_mptnc.cfg` file, then, in this circumstance, the caller is sent ACKV qual 0 - this is usually displayed on the caller's radio as "Not Home".

Mpt1343BcdDecode (*Decode SDMs to BCD on dispatcher*)

This parameter is used to specify how Short Data Messages (SDM) that are encoded as BCD appear on the dispatcher interface. It can have one of two values, 0 or 1:

- 0 - BCD encoded SDMs appear as type RAW on the dispatcher interface
- 1 - BCD encoded SDMs appear as type BCD on the dispatcher interface

See the T1541 Dispatcher Interface Protocol Manual (MNA-00014-xx) for more details about data types.

In version 3 node software, MPT1343 short data messages with coding types that were not understood by the node software, were presented to the dispatcher interface as type 'RAW'.

In version 4 node software, support for the SDM coding type 'BCD' was introduced. BCD coded SDMs were presented to the dispatcher interface as

type 'BCD' rather than 'RAW'. This caused problems for applications that required the BCD coded SDMs to be presented as coding type 'RAW'.

A facility has since been added to disable the version 4 behaviour and to force the node to present BCD coded SDMs as type 'RAW'. To disable the version 4 behaviour, add the following entry to the `tait_mptnc.cfg` file:

```
Mpt1343BcdDecode: 0
```

AbortGroupSdmToBusyGroup

By default this feature is enabled (1), and means that an SDM sent to a group address is not queued if the group is busy. To queue an SDM sent to a busy group, this parameter must be added and set to value 0.

ConvertSinglePartyGroupsToLocal (*Make a one site group call local*)

If enabled (1), when an intersite group call is set up as a single site group call because all other sites in the group call are not available (i.e. busy or failed, but not essential sites), then the call is converted to a local only group call and is handled at the calling site.

By default this parameter is not enabled (0) and single site group calls remain under node control.

Node.AbortConflictingCalls

By default, if a node receives a call request from a radio on a different site to the site that the radio is registered on (according to the node database), it will tell the site that received the call request to abort the call. The radio will need to register on the new site before making a call request.

By default this parameter is enabled (1). Disabling (0) this parameter speeds call setup when a unit moves between sites, but it increases the risk of dual registration. With nodes using Q1541NC version 4.08.00 and later, it is safe to disable (0) this parameter only in networks with no control channel frequency re-use and good (reliable) node to site links.

DMM.AllUnitsEnabled (*TNDS: Units enabled at startup*)

If enabled (1) in a system that is enabled for TNDS, all registered units will automatically be assigned a slot. This parameter is a 'work around' for systems that are unable to control the assignment of units to TNDS slots with third-party equipment that communicates with the node through the DIP interface.

NetworkCheckIPA

NetworkCheckIPB

These parameters are used by the node controller to perform automatic network integrity checks. The two parameters should be set to two different IP addresses on your network. The equipment with the specified IP addresses should be capable of being ‘pinged’. Every 5 seconds the node controller pings these addresses to check network integrity. The result of the check is written to the file `net-check.txt` as either `network-okay` or `network-failed`. If both pings are not returned then the node will enter a failed state.

If these parameters are left undefined or are absent from the configuration file, then the checks are not performed and the node does not enter the failed state.

NetworkCheckAttempts⁵ **(Attempts before network failed)**

This parameter determines the number of sequential failed Network Checks that must occur before the network is considered failed. The default value is 1, but values between 1 and 6 may be entered. As network checks occur every 5 seconds, if a value of 6 is entered, the network would be in a failed condition for 30 seconds before the node enters a failed state.

NetworkManager.Address

The value of this parameter should be a comma separated list of IPv4 addresses in dotted quad format of server NMTs that are allowed to connect to this node. If no value is supplied or the value is set to any, then the node will accept a request for connection from any server NMT.

To restrict access to the node, add this parameter and set its value to the IP address of the server NMT. While each network should have only one server NMT, a backup PC or client NMT that is to be used as the server NMT in the event that the primary server NMT fails should also have its IP address listed here.

ActivationTimeout (*Standby node activation timeout*)

Default 20 (seconds). The number of seconds that a standby node waits when it is no longer receiving ‘keep alive’ messages from the active node before it takes over as the active node. This is to prevent the standby node going active with an intermittent network fault.

5. Parameter added in Q1541NC v4.11.00

StartupTimeout (*Node startup timeout*)

Default 60 (seconds). The number of seconds that a node waits after starting before it tests the Node - DAS and Node - Site links and reports link error to the NMT.

5.2.5 Additional Configuration Parameters

These parameters are not processed in the config utility. If required, they must be added or modified by editing the `tait_mptnc.cfg` file 'by hand'. Indiscriminate use of these parameters is likely to break the node software with undefined consequences. Modification of these parameters must occur only if authorised by a senior support engineer at Tait support.

MonitorComPort

Default 0. If set to a non-zero value, the node sends a text string with node status information out from the defined serial port every second.

The format of the text is:

```
<year><month><day> <hour>:<minute>:<second> <statusText>
```

where *<statusText>* is one of:

- DISABLED
- ACTIVATING
- ACTIVE
- STANDBY
- PROGRAM
- FAILED
- DAS_FAILED
- NETWORK_FAILED
- LICENSE_FAILED
- UNKNOWN

The receiving equipment should be set to:

- Baud - 9600
- Parity - none
- Flow control - none
- Data bits - 8
- Stop bits - 1

This information may be used by third-party equipment to switch the MUX equipment from the primary node to the backup node and back again in the event of node failure.

CheckConflictingRegistrations

Default is enabled (1). If the unit is registered on another site with the same control channel frequency as this site, then the registration manager⁶ will not accept the unit registration but instead demand an ESN check immediately. When the registration manager receives the ESN report it then accepts the unit registration on the new site (and cancels the registration on the previous site). This feature prevents dual registration from occurring in almost all cases. Dual registration is highly undesirable, and for this reason Tait strongly discourages

6. In any network, the lowest numbered active node is the registration manager.

users from disabling (0) this feature. On networks where there is no control channel re-use, this parameter is ignored.

DipMpt24ByteSDM

Default is enabled (1). Determines how the number of codewords in an SDM transmitted or received on the DIP interface is calculated. If enabled (1), this is determined by the value of the LEN parameter (located in data byte 7, bits 7 and 6). If disabled (0), this is determined only by the number of bytes of data in the SDM.

Device.Handshake

This parameter sets the serial port handshaking protocol

Value	Meaning
0 (default)	none
1	RTS/CTS
2	RTS/CTS/DTR

ForwardRegsToGateway

Default is enabled (1). If there is a gateway-site on this node and the unit's registration did not come from the gateway-site and the radio is allowed on this gateway-site then forward the registration notification to the gateway. (If no gateway-site, this parameter does nothing.)

GroupCallsOnHoldTimeoutForInactivity⁷

Default is enabled (1). If disabled (0), in networks with more than one dispatcher, group calls may not timeout for inactivity, as they may be 'held up' by a dispatcher (or dispatchers) that did not answer and was not involved in the call.

InterimCallRecordsSize

Default is 1000. Interim call records store node call information until call record data arrives from the site. This is the maximum number of interim call records to store. If this number is exceeded, the oldest record is deleted.

MaxConferenceSize

Default is 50 when the DAS ECC has firmware version 4.07 or later, and 32 otherwise. The ECC has 4 conference controllers, so the number of conference ports is 4 times this value.

Node.DispatcherIncludeCalls

The dispatcher include calls feature allows a dispatcher operator to include other radios or groups into a radio to dispatcher call. The feature is enabled (1) by default, but cannot be used unless it is also enabled in the site configuration parameters and the dispatcher supports this feature. The feature is designed for single node networks only. It is safe to leave this parameter enabled even if the include call feature is not required as it will be ignored unless enabled at the sites. Disabling (0) this feature is required only if there is an error in the include calls logic.

Node.InhibitPooledChannelAlarm

Default is enabled (1). If a call to a site fails because all available pooled channels are busy, this is normally not a fault, so no alarm is generated. However, if problems with pooled

7. New in Q1541NC version 4.09.00.

channels are suspected it may be useful to flag all instances where calls fail due to lack of pooled channel resource. Add this parameter and set the value to 0.

RCGAGatewayIdent

Default is 8136. The ident to which units send group affiliation request SDMs.

ResetAllPortsOnLinkUp

Default is disabled (0). If enabled (1), whenever the Node to DAS link goes from the 'link down' to the 'link up' state, a command is sent to the DAS ECC to reset all DAS port cards.

Site Link Parameters

These parameters are used with sites using SMM software earlier than Q1722SMX v7.30

The first three parameters set link values when "Enable slow poll mode" is not enabled in the NMT's *Site > Configuration* window. The default values mean that the site link may be in a failure condition for approximately 12 seconds before it is reported as failed.

The other three parameters set link values when "Enable slow poll mode" is enabled in the NMT's *Site > Configuration* window. The default values mean that the site link may be in a failure condition for approximately 2 minutes before it is reported as failed.

Reply time is the minimum time to wait after receiving a message or acknowledgement before sending another message.

Poll time is the maximum time to wait for a message acknowledgement before deeming that the message is lost.

Retries is the number of times to attempt to send a message before deeming that the link is broken.

Name	Default Value	Units
SiteReplyTime	10	milliseconds
SitePollTime	500	milliseconds
SiteRetries	24	
SiteSlowReplyTime	200	milliseconds
SiteSlowPollTime	5000	milliseconds
SiteSlowRetries	24	

When sites are using SMM software Q1722SMX v7.30 or later, the parameters SiteLinkRetryTime and DmmRetries set the site link values.

SiteLinkRetryTime

Used only with SMM v7.3x. Value in milliseconds. If set to 0 (default), the value that is used depends on the link speed as in the table:

Link speed (baud)	Retry time (milliseconds)
1200	3000
2400	2000
9600	1000

Timeouts

Name	Default	Units
Node.ESN.PollingTimeout	1	seconds
Node.Stun.PollingTimeout	10	seconds
Node.Recover.PollingTimeout	10	seconds
Node.Regroup.PollingTimeout	10	seconds
Node.MemoryRead.PollingTimeout	10	seconds
Node.ValidationRead.PollingTimeout	10	seconds
Node.Timeout.DiskSpaceCheck	10	minutes
MinsToKeepInterimCallRecords	60	minutes
PortAssociationsCheck.FrequencyMinutes ¹	5	minutes
Ini.InboundSocketTimeout ²	30	seconds

1. The frequency with which the node checks and updates DAS port to channel controller associations.
2. New in Q1541NC v4.11.00. Used for the listening socket of a lower-numbered node. Tear down and recreate the socket if timer expires without a connection getting established.

Line testing

Name	Default value	Units	Notes
LineTest.Freq	420	Hz	
LineTest.TestLevel ¹	10	-dbm	min 1, max 127
LineTest.NullLevel ¹	90	-dbm	min 1, max 127
LineTest.Period	1	seconds	min 1

1. Line tests are performed at both the test level and the null level. The null level is a background level.

Port Assignments

Name	Default value	Notes
NetworkManager.Port	9012	NMT
DispatcherInterface.Port	9005	DIP
DispatcherMonitorInterface.Port	9013	DIP monitor

DMM Parameters

Name	Default value	Notes
DmmRetryTime	0	
DmmRetries	10	When site software Q17225MX v7.3x is used, this parameter also sets the number of site retries.
Dmm.Sync	0xb433	
Dmm.TxDataPacketSize	14	
Dmm.RxDataPacketSize	12	
Dmm.TxldLocation	4	
Dmm.FillerSize	2	
Dmm.OverTheAirSpeed	1	
Dmm.TransmitReceivedData	0	

SNMP

Name	Default value	Notes
SnmpAlarmTrapSendIntervalMs	1000	Defaults send max. of 50 traps per second
SnmpAlarmTrapsSentPerCycle	50	
SNMP.ShowMissingData	0	

Test Modes

Name	Default value	Notes
TestMode.PooledChannels	0	
TestMode.Conf	0	
TestMode.Alarm	0	

5.2.6 Example tait_mptnc.cfg File

The contents of a typical configuration file are presented below:

```
! TaitNet Node Configuration file

! The node number. If this is changed on a node that has been used,
! the registration database will become invalid.
Node.Number: 7

! Set to 1 if this is a standalone node or the primary node of a
! high availability pair. Set to 0 if this is a backup node.
PrimaryNode: 1

! Set to 0 for MPT1343, 1 for ANN or 2 for CPSx
NumberingMode: 0

! The node will try to open the serial port device specified here.
import: tait_mptnc.cfg.el32

! The name of the network interface.
EthernetInterface: nge0
```

```

! If enabled, generate an alarm when a link error is detected.
LinkErrorAlarms: 0

! If the amount of free disk space falls
! below this value(in MB), raise an alarm.
Node.DiskSpace.Min: 500

! If the amount of free disk space falls
! below this value(in MB), the node will shutdown.
Node.DiskSpace.Die: 10

! Keep call records, site and DAS stats for this many days.
! Older databases will be deleted.
DaysToKeepDatabases: 30

! The number of days to store node logs for.
LogAgeLimit: 10

! Maximum size of any single log file.
LogSizeLimit: 100

! Maximum number of log files to store stored in a single 24 hour
! day. If set to a value greater than 1 each file will have -xx
! appended, where xx is a 2 digit number starting from 00, used to
! identify the specific file. If the amount of logging generated
! exceeds this limit, then the most recent log file is deleted and
! overwritten.
LogNumLimit: 1

! Used to control if dispatcher can override an existing conference
! they have joined. Note: forces all calls to use the conference
! controller.
DispatcherConsoleOverride: 0

! Used if console override is enabled and the system uses V110 over
! NPD. Note: forces one and two party NPD calls not to use the
! conference controller
V110OverNPD: 0

! Used to control the response to a radio that attempts
! to call a radio that is not registered.
! If set to 0, ACKX qual 0 (invalid call) is sent to the calling
! party. If set to 1, ACKV qual 0 (not home) is sent to the calling
! party.
SendNotHomeOnNotRegistered: 0

! Used to control how SDMs with BCD encoding
! are presented on the dispatcher interface.
! If set to 0, BCD encoded SDMs are presented as type 'RAW'.
! If set to 1, BCD encoded SDMs are presented as type 'BCD'.
Mpt1343BcdDecode: 1

! If enabled an SDM sent to a Group address is not queued if the
! Group is busy. If not enabled an SDM sent to a Group address is
! queued if the Group is busy.
AbortGroupSdmToBusyGroup: 1

! If enabled, an intersite group call that is set up as a single site
! group call because all other sites in the group call are not
! available (ie. busy or failed, but not essential sites) then the
! call is converted to a local only group call and is handled at the
! calling site. If not enabled, single site group calls remain under
! node control.
ConvertSinglePartyGroupsToLocal: 0

! If enabled in a system that is enabled for TNDS, all registered

```



```

! units will automatically be assigned a slot. A 'work around' for
! systems that are unable to control the assignment of units to TNDS
! slots with third party equipment that communicates with the node
! through the DIP interface.
Dmm.AllUnitsEnabled: 0

! If enabled, when a node receives a call request from a radio on a
! different site to the site that the radio is registered on (in to
! the node database), it will tell the site that received the call
! request to abort the call. The radio will need to register on the
! new site before making a call request. Disabling this parameter
! speeds call setup when a unit moves between sites, but it increases
! the risk of dual registration. With nodes using v4.08.00 or
! later it is safe to disable (0) this parameter only in networks
! with *no* control channel frequency reuse and good (reliable) node
! to site links.
Node.AbortConflictingCalls: 1

! Ping the following addresses at 5 second intervals.
! If both pings fail, the node will enter the failed state.

NetworkCheckIPA: none
NetworkCheckIPB: none
NetworkCheckAttempts: 1

! A comma separated list of IPv4 addresses in dotted quad format of
! Server NMTs that are allowed to connect to this node. If no value
! or the value is 'any' then the node will accept a request for
! connection from any Server NMT.
NetworkManager.Address: 172.25.140.2,172.25.140.18

! The number of seconds that a standby node waits when it is no
! longer receives 'keep alive' messages from the active node before
! it takes over as the active node. Prevents standby node going
! active with an intermittent network fault.
ActivationTimeout: 20

! The number of seconds that a node waits after starting before it
! tests the Node - DAS and Node - Site links and reports link error
! to the NMT.
StartupTimeout: 60

```

5.2.7 Installing the run-active Script (optional)

When the node controller enters the active state, it searches for, and, if it exists, attempts to execute the run-active file located in the /user/taitnet directory. This file usually contains a script to alert third-party equipment that the TaitNet node is now active. It is not installed when the node controller software is installed, neither is its content specified. If required, it will be customer specific.

6 Node Upgrade Procedure

From time to time you will need to upgrade the node controller software. This will provide you the benefits of new features and bug fixes.

6.1 Upgrading T1541 Firmware

This is done from the TaitNet Administration application, using Q1541 gateway application upgrade packages.

1. Save the received upgrade packages to a PC.
2. Open the PC browser.
3. Enter the IP address of the Administration application.
4. Log in and select Files > Firmware.
5. Load, validate and install the Q1541upgrade package, using [Section 3.1 CentOS Systems](#) and/or the online help for assistance.

6.2 Upgrading the Operating System

This is done from the TaitNet Administration application, using only the supplied TaitCentOS upgrade packages. (The TaitCentOS package also includes the TaitNet Administration application.) This upgrade procedure may take up to 10 minutes and should only be done with care.

1. Save the received upgrade packages to a PC.
2. Open the PC browser.
3. Enter the IP address of the Administration application.
4. Log in and select Files > Firmware.
5. Load, validate and install the TaitCentOS upgrade package, using the online help for assistance.

7 Node Roll-back Procedure

7.1 Recovering from a Failed Firmware Upgrade

If a firmware upgrade has failed part way through (e.g. from a power cut), or fails to finish with the 'upgrade complete' message, the T1541 may be left in a state where attempts to re-install the upgrade from the WebUI will fail due to the T1541 believing the upgrade has been completed.

The following instructions describe how to recover from a failed upgrade of the T1541 firmware.

1. Log into the Administration application.
2. Select Files > Logs.
3. Check the `tait_upgrade` log file for one or more of the following messages (or similar):

- There are unfinished transactions remaining. You might consider running `yum-complete-transaction first` to finish them.
- Transaction Check Error: package `taitnet-mptnc-05.00.02_426778REL.el6.x86_64` is already installed

or the log file may end before all the expected messages/step have taken place, e.g. the end of the log file showing:

- Updating : `taitnet-mptnc-05.00.02_426780REL.el6.x86_64` 1/2

Which indicates that step 2/2 has not been executed.

4. To recover from this and guarantee a fully installed upgrade:
 - a. `ssh` into the Administration application with root privileges
 - b. Resolve any uncompleted yum transactions by entering:
`yum-complete-transaction`
 - c. Remove the package that the upgrade failed on (for the ING package enter):
`yum remove taitnet-mptnc.x86_64`

Re-install the upgrade package from the WebUI. As the configuration databases should still be intact, once the upgrade has been installed the configuration should automatically load back into the system.

8 Operating the Node Controller

This chapter tells you how to carry out basic maintenance and operational tasks by logging onto the node controller and using the CentOS command line interface and/or WebUI.

8.1 Logging on to the Node Controller Using SSH

You can connect to the node controller using an SSH terminal application.

1. Use an SSH terminal application to connect to the IP address of the node controller .
2. You should see the following prompt:
login as:
Enter **taitnet**.
3. You will be asked for a password, the default is **tait**. Enter the password and press enter.
You should now be logged on to the node controller using the default command shell (bash).
When you are ready to logout, enter **logout** or just press **Ctrl-d**.

8.2 Logging on to the Node Controller as 'root'

Some tasks can only be carried out if you are logged in as root. To do this you use the UNIX su command.

1. Logon as user taitnet as described above.
2. At the prompt enter:
su -
3. You will be prompted for the root password. The default is **k1w1k1w1**.
4. When you are done, press **Ctrl-d** to logout. You will switch back to being the taitnet user.

8.3 Administration Application Backups

Backup files in the Administration application contain server database and configuration settings. Backup files are created automatically.

To create a backup file


1. Select Files > Backups and then click Backup.
2. Give the server time to create the backup. The display will update to show the file that has been created.

To download a backup file

1. Select Files > Backups.
1. Click the name of the file you wish to download.
2. Save the file to a suitable location on your PC.


To upload a backup file

1. Select Files > Backups and then click Upload.
1. Select the name of the file you wish to upload.

 When the Upload button is used, the maximum file size that can be selected to upload is 700 MB.

To restore a configuration from backup

1. Select Files > Backups.
1. Click the check box to select the row of the file and then click Restore and confirm.

 The server automatically deletes backup files that are older than 30 days.


8.4 Advanced `taitnet.mptc` commands

When some of these commands are executed, a `console.log-<date>.log` file is created in the `logs` directory. Errors encountered during the execution of the command are listed in this file. Where specified, `<address>` must be entered in MPT1327 address format, with a / between the prefix and ident and with leading zeros omitted (unless the prefix is 0). For example: 2/824 0/1024 64/34

Notice Unless indicated otherwise, these commands should be used only when the node controller software is **not** running. Indiscriminate use of these commands, especially when the node software is running, can have unpredictable and undesirable outcomes.

`./tait_mptnc -cr <address>`

This command directly modifies the node registration database, and is used to remove information about where a radio was last registered from the network. If required, it should be used on the lowest numbered node in the network, and only when that node is not operational.

 TaitNet MPT networks **never** forget where a radio was last registered, even when the radio is switched off for an extended period or is decommissioned. Normally this is not a problem, but there are a few situations where it is necessary to completely remove a radio from the node database. The most common of these is when an address that was formerly assigned to a radio is to be assigned to a dispatcher.

`./tait_mptnc -cv <address>`

This command directly modifies the node validation database, and is used to remove information about the validation of a radio from the network. If

required, it should be used on the lowest numbered node in the network, and only when that node is not operational.

./tait_mptnc -b

Print version and build (equivalent to `taitnet build-version`).

./tait_mptnc -e

Print all registration database information (equivalent to `taitnet viewreg`).

./tait_mptnc -E <address>

Print registration information for `<address>` (equivalent to `taitnet viewreg <address>`).

./tait_mptnc -g

Print all RCGA database information (equivalent to `taitnet viewRCGA`).

./tait_mptnc -G <address>

Print RCGA information for `<address>` (equivalent to `taitnet viewRCGA <address>`).

./tait_mptnc -h

Print version number (equivalent to `taitnet version`).

./tait_mptnc -import-database

Refer to `taitnet import-database` for details.

./tait_mptnc -import-sqlite-database

Open the sqlite based NMT backup-database file used by node controllers v4.00.00 to v4.00.07 and import the data into the database used by node controllers from v4.00.08 on.

./tait_mptnc -l

Does nothing unless executed when the node is running. Causes all logging to be printed to the console, instead of the `node-<date>.log` file. Use of this command is not recommended without good reason.

./tait_mptnc -P

Print all validation database information (equivalent to `taitnet viewval`).

./tait_mptnc -p <address>

Print validation information for `<address>` (equivalent to `taitnet viewval <address>`).

./tait_mptnc -v

Print version number (equivalent to `taitnet version`).

Test modes

These are listed below for completeness only. For further information, refer to the Q1541NC source code.

./tait_mptnc -t -c

Load the database with 1000 call records.

./tait_mptnc -t -d

Load the database with 35 days of das statistics test data.

./tait_mptnc -t -r

Load the database with registration test data.

./tait_mptnc -t -s

Load the database with 35 days of site statistics test data.

```
./tait_mptnc -t -u
```

Load the database with validation test data.

```
./tait_mptnc -t -dc ...
```

Hex dump. Refer to source code.

```
./tait_mptnc -C
```

Print database checksums.

8.5 Directory Structure

The node software is installed in its own folder under the home directory of the user taitnet. This can be found in the following location.

```
/home/taitnet/mptnc
```

When you log in as taitnet you will automatically be placed in /home/taitnet. Change to the node controller directory:

```
cd mptnc
```

To see the contents of the directory, enter:

```
ls -l
```

You should see something like the following:

```
drwxrwxr--. 2 taitnet taitnet  4096 Jul 31 11:04 backups
-rwxrwx---. 1 taitnet taitnet  89239 Jul 31 11:04 config
drwxrwxr--. 2 taitnet taitnet  4096 Sep 26 00:00 db
-rwsrws---. 1 root    taitnet 131952 Jul 31 11:04 ipcfg
-rw-r--r--. 1 taitnet taitnet   231 May 29 13:15 license.dat
-rw-r--r--. 1 taitnet taitnet   251 Sep 26 21:43 license-request.txt
drwxrwxr--. 2 taitnet taitnet  12288 Sep 26 00:01 logs
-rwxrwx---. 1 taitnet taitnet   756 Jul 31 11:04 serial.cfg.el16
-rwxrwx---. 1 taitnet taitnet  1348 Jul 31 11:04 serial.cfg.el32
-rwxrwx---. 1 taitnet taitnet   461 Jul 31 11:04 serial.cfg.el8
-rwxrwx---. 1 taitnet taitnet   838 Jul 31 11:04 serial.cfg.ts2
-rwsrws---. 1 root    taitnet 956688 Jul 31 11:04 tait_mptnc
-rw-r--r--. 1 taitnet taitnet   7200 Aug  3 02:09 tait_mptnc.cfg
```

This is a list of all the files and directories in the current location. The first column details the file type and access permissions. The type is given by the first character, which can be one of:

- `a` the entry is a directory
- `l` the entry is a symbolic link to another file
- `-` the entry is a file

The last column is the file/directory name. A description of each file follows:

config

This is the script that generates the `tait_mptnc.cfg` file. Refer to [Section 5.2.1 Configuration Procedure](#) for more details.

db	db is short for database. The node controller uses this directory to store data such as unit registrations and call records. Each database file has a filename with the extension <code>.db4</code> or <code>.db5</code> .
ipcfg	<p>This is a program that allows the root user to change the network settings of the node controller. To use it enter:</p> <pre>ipcfg <action> <ip address> <subnet> <gateway></pre> <p>Where the parameters should be set as follows:</p> <ul style="list-style-type: none"> ■ <code><action></code> - set this to activate to start the network, or deactivate to stop the network ■ <code><ip address></code> - use this to set the IP address of the node controller ■ <code><subnet></code> - use this to set the sub-net mask to be used by the node controller ■ <code><gateway></code> - use this to set the IP address of the gateway to be used by the node controller
license.dat	This is the license file for the node controller software.
logs	The node controller uses this directory to store log files. In the event of a problem, Tait engineers will examine the log files to diagnose the cause.
net-check.txt	Every 5 seconds the node attempts to ping each of the addresses supplied in the <code>tait_mptnc.cfg</code> parameters <code>NetworkCheckIPA</code> and <code>NetworkCheckIPB</code> (see Section 5.2.4 Configuration Parameters). If both pings fail, this file will contain the text <code>network-failed</code> , otherwise it will contain the text <code>network-okay</code> . The text in this file has meaning only when <code>NetworkCheckIPA</code> and <code>NetworkCheckIPB</code> are defined in <code>tait_mptnc.cfg</code> .
tait_mptnc.cfg	This is the node configuration file. See Section 5.2.5 Additional Configuration Parameters for more details.
serial.el16 serial.el32 serial.el8 serial.ts2	These files are used to configure the serial port server.
taitnet	This is the script that is used to start and stop the node controller software.


9 Installing the NMT Software

This section describes how to install the T1541 Network Management Terminal (NMT) software onto a suitable computer.

Recommended system configuration

Essential for Server NMTs in multi-node or large single node networks:


- x86 compatible PC
- 2.8GHz processor
- 1 GB RAM
- Dual Flat Panel Video Display
- MS Windows XP Pro SP2

 Systems using MS Windows Vista¹ require a dual core processor and 2 GB RAM.

Minimum configuration

Suitable only for Client NMTs or Server NMTs on smaller networks:

- x86 compatible PC
- with 1Ghz processor
- 256 MB RAM
- MS Windows 2000 Professional

 Systems using MS Windows Vista require 1 GB RAM.

Supported legacy configuration

Please refer to the Issue 02 of this manual (MNA-00008-02):

- Sun Microsystems Ultra 5 or Sun Blade 100
- At least 512 MB RAM
- Solaris 8

9.1 Installation Procedure

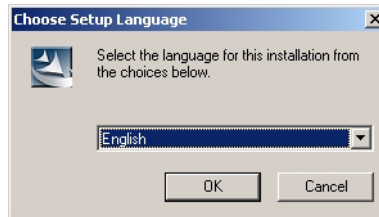
1. Close any applications running on the PC. Insert the NMT install CD.
2. There are two directories on the CDROM named `solaris` and `windows`. Navigate to the `windows` directory.

1. To use MS Windows Vista you require Q1541NMT v4.06.00 or later. To use MS Windows 7 you require Q1541NMT v4.08.01 or later.

3. Click on the application `TaitNet Network Management Terminal.exe`.

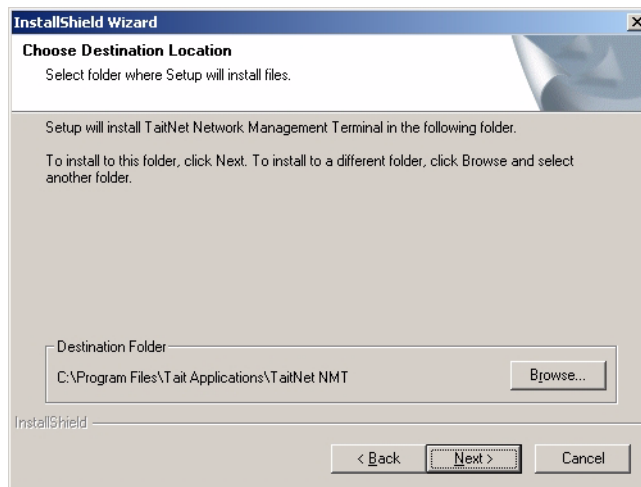


4. The application will start expanding the files needed for the installation. When this is finished you will be prompted to select the language to use for the installation.



Select English and click OK.

5. You will now be asked to choose the location into which the NMT will be installed.



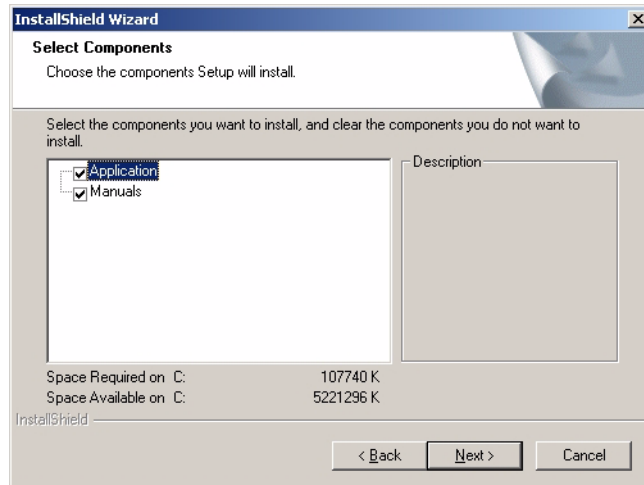
The default destination is:

`C:\Program Files\Tait Applications\TaitNet NMT`

If you are happy with the default, simply click Next. Otherwise, click

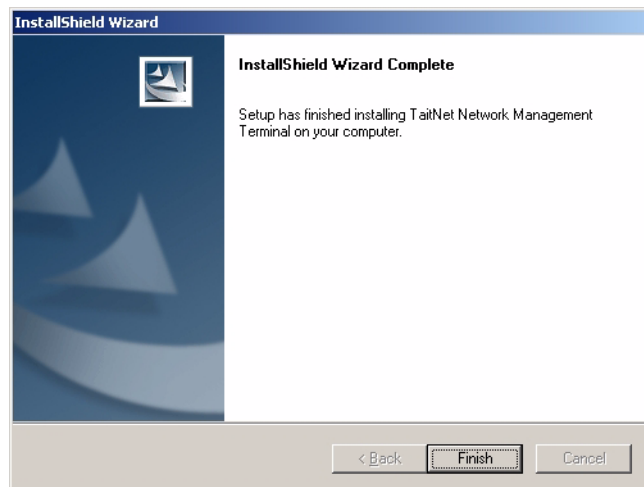
Browse to select a different location.

6. You will now be asked to choose which components to install. The options are Application and Manuals.



To install both components (recommended) simply click Next.

7. The installation will proceed. When it has completed, you will see the following screen:



Click Finish to complete the installation.

The NMT is now installed. A short cut will appear on your desktop:



8. A valid license file is required before you can use the NMT. One should have been provided to you on a floppy disk. If you do not have a valid license, contact Tait support.

The license file will be named either `license.dat` or `xxx.xxx.xxx.xx.lic`, where `xxx...` represents the IP address of the NMT computer. If the file is not named `license.dat`, it should be renamed.

Copy the license file from the license floppy disk into the install destination that you specified during installation. The default is:

```
C:\Program Files\Tait Applications\TaitNet NMT
```

9. **If using Windows Vista OS:** Both `TaitNet NMT.exe` and `java.exe` need to operate with Administrator privilege. Go to directory `C:\Program Files\Tait Applications\TaitNet NMT`. Right click `TaitNet NMT.exe` and select Properties. Tick the check box Allow To Run As Administrator, then click Apply and close the window. Then go to directory `C:\Program Files\Tait Applications\TaitNet NMT\jre\bin`. Right click `java.exe` and select Properties. Tick the check box Allow To Run As Administrator, then click Apply and close the window.
10. To start the NMT, double-click the shortcut icon on the desktop.

9.2 Running the NMT on a Computer Without a Sound Card

The NMT is designed to be run on a PC with sound card and speakers. If it is to be used on a computer without a sound card, then, after starting the NMT for the first time, open the file `%userprofile%\Documents\Tait Applications\TaitNet NMT\config\NMT.cfg2` with a text editor (e.g. Notepad) and add the line

```
NoSoundCard=true
```

Text in `NMT.cfg` is case sensitive and there is no whitespace in this line. Save the change, then stop and restart the NMT application. Failure to do this will result in a large number of unnecessary Exceptions logged, and, in a large network, the amount of additional logging generated may be enough to impair NMT performance.


9.3 Increasing the Memory Allocated to the NMT

In large networks, especially those connected to an SQL database, the Server NMT (hosted on a PC with 4 Gigabytes or more of RAM), will benefit from being allocated more of the host PC's RAM.

To do this, follow these steps:

-
2. `%userprofile%` is a system defined path, often `C:\Users\<username>\`

1. Right click the TaitNet NMT shortcut on the desktop and select Properties.
2. In the Taitnet NMT Properties window, select the Shortcut tab.
3. The Target field should read something like:
`"C:\Program Files (x86)\Tait Applications\TaitNet NMT\TaitNet NMT.exe"`
Modify this by adding the command line argument `-Jmaxheap`, for example:
`"C:\Program Files (x86)\Tait Applications\TaitNet NMT\TaitNet NMT.exe" -Jmaxheap=536870912`

 The command line argument must be *after* the closing speech mark.

There must be a single whitespace before the command line argument, and no whitespace within it.

The value following the = is the number of bytes. Abbreviations such as k or M *cannot* be used.

Command line arguments always start with a dash -

Do not set the heap size to more than the available memory on the PC, with a maximum value of 2 Gigabytes, i.e.
`-Jmaxheap=2147483648`

9.4 Setting up for Multiple Users

In many medium-sized networks and in most large networks, the Server NMT runs continuously, collecting Call Records and monitoring Alarms.

If different operators need to access this NMT, it is appropriate to supply each operator with their own username, access level and password.

An operator starts by selecting File > Login, and logs in with their username and password. In this manner each operator has an access level appropriate to their function. When an operator finishes with the NMT, they select File > Logout. The NMT continues to run, but most User functions are disabled. Likewise, at startup, NMT Server functions start immediately; it is only User functions that are disabled until the user logs in.

Refer to the T1541 Operations Manual (Part E Configuration Menu, Chapter 2 Users), for instructions for adding Users.

Notice It is strongly recommended that all NMT users have the same Windows username (e.g. NMT user) and log on to the PC (if necessary) with this name. The individual username should be used only to log on to the NMT. This ensures all configuration files are stored in the same directory and makes maintaining the NMT software and configuration files much easier. Configuring the NMT in this manner is **essential** in

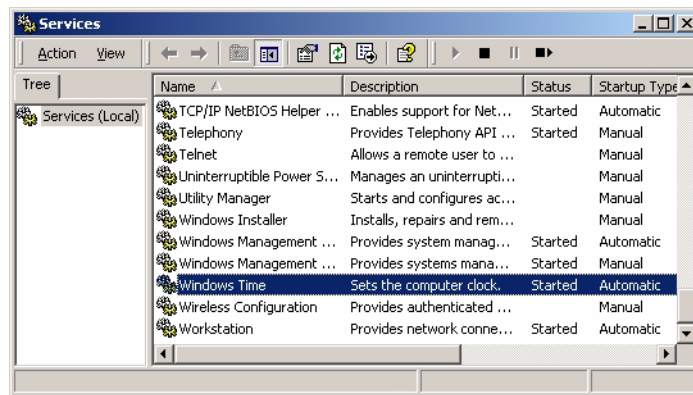
the case of the Server NMT, and is recommended in the case of Client NMTs.

9.5 Configuring NTP for NMTs running Windows 2000

For correct operation and download of call records, the NMT needs to be synchronised to the same NTP server as the nodes.

1. First, obtain a DOS prompt.
2. Stop the W32Time Service by entering:
net stop w32time
3. Now set the IP address of the NTP server. Do this by entering:
net time /setsntp:<ntpServer>
Where <ntpServer> is the IP address of the NTP server.
4. Start the W32Time Service by entering:
net start w32time

From the Windows Control Panel, open the Administrative Tools. From the available options, open Services. Scroll downwards until you find an entry named Windows Time. Check that the Startup Type is set to 'Automatic'. If it is not, you will need to double click the service and edit it.



5. Verify that the time service is synchronising time by entering:
w32tm -v -once -test

This instruction should display a similar output to the example printed below.

Windows will synchronize once every 45 minutes until it has been successful three times, then once every eight hours (three times per day).

Sample output for W32Time Service test

```
W32Time: BEGIN:InitAdjIncr
W32Time:   Adj 100144 , Incr 100144 fAdjust 0
W32Time: END:Line 2473
W32Time: BEGIN:TsUpTheThread
```

```

W32Time: END Line 1384
W32Time: TimeMInit()
W32Time: Kernel timer : using default maximum resolution
W32Time: MaximumTime = 100144
W32Time: CurrentTime = 100144
W32Time: Timer calibrated, looped 1 times
W32Time: BEGIN:InitTmCfg
W32Time: END:Line 752
W32Time: BEGIN:InitTmCli
W32Time: END:Line 2566
W32Time: BEGIN:InitTmData
W32Time: END:Line 2588
W32Time: AvoidTimeSyncOnWan 0
W32Time: ntpserver - ntpserver.main.tait.co.nz
W32Time: BEGIN:CMOSSynchSet
W32Time: Setting adjustment 100144 - Bool 0
W32Time: BEGIN:SetTSTimeRes
W32Time: END:Line 1272
W32Time: END:Line 841
W32Time: BEGIN:InitializeDC
W32Time: BEGIN:GetRole
W32Time: Role is 'workstation'
W32Time: END Line 670
W32Time: END:Line 702
W32Time: timeBeginPeriod: setting resolution 9
W32Time: BEGIN:TimeSync
W32Time: BEGIN:FGetType
W32Time: END Line 252
W32Time: BEGIN:FDoTimeNTPType
W32Time: BEGIN:ChooseNTPServer
W32Time: END Line 2150
W32Time: BEGIN:GetSocketForSynch
# should be an IP address or DNS name of the ntp server
# (see text in italics in following lines)
W32Time: NTP: ntpptrs[0] - NTPSERVER.MAIN.TAIT.CO.NZ
W32Time: rgbNTPServer NTPSERVER.MAIN.TAIT.CO.NZ
W32Time: Port Pinging to - 123
W32Time: Connecting to "NTPSERVER.MAIN.TAIT.CO.NZ"
(172.27.1.40)
W32Time: END:Line 1147
W32Time: BEGIN:GetDefaultRid
W32Time: END Line 2329
W32Time: BEGIN:ComputeDelay
W32Time: BEGIN:NTPTry -- init
W32Time: END Line 1660
W32Time: BEGIN:NTPTry -- try
W32Time: BEGIN:ComputeInterval
W32Time: END Line 2449
W32Time: Sending to server 48 bytes...
W32Time: Recv'ed from server 48 Bytes...
# there should be no mention of any failing lines here
W32Time: END Line 1860
W32Time: BEGIN:NTPTry -- delay
W32Time: END Line 1984
W32Time: Round trip was 0ms
W32Time: BEGIN:NTPTry -- gettime
W32Time: BEGIN:Fgmtimetonttime
W32Time: END Line 2533
W32Time: END Line 1970
W32Time: one-way delay is 0ms
W32Time: END Line 1622
W32Time: END Line 366
W32Time: BEGIN:TimeDiff
W32Time: ClockError --2051
W32Time: END Line 2512
W32Time: BEGIN:FCheckTimeSanity
W32Time: END Line 547

```

```

W32Time: BEGIN:SetTimeNow
# the following lines should be present
W32Time: ***Would have set system time***
W32Time: Time 5/2/2002 22:53:45:593
W32Time: END Line 1257
W32Time: Time was 53min 43.542s
W32Time: Time is 53min 45.593s
# difference in time left
W32Time: Error -2051ms
W32Time: BEGIN:CheckLeapFlag
W32Time: END:Line 583
W32Time: BEGIN:ComputePostTimeData
W32Time: BEGIN:ComputeInterval
W32Time: END Line 2449
W32Time: BEGIN:ComputeSleepStuff
W32Time: Computed stagger is 0ms, bias is 0ms
W32Time: Time until next sync - 2699.960s
W32Time: END:Line 793
W32Time: END:Line 219
W32Time: END:Line 194
W32Time: BEGIN:TermTime
W32Time: TimeMMCCleanup()
W32Time: BEGIN:FinishCleanup
W32Time: BEGIN:TsUpTheThread
W32Time: END Line 1384
W32Time: Time service stopped.
W32Time: END:Line 383

```

9.6 Porting an Existing NMT to a New PC

This is a fast way of re-installing the Fleet and other databases when a new NMT is commissioned (for example, when the PC on which the NMT is run is upgraded), but the steps outlined below must be closely followed to do this successfully.


Notice The steps below assume that the new PC has the same IP address as the PC it is replacing. If this is not the case, you **must** contact Tait support before commencing the PC upgrade.

9.6.1 For the Server NMT:


1. On the old NMT, select File > System Backup. In the file chooser window's File Name field, supply a name for the backup file (the suffix must be .tbf) and press the Backup button.
2. Locate the backup file you just created (in %userprofile%\My Documents\Tait Applications\TaitNet NMT\backups) and copy it to a secure location.
3. Locate the config files CR.cfg, ETC.cfg and NMT.cfg⁴ in %userprofile%\My Documents\Tait

 3. %userprofile% is a system defined path, often C:\Documents and Settings\ - 4. Any other customer specific config files (these always have the suffix .cfg), must also be copied and saved.

Applications\TaitNet NMT\config and copy to a secure location.


 Whether you want to save VIEW.cfg is up to you. VIEW.cfg lists the current location and size of all NMT windows. If you are moving to a different screen configuration in the new PC it may be better not to save VIEW.cfg and allow all NMT windows to return to their default values.

4. Locate the file C:\Program Files\Tait Applications\TaitNet NMT\license.dat and cut and paste to a secure location.
5. Install the NMT on the new PC, as described above in [Section 9.1](#).
6. Cut and paste the file license.dat to C:\Program Files\Tait Applications\TaitNet NMT\ on the new PC.
7. Launch the NMT application. When the login screen appears, press the Cancel button and then close the NMT application. (This step creates the required directory structure in %userprofile%\My Documents.)
8. Copy the saved config files CR.cfg, ETC.cfg, NMT.cfg⁵ (and VIEW.cfg if required) to %userprofile%\My Documents\Tait Applications\TaitNet NMT\config\.
9. Copy the saved backup file to %userprofile%\My Documents\Tait Applications\TaitNet NMT\backups\.
10. Launch the NMT application again. Login with the default username **admin** and password **tait**.
11. Select File > System Restore. In the file chooser window, select the backup file and press the Restore button.

 This last step restores the User database, so that, if the admin password has been changed from 'tait' previously, next time a user logs in they will need to use the correct password.

9.6.2 For a Client NMT:

1. Locate the config files CR.cfg, ETC.cfg and NMT.cfg⁴ in %userprofile%\My Documents\Tait Applications\TaitNet NMT\config and copy to a secure location.

 Whether you want to save VIEW.cfg is up to you. VIEW.cfg lists the current location and size of all NMT windows. If you are moving to a

-
5. Any other customer specific config files (these always have the suffix .cfg), must also be copied and saved.

different screen configuration in the new PC it may be better not to save VIEW.cfg and allow all NMT windows to return to their default values.

2. Locate the file C:\Program Files\Tait Applications\TaitNet NMT\license.dat and cut and paste to a secure location.
3. Install the NMT on the new PC, as described above in [Section 9.1](#).
4. Cut and paste the file license.dat to C:\Program Files\Tait Applications\TaitNet NMT\ on the new PC.
5. Launch the NMT application. When the login screen appears, press the Cancel button and then close the NMT application. (This step creates the required directory structure in %userprofile%\My Documents.)
6. Copy the saved config files CR.cfg, ETC.cfg, NMT.cfg⁶ (and VIEW.cfg if required) to %userprofile%\My Documents\Tait Applications\TaitNet NMT\config\.
7. Launch the NMT application again. Login with your usual username and password.

9.7 Installing a Client NMT Without a License File

Q1541NMT version 4.10.06 or later can be used as a Client NMT without requiring a license. But a “pre-made” NMT.cfg file is required when no NMT license is available.

To create a “pre-made” NMT.cfg file, follow these instructions. They ensure that the fleet configuration is the same in both Client and Server. Consistency of fleet information between Client and Server is essential for correct operation of the network.

1. Run the install CD as described in [Section 9.1 Installation Procedure](#).
2. Launch the Client NMT application (This step creates the correct file structure within %userprofile%\My Documents).
3. When the dialog box saying that you need a license appears, click OK. The NMT shuts down.
4. Copy the %userprofile%\My Documents\Tait Applications\TaitNet NMT\config\NMT.cfg file from the Server NMT to the new Client. It must be installed in the same location: %userprofile%\My Documents\Tait Applications\TaitNet NMT\config

6. Any other customer specific config files (these always have the suffix .cfg), must also be copied and saved.

5. Edit the `NMT.cfg` file in the Client (the file you just copied). Change `Database.Server=true` to `Database.Server=false`
6. Check, and if necessary edit, this file so that the line `Database.Host=` is set to the IP address of the NMT Server.
7. Re-launch the Client NMT application.

9.8 NMT Configuration Files

NMT Configuration files are stored in `%userprofile%\My Documents\Tait Applications\TaitNet NMT\config\7`.

The format of these files is `key=value`, with one parameter per line. There must be no whitespace in the key, or around the '='. Whitespace is permitted in the value. Key names are case sensitive. Lines beginning with `#` are ignored by the NMT software.

All NMT installations have four standard configuration files, and customer specific configuration files may also be present. All configuration files have the filename in uppercase and the suffix `.cfg`. Standard configuration files are:

- `CR.cfg`
Stores all call record configuration settings. This includes internal information required to ensure that, after an NMT shutdown, when the NMT is restarted, it remembers the most recent sequence number of the last call record it received from each node. If this file is deleted, not only are all user modifications generated by changes made using the Configuration > Call Records window lost, but there are also may be issues with getting call record downloading from the nodes re-established.
- `ETC.cfg`
Stores all alarm settings and backup file locations that have been modified by the user. If this file is deleted, all alarms revert to their default priorities, and all user modifications generated by changes made using the Configuration > Alarms window are lost.
- `NMT.cfg`
Stores general configuration information not specifically stored in other configuration files, including information on the numbering scheme used by the network. If this file is deleted, and there is a Client NMT available, it is possible to copy the `NMT.cfg` file from the Client over to the Server NMT, change the line `Database.Server=false` to `Database.Server=true`, delete the line that starts with `Database.Host=` and restart the Server NMT. This should get you underway again.
- `VIEW.cfg`
Stores the location and the size (if the window is resizable) of all NMT windows. When a window is closed, the values stored in this file ensure

7. `%userprofile%` is a system defined path, often `C:\Users\<username>`

that when opened again, it displays in the same location on the screen. If this file is deleted, all windows revert to their default size and location. If your super-large-display monitor dies, and the replacement monitor is much smaller, you may need to delete this file in order to find your NMT's windows again.

9.8.1 Additional NMT.cfg Parameters

Most configuration parameters are written by the NMT application software when the user clicks Apply after modifying a window in the NMT's Configuration menu. There are a few configuration parameters that, if required, must be manually added to NMT.cfg. Indiscriminate use of these parameters is strongly discouraged. Most are reserved for special case situations and should not be used without recommendation from a senior support engineer at Tait support. An exception is Statistics.DaysToStore which should be set the same value as the parameter DaysToKeepDatabases in tait_mptnc.cfg (refer [Section 5.2.4 Configuration Parameters](#)).

Type definitions:

- Boolean: true or false, always in lowercase.
- Number: decimal digits representing a positive integer.
- String : alphanumeric characters, including symbols where appropriate. May include whitespace.
- 24-bit color: 6 hexadecimal digits representing a 24-bit color value.

Parameter name	Type	Default value	Comment
AutoBackups.Prefix	String	AutoBackup-	Autobackup filenames all start with this string
ControlChannel.Rx LoadFactor	Number	35	Refer to T1541 Operations Manual Part H: Ch 4.3 Viewing Site Statistics as Graphs
ControlChannel.Tx LoadFactor	Number	35	
Color.Separator	24-bit color	EEEEEE	The background color used in alternating lines in tables
Database.AlarmSize	Number	2000	The maximum number of alarms stored in the alarms.db2 database. If this is exceeded, the oldest alarms are deleted.
Default.Font	String	win.menu.font	The font used by the NMT User Interface
Default.FontSize	Number	11	
Default.Formatting	Boolean	false	If true, all new lines in the log file output are replaced with whitespace and then the text is cut into lines always 100 characters in length
Default.LogKeepDays	Number	90	Number of days to keep audit and log files before deletion

Parameter name	Type	Default value	Comment
Default.LogToConsole	Boolean	false	If true, logs are written to both logfile and a console display (stdout)
Default.ShowGrid Lines	Number	2	1: Display grid lines in tables 2: Hide grid lines in tables
MainWindow.MemoryUsageBar	Boolean	false	Refer T1541 Operations Manual Part A: Ch 3.4 Status Bar
Menubar.ClientServer Connection	Boolean	false	Used in testing NMT client only. Add items to File menu to connect and disconnect from NMT server.
Menubar.Edit Translations	Boolean	false	Refer to T1541 Operations Manual Part E: Ch 7 Advanced Options
Menubar.ImportTools	Boolean	false	
Menubar.TimeZone	Boolean	false	
NetworkView.Simulate	Boolean	false	Used for testing or demonstrating the Network View feature. If true, generates a random dummy load to exercise the Network View display.
NoSoundCard	Boolean	false	If true, disable all alarm sounds. Refer "Running the NMT on a Computer Without a Sound Card" on page 68.
SQL.MaxSyncTimeSec	Number	120	Generate an alarm if the SQL connection has not synchronized within this time period (seconds) after NMT startup or a reconnection after a network issue. May need to increase this if bandwidth between the NMT and SQL Server is severely constrained.
SQL.monitor	Boolean	false	If true, adds Reports > SQL Monitor, a window that displays all transactions on the interface between the NMT and SQL Server
Statistics.DaysToStore	Number	30	The number of days that Site and DAS statistics are stored. Should be set to the same value as the <code>tait_mptnc.cfg</code> parameter <code>DaysToKeepDatabases</code> (refer "Configuration Parameters" on page 42.)
SwitchoverTestBox.Display	Boolean	false	If true, displays a button on <code>node > Configuration</code> window to enable a testing regime for HA switchover
SwitchoverTestBox.MinTestInterval	Number	20	Allows the tester to vary the time (seconds) between HA switchover tests. Actual time between tests will be randomly selected between this value and 3 x this value.


Parameter name	Type	Default value	Comment
sx.aps.port	String	08	Parameters used to set up and manage call diversions between TaitNet and SX networks. Refer to SX documentation for more information.
sx.delay	Number	60	
sx.LogToFile	Boolean	false	
sx.monitor	Boolean	false	
sx.password	String	VALIDS	
sx.port	String	COM1	
sx.use	Boolean	false	

10 NMT Upgrade Procedure

From time to time you will need to upgrade the NMT software. This will provide you with the benefits of new features and bug fixes.

This section describes how to upgrade your NMT from version 3 or above, to a later version. If you have an earlier version NMT, first upgrade to version 3.

The purpose of the upgrade procedure is to leave the original installation intact. This allows you to fall-back to using the old software should you encounter problems with the new version.


 In the following procedure, it is assumed that your current NMT installation is in the default location.

1. First, you should make a backup of your current installation. Make a copy of the following directory and all of its contents:

```
C:\Program Files\Tait Applications\TaitNet NMT
```

The copy should be called:

```
C:\Program Files\Tait Applications\TaitNet NMT vX.X.X
```

 X.X.X will be used throughout this document to refer to the version number of the current installation. Wherever you use this, you should replace it with the actual version number of your existing software.

2. If you have a shortcut to the NMT on your desktop, you should edit its properties. Right-click the icon and select Properties. Edit the Target field and change it to the following:

```
"C:\Program Files\Tait Applications\TaitNet NMT vX.X.X\  
TaitNet NMT.exe
```

Edit the Start in field and change it to the following:

```
"C:\Program Files\Tait Applications\TaitNet NMT vX.X.X"
```

Change the name of the shortcut to:

```
TaitNet NMT vX.X.X
```

3. From the Windows Control Panel, select Add/Remove Programs and uninstall the NMT.

4. Install the new NMT software, see [“Node Controller Parameter Definitions”](#) on page 42 for details.

5. Copy the license file from the old installation. Copy the file:

```
C:\Program Files\Tait Applications\TaitNet NMT  
vX.X.X\license.dat
```

to location:

```
C:\Program Files\Tait Applications\TaitNet NMT
```

6. *If upgrading from a software version 4.05.01 or earlier to a software version 4.06.00 or later:* Double click the TaitNet NMT icon to launch the


(new) NMT. A default (empty) NMT will start up. When the login screen displays, close down this NMT. (This action automatically creates the new directories required.)

Copy the configuration files from the old installation to the new one. Copy the contents of the directory:

```
C:\Program Files\Tait Applications\TaitNet NMT vX.X.X\config  
to location:
```

```
%userprofile%\My Documents\Tait Applications\TaitNet  
NMT\config
```

(Do not copy the file `properties.xml`. This file must never be copied between versions of software.)

 If you are not using default (application-supplied) names for the directories under `C:\Program Files\Tait Applications\TaitNet NMT` you must manually change the directory names under `%userprofile%\My Documents\Tait Applications\TaitNet NMT`. For example, if you save call records into directory `Call Records` instead of `callrecs`, you must change `%userprofile%\My Documents\Tait Applications\TaitNet NMT\callrecs` to `%userprofile%\My Documents\Tait Applications\TaitNet NMT\Call Records`.


7. *If upgrading from a software version 4.05.01 or earlier to a software version 4.05.01 or earlier:* Copy the configuration files from the old installation to the new one. Copy the contents of the directory:

```
C:\Program Files\Tait Applications\TaitNet NMT vX.X.X\config
```


to location:

```
C:\Program Files\Tait Applications\TaitNet NMT\config
```


(Do not copy the file `properties.xml`. This file must never be copied between versions of software.)

 If upgrading from software version 4.06.00 or later, no configuration files need to be copied. Your existing files in `%userprofile%\My Documents\Tait Applications\TaitNet NMT` will apply.


8. **If using Windows Vista OS:** Both `TaitNet NMT.exe` and `java.exe` need to operate with Administrator privilege. Go to directory `C:\Program Files\Tait Applications\TaitNet NMT`. Right click `TaitNet NMT.exe` and select Properties. Tick the check box `Allow To Run As Administrator`, then click Apply and close the window. Then go to directory `C:\Program Files\Tait Applications\TaitNet NMT\jre\bin`. Right click `java.exe` and select Properties. Tick the check box `Allow To Run As Administrator`, then click Apply and close the window.
9. You should now have two NMT icons on your desktop. To run the new NMT, launch `TaitNet NMT`. Should you need to run the old NMT, launch `TaitNet NMT vX.X.X`.

1. `%userprofile%` is a system-defined path, often `C:\Documents and Settings\<username>`.

10. If you were using the MySQL feature and intend to continue using it, you must, before starting the new NMT software for the first time, log on to the MySQL database as the user TaitNet. Select Tools > MySQL Command Line Client and enter this command at the prompt:

```
use t1541;
```

If you find you are unable to use the MySQL feature after any upgrade, please consult Technical Note TN-1267 “MySQL Setup” for further advice.

-  Version 3 software configuration databases use the extension .db. Version 4 software configuration databases use the extension .db2. When you upgrade from version 3 software, .db database files are automatically converted to .db2 database files; there is no need to manually alter the filename extension.

Notice After upgrading to NMT version 4.06.00 or later, when the NMT is restarted new log files, backup files, call record files, etc. will be created in the appropriate directory under %userprofile%\My Documents\Tait Applications\TaitNet NMT\. However, files that were created by the previous version of NMT software will remain in the directory where they were created (i.e. under C:\Program Files\Tait Applications\TaitNet NMT\). These old files will remain until manually moved or deleted by the user. This is especially important to remember should you need to restore files from a time earlier than when the upgrade was done. In this case, use the File Chooser window to navigate to the appropriate directory.

11 High Availability Options

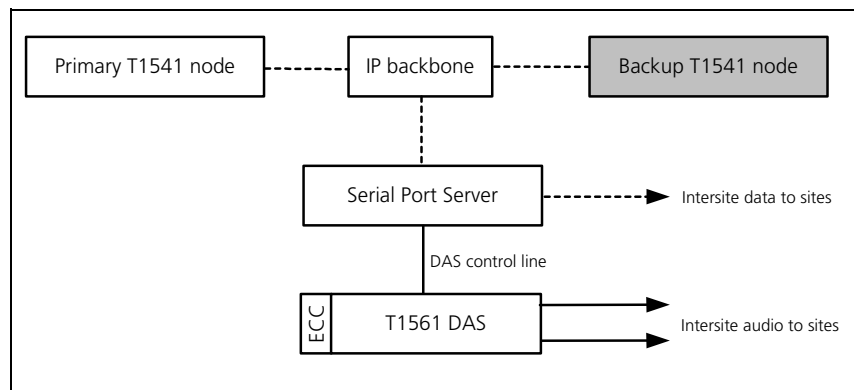
- i** The description and screen shots used in this section use Node Controller software and NMT software version 4.08.00. If your NMT software version is earlier than this, most of the steps listed here still apply, but the NMT screens are not the same as in the screen shots here. In particular, the NMT's Node Configuration parameter "High Availability type" is not present and cannot be set.

In the instructions below, the serial port server used is assumed to be an EL32, so that wherever this abbreviation is used, it refers to the serial port server that is installed.

11.1 Option 1: Standby Node Only

11.1.1 Operation

This configuration provides the most basic and cost effective arrangement to secure the trunked radio system. It provides a backup node controller that will take over the functions of the primary node controller should the primary fail.



In the event of the failure of the serial port server (EL32), all intersite and internode calls will be terminated. Local site call setup is not affected.

In the event of the failure of the Embedded Controller Card (ECC), all intersite and internode speech/non-prescribed data calls will be terminated.

Although the failure of either the serial port server or the ECC results in significant system disruption, the probability of failure for these two modules is relatively low in comparison to the node controller.

11.1.2 Setup

Each node has the same node number

Each node has a unique IP address set during the O/S installation

Both nodes have an active IP address set in the `tait_mptnc.cfg` file. One node should be marked as the primary node and the other as the backup node. Use the node configuration script to set these.

```
Enter the node number (0-31) [0]: 1
Is this a standalone node (y/n) [n] ? n
Enter the active node IP []: 172.27.1.48
Enter the active node netmask or none []: 255.255.255.0
Enter the active node gateway or none []: 172.27.1.255
Is this the primary node (y/n) [y] ? y
Enter the Backup Node IP []: 172.27.1.50
```

The network check IP addresses should be set to the addresses of switches, EL32s or other normally contactable IP addresses. The network check IP addresses are used by the node to confirm if the network is broken. If one or both of these addresses are set, the node software will change to a failed state if these addresses are not contactable.

```
Enter the network check A: IP address or none [none]:
172.27.1.254
Enter the network check B: IP address or none [none]:
172.27.1.13
```

The network interface to use should normally be `eth0`. If the software is installed on older machines the network interface may be different. This parameter is used by the `ipcfg` program to set the active node IP address.

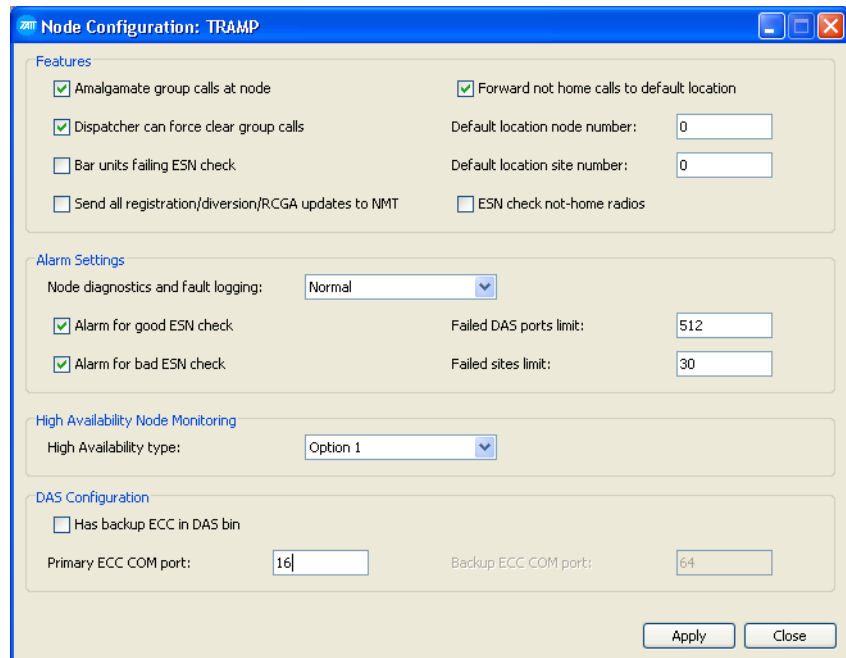
Enter the network interface to use: [eth0]: **eth0**

On the NMT, add a new node. Set the Primary and Backup Node IP addresses. The Server NMT does not use the active node IP address.

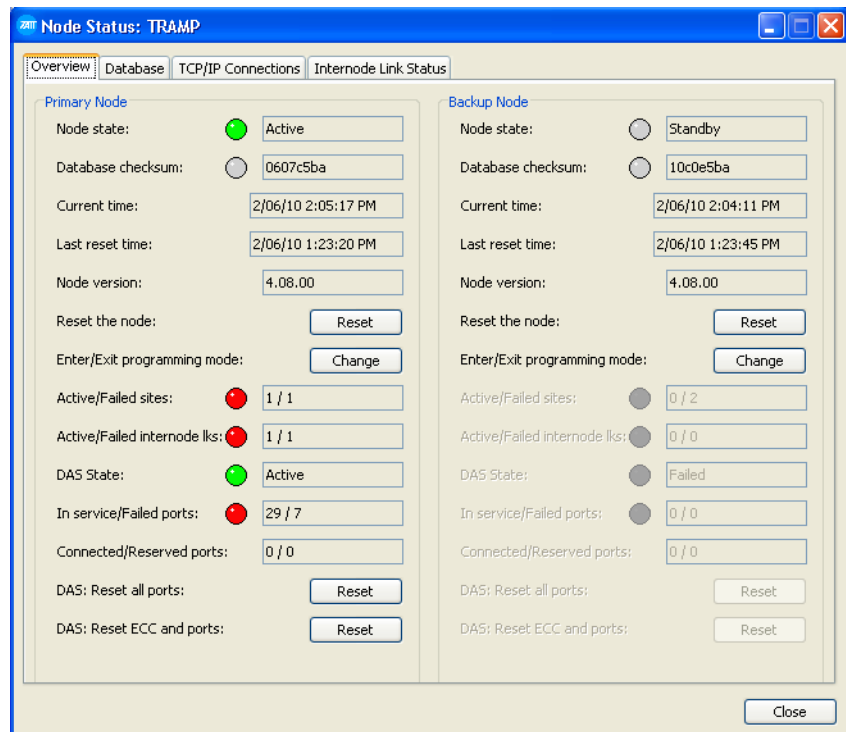
	Full Name	Mnemonic	Active
0	Site-0	TR0	<input checked="" type="checkbox"/>
1	Site-1	TR1	<input checked="" type="checkbox"/>
2			<input type="checkbox"/>
3			<input type="checkbox"/>
4			<input type="checkbox"/>
5			<input type="checkbox"/>
6			<input type="checkbox"/>
7			<input type="checkbox"/>
8			<input type="checkbox"/>
9			<input type="checkbox"/>
10			<input type="checkbox"/>
11			<input type="checkbox"/>
12			<input type="checkbox"/>

In the Node Configuration window set the High Availability type to Option 1.

Check that the “Has backup ECC” parameter is not ticked. Set the Primary ECC COM port to the number of the serial port on the EL32 that the primary ECC is connected to.



You can check the node status from the NMT by looking at the Node Status window.



Make sure the database checksums are the same. If they are not, then do a batch validation and a node backup and restore. The restore resends all configuration data to both nodes.

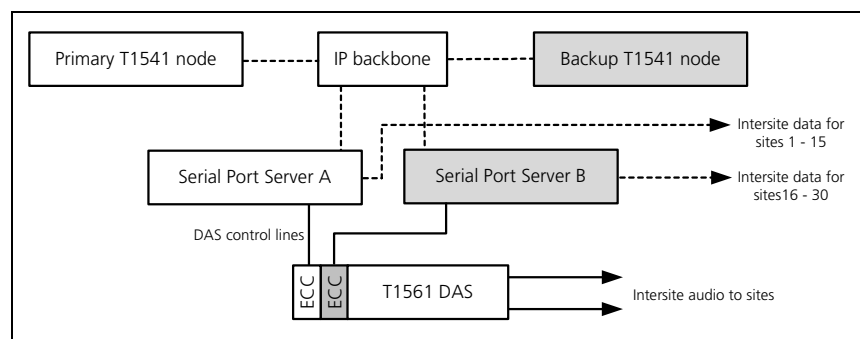
11.2 Option 2: Standby Node/DAS with Split Serial Ports

11.2.1 Operation

This configuration provides redundancy for all critical node components including:

1. T1541 Node Controller
2. T1541 Etherlite Serial Port Server
3. T1561 Embedded Controller Card

The backup node controller will take over the functions of the primary node controller should the primary fail. In the event of a switchover all intersite and internode calls will be terminated.



In the event of the failure of a serial port server, the sites attached to the failed server will be isolated from the node. Intersite calls to and from these sites will not be possible. The sites connected to the other serial port server remain in normal operation. To resume normal operation of the isolated sites, the intersite data lines may be shifted from the failed serial port server to the operational one.

11.2.2 Setup

The initial setup is the same as in [“Option 1: Standby Node Only”](#).

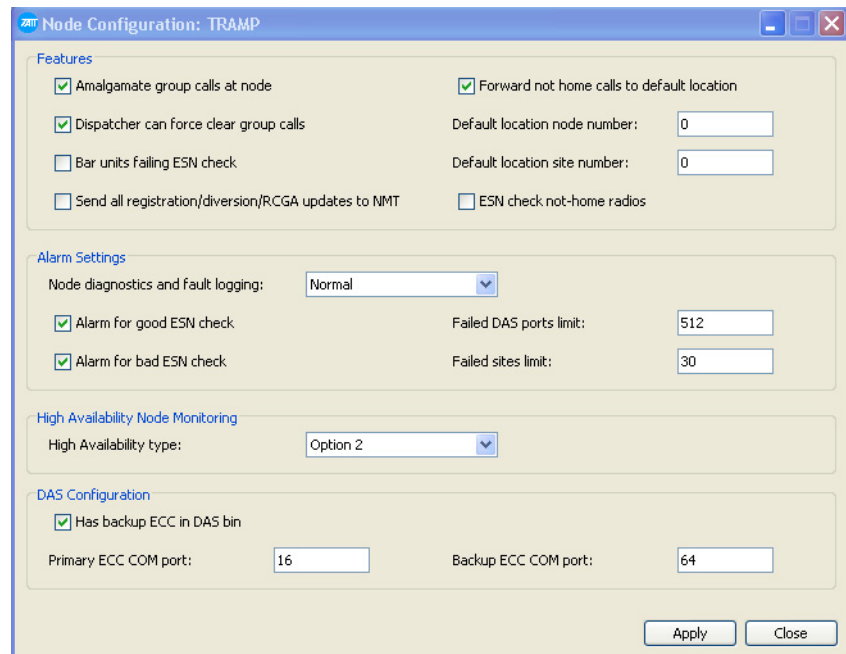
Connect the primary ECC to one EL32, the backup ECC to the other EL32. Make sure the ECC DIP switch for “dual ECC” operation is enabled - on both ECCs.

S304 (DIP 1)	S305 (DIP 2)
1 On: ConferenceTimerDisable	1 Off: Card Test Disabled
2 Off: DSP 0 Enabled	2 Off: not used
3 Off: DSP 1 Enabled	3 Off: Reset Timer Enabled
4 Off: DSP 2 Enabled	4 Off: Console Timer Enabled
5 Off: DSP 3 Enabled	5 On: Dual ECC
6 On: \\\	6 Off: not used
7 Off: SerOpt1: 512PrtNoDASC	7 Off: PCM Sync Free Running
8 Off: ///	8 On: Companding u-Law

When installing the real port drivers for the EL32s make sure that the primary EL32 is given a tty device ID of “cu” and the backup a tty device ID of “cv”.

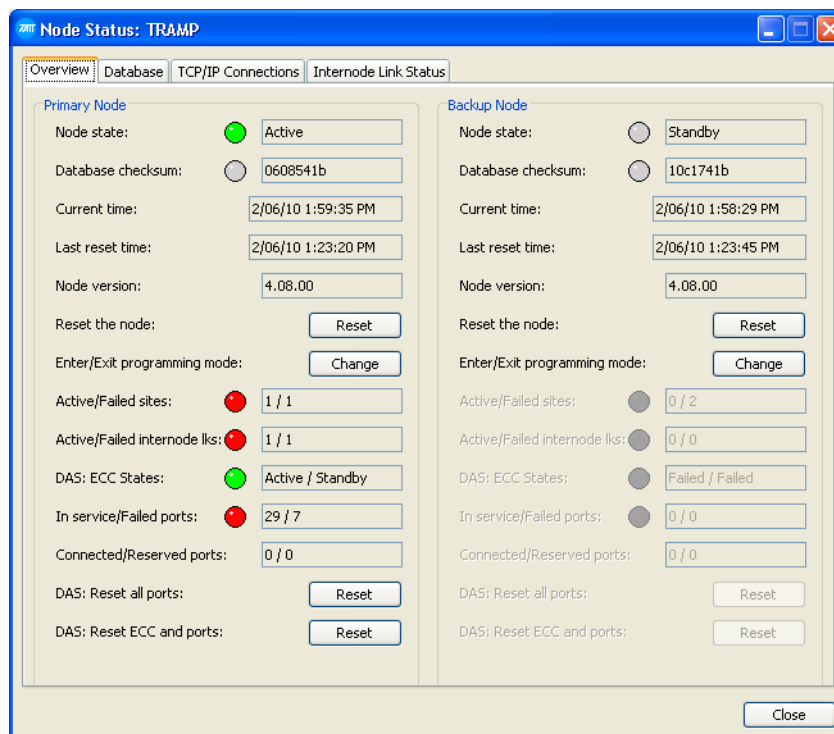
In the Node Configuration window set the High Availability type to Option 2.

Tick the “Has backup ECC” parameter. Set the Primary ECC COM port to the number of the serial port on the EL32 that the primary ECC is connected to. Repeat this for the backup ECC. The ECCs should normally be on different EL32s – but they don't have to be.



The “Failed DAS ports limit” and “Failed sites limit” parameters are not used in either this or in the Option 3 configuration.

You can check the node status from the NMT by looking at the Node Status window.



11.3 Option 3: Standby Node/DAS and Site Management Modules

11.3.1 Operation

This configuration provides redundancy for all critical node and site components including:

1. T1541 Node Controller
2. T1541 Etherlite Serial Port Server
3. T1561 Embedded Controller Card
4. T1722 Site Management Module

The configuration requires two intersite data lines to be provisioned for each site. For each site, the primary data line provides communications from the node to the primary SMM, and the backup data line provides communications from the node to the backup SMM.

In the event of the failure of a serial port server the following occurs:

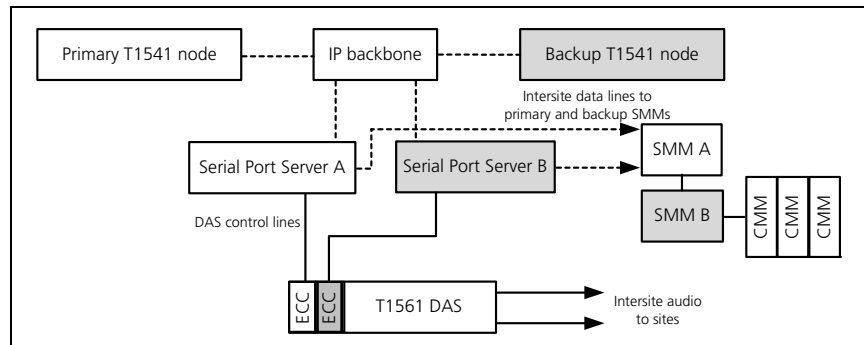
The SMMs connected to the serial port server will enter the failed mode. At these sites, if the peer SMM has a valid communication link to the node and it is not already active, it will become active.

If the active ECC is connected to this serial port server, the node

controller will order the other ECC to become active and assume the functions of the now failed card.

In the event of the failure of the active ECC, the backup will assume the functions of the primary. In the event of a switchover, all intersite and internode audio and non-prescribed-data calls will be terminated.

In the event of the failure of the active SMM, the standby will assume the functions of the failed module. In the event of a switchover, all intersite and local calls will be terminated. Some calls in the process of call setup may hang until the internal radio call timers expire.

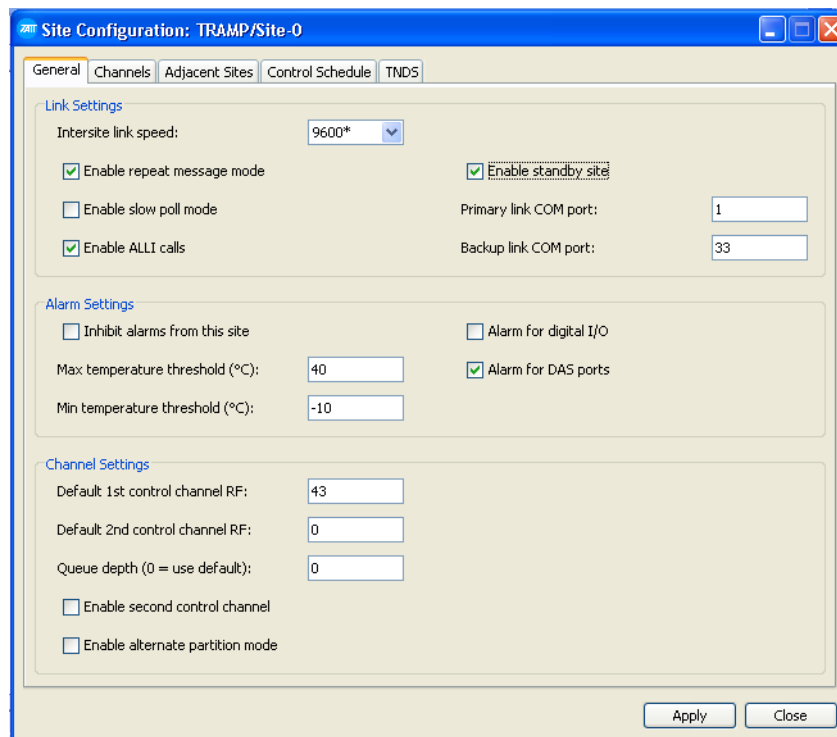


11.3.2 Setup

The initial setup is the same as in [“Option 2: Standby Node/DAS with Split Serial Ports”](#).

In the Node Configuration window set the High Availability type to Option 3.

Connect the primary SMM to the primary EL32 and the backup SMM to the backup EL32. In the Site Configuration window set the Primary link COM port to the number of the serial port on the EL32 that the primary SMM is connected to. Repeat this for the backup SMM. The SMMs should normally be on different EL32s - but they don't have to be.



In the SMM configuration make sure “Standby Mode” is enabled:

```

Menu : System Parameters
Exit to Main Menu
Determine Call Answer by line Reversals. . . . . : Yes
Pass Line Reversals and Meter Pulses . . . . . : No
Add Call Answer Time to Time Queued. . . . . : No
FOACSU for Incoming Phone Calls. . . . . : Enabled
Foacsu for Radio to Radio Calls. . . . . : Disabled
Modified OACSU for Incoming Phone Calls. . . . . : Disabled
No. of Signalling Retries. . . . . : 1
No. of GTC Msgs to Send. . . . . : 2
No. of ACK Msgs to Send. . . . . : 2
No. of CLEAR Msgs to Send. . . . . : 2
Extra Wait Slots . . . . . : 0
CWID String. . . . . :
CWID Interval. . . . . : 0 Minutes (0=Disable)
Traffic Channel Rotation . . . . . : Enabled
Standby Mode . . . . . : Enabled
>FFSK Muting. . . . . : Enabled
Minor Alarm Disable. . . . . : Recover

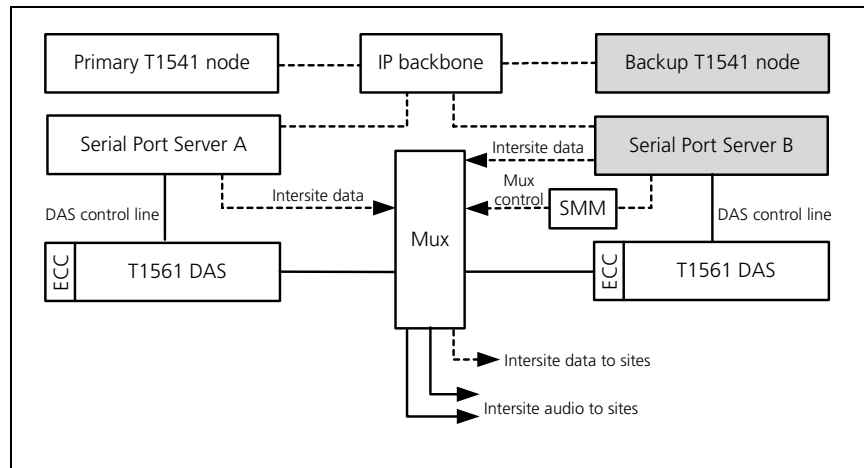
```

11.4 Option 4: Geographically Diverse Nodes

11.4.1 Operation

This configuration supports a system where a complete set of standby equipment may be installed in a separate location, far enough from the primary equipment so that external causes (power outage, lighting damage, fire, etc.) that have disabled the primary equipment have less chance to affect the backup as well. There are several different levels of redundancy available

within Option 4, but the key difference between this option and other options is that the entire DAS is duplicated, not just the DAS Embedded Control Card (ECC).



When the standby equipment is in operation, all the lines must be redirected from the primary to the standby location. These lines include:

1. Intersite data lines
2. Intersite audio lines
3. PABX/PSTN lines
4. Line dispatcher lines
5. Internode audio lines

The backup node controller will take over the functions of the primary node controller should the primary fail. If the backup node controller becomes active, it asserts the RTS signal on an RS-232 port to indicate this state. This signal may be connected to a PCM multiplexer/cross-connect to automatically switch the lines from the primary site to the backup site.

Care must be taken to ensure that a single multiplexer does not become a critical component whose failure would disable both the primary and the standby nodes. Using parallel units and spare routes in the transmission network provides the needed reliability.

This configuration supports the use of backup SMMs, intersite data lines and backup DAS ECCs.

One or two EL32s may be fitted at each node. Likewise, the DAS at each node may have one or two ECC cards installed. Option 4 can be used with or without backup Site Management Modules at each site.

11.4.2 Setup

If each node has one EL32 and one ECC card in each DAS, the initial setup is the same as Option 1. If each node has two EL32 and two ECC cards in each DAS, the initial setup is the same as Option 2. If backup SMMs are used at each site, the initial setup is similar to Option 3.

Use the config script to edit the `tait_mptnc.cfg` file. Set the `MonitorComPort` parameter to the EL32 serial port number the MUX switching equipment is connected to.

```
MonitorComPort: 31
```

In the Node Configuration window set the High Availability type to Option 4.

The screenshot shows the 'Node Configuration: TRAMP' window with the following settings:

- Features:**
 - Amalgamate group calls at node
 - Dispatcher can force clear group calls
 - Bar units failing ESN check
 - Send all registration/diversion/RCGA updates to NMT
 - Forward not home calls to default location
 - Default location node number: 0
 - Default location site number: 0
 - ESN check not-home radios
- Alarm Settings:**
 - Node diagnostics and fault logging: Normal
 - Alarm for good ESN check
 - Alarm for bad ESN check
 - Failed DAS ports limit: 14
 - Failed sites limit: 2
- High Availability Node Monitoring:**
 - High Availability type: Option 4
- DAS Configuration:**
 - Has backup ECC in DAS bin
 - Primary ECC COM port: 16
 - Backup ECC COM port: 64

If there is a single ECC card in each DAS, ensure the “Has backup ECC” parameter is not ticked. The ECCs at each DAS must use the same COM port. The port number is entered in the “Primary ECC COM port” field. Make sure the ECC DIP switch for “dual ECC” operation is not enabled – on both ECCs.

If there are two ECC cards in each DAS, the “Has backup ECC” parameter is ticked, and port numbers are entered in both “Primary ECC COM port” and “Backup ECC COM port” fields. Make sure the ECC DIP switch for “dual ECC” operation is enabled – on all four ECCs.

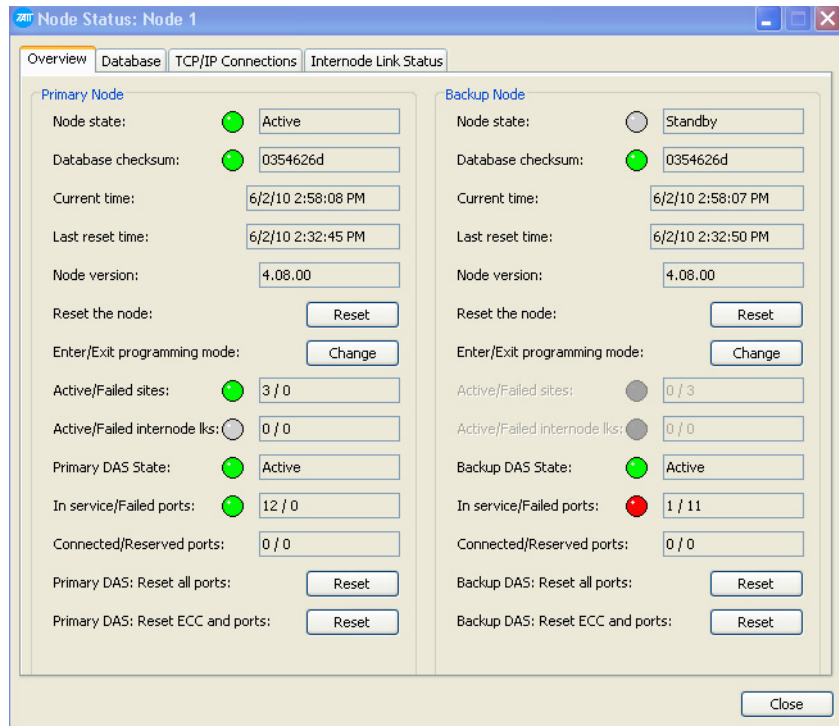
The “Failed DAS ports limit” and “Failed sites limit” parameters are used by the nodes to tell if a partial equipment failure has occurred. These might need to be set.

If the number of failed DAS ports on this node exceeds the figure entered in this box, the node will consider itself to be in the 'failed' state (and the other node will take over).

If the number of failed sites on this node exceeds the figure entered in this box, the node will consider itself to be in the 'failed' state.

The screen shot below shows the NMT's Node Configuration window set up for a single ECC card in the DAS at each node.

Once the node is in a failed state due to these parameters, it will not take over again until it is reset. Use the reset button on the Node Status window.



Be aware that the DAS connected to the Standby Node Controller is in an active but idle state. It is not performing any call functions, but it is actively monitoring its DAS ports. Therefore, in the active idle DAS, ports that have fully separate links should be reported as 'In-service', while those that share links with the DAS connected to the Active node should be reported as 'Failed'. In the active idle DAS there should be no Connected or Reserved ports so this field should display '0/0'.

12 Adding or Replacing a High Availability Node Controller


The information in this section is accurate for Q1541NC and Q1541NMT software versions 5.00 and later. It may also be (but is not tested to be) accurate for earlier versions.

12.1 Introduction

If a Node has failed and a new node controller is being prepared for use, the data in the new node controller must be set up to match the node controller it is replacing.

This is also important if a system is either being upgraded to a high availability configuration (where previously the system had operated in stand-alone mode), or the node controllers in an existing high availability system do not contain matching data.

In these situations, it is important that the data on both node controllers is identical, so that the database checksums for each node controller match.

-  In a Dual DAS High Availability (Option 4) node, if the data in the DAS a and DAS b configuration fields is not the same (refer to “Dual DAS” on page 228 of the T1541 Operations Manual), the two nodes will have different information and the node database checksums will never match. This means it is not possible to check for successful node alignment by comparing node database checksums.

12.2 Preparing the System

The procedures for preparing the system to upgrade or replace a node controller are the same for any of the following scenarios:

- a stand-alone node has failed and a replacement node controller is required
- a stand-alone node is being upgraded to a high availability node
- a high availability node where the primary node controller is Active, and the backup node controller (which has been removed) has failed. The procedures can be reversed if it is the primary node controller that has failed.

To prepare for the replacement or upgrade the following steps must be taken:

1. A new server must be prepared with the correct operating system, the correct IP address, subnet mask, and routing.

2. The matching version Node software and correct license must be installed from the Tait Node install media. The configuration of the L32 or TS2 serial devices must be correct. The `taic_mptnc.cfg` file must be configured as part of the installation, and checked against the Primary Node (for high availability systems this should be similar but slightly different in the areas of the netcheck IP and primary/secondary configuration).
3. The primary node is set to active (existing hardware) and the backup node is in standby (new hardware).

At this stage, when the Database tab of the Node Status window is viewed from the NMT, the database checksums of the primary and backup nodes will not match and will need to be aligned.

12.3 Standard Alignment Method

Before beginning this procedure, please ensure you have read all of [Section 12](#) and that you comprehend all of the steps. Refer to the T1541 Operations Manual for more information on NMT operations.

There are several node restarts which will cause brief system outages, and the node log files will be deleted.

1. On the NMT, select *Node* > Status to display the Node Status window. Check that the primary node is in Active mode on the Overview tab, then select the Database tab.
2. From the Backup/Restore Configuration Area of the Database tab, select the Backup button for Backup Configuration Database. Follow the steps to create the backup. This will save the data from the active primary node databases.
3. From the Backup Node area of the Database tab, clear all the backup node's databases (call record, registration, diversion, and validation) from the NMT.
4. From the Backup/Restore Configuration Area of the Database tab, select the Restore button for Restore Configuration Database. Follow the steps to restore the configuration databases. This will restore the backup data created in step 2 to both the primary and backup nodes.
5. Select Fleets > Batch Validate and perform a batch validation for all the fleets. This data will be sent to both the primary and backup nodes.
6. Telnet to the backup node (which should be in Standby mode), and perform a "taicnet restart".
7. Once the backup node has restarted and re-entered Standby mode, check the database checksums of the nodes (on the Overview tab of

the Node status window). If the checksums match, the process is complete. If they do not match, complete the steps in [Section 12.4](#).

12.4 Full Alignment Method

Before following this procedure you must first have completed [Section 12.3 Standard Alignment Method](#).

12.4.1 Determine Cause of Mismatched Checksums


If the database checksums do not match, it is useful to determine which of the databases on the nodes are not matching.

With Q1541NC version 4.10.03 and later, the command `./tait_mptnc -C` (refer [Section 8.4 Advanced taitnet.mptc commands](#)) will list the databases and their checksums. This command should be executed on both nodes, and the results compared.

12.4.2 Perform Full Alignment

1. On the NMT, select *Node > Status* to display the Node Status window. In the Primary Node area of the Overview tab, select the Enter/Exit Programming Mode Change button to change the node status to Program. The backup node will take over and promote itself to Active mode.
2. Ensure that the backup node is operating correctly. Specifically, check that the validation data is correct, and that the subscribers are able to register and make calls on the system.
3. From the Primary Node area of the Database tab, clear all the primary node's databases (call record, registration, diversion, and validation) from the NMT while the primary node is still in Program mode.
4. From the Backup/Restore Configuration Area of the Database tab, select the Backup button for Backup Configuration Database. Follow the steps to create the backup. This will save the data from the active backup node databases.
5. From the Backup/Restore Configuration Area of the Database tab, select the Restore button for Restore Configuration Database. Follow the steps to restore the configuration databases. This will restore the backup data created in step 4 to both the primary and backup nodes.
6. Select Fleets > Batch Validate and perform a batch validation for all the fleets. This data will be sent to both the primary and backup nodes.

7. Telnet to the backup node (which should be in Standby mode), and perform a “tairnet restart”. The primary node should restart and re-enter Standby mode.
8. Select *Node* > Status to display the Node Status window. On the Overview tab, check that the database checksums of the nodes match.
9. If the customer prefers that the primary node be Active, and the backup node be Standby in normal operation, perform the following procedure:
 - a. On the Overview tab of the Node Status window, set the backup node to Program mode by selecting the Enter/Exit Programming Mode Change button. This will promote the primary node back to Active status.
 - b. Telnet to the backup node and perform a “tairnet restart”. The backup node will restart and revert to Standby mode.

 The reason why the procedures in [Section 12.4](#) are sometimes required to be performed is as follows:

Tait have found that it is common for a fleet to be created, validated to the node database, and then later deleted from the NMT. This leaves data on the node validation database that is not present in the NMT fleet database.

When the batch validate operation sends all of the NMT fleet database data to the fresh node, the deleted fleet data is not sent, because this data no longer exists in the NMT database. This results in the validation data on the two nodes being different. As the validation data is different, the overall database checksum of each node will not match. This checksum is the product of several database checksums from databases in the node. Typically, all of the databases will be identical, apart from the validation database.

Appendix 1: Transferring an ISO Image to a USB Flash Drive

Bootable ISO images, such as the Tait CentOS ISO, can be transferred to a USB flash drive using either Win32DiskImager or another tool such as Rufus, both of which are documented here. Non-bootable ISO images, such as the TaitNet installation software, requires Win32DiskImager.

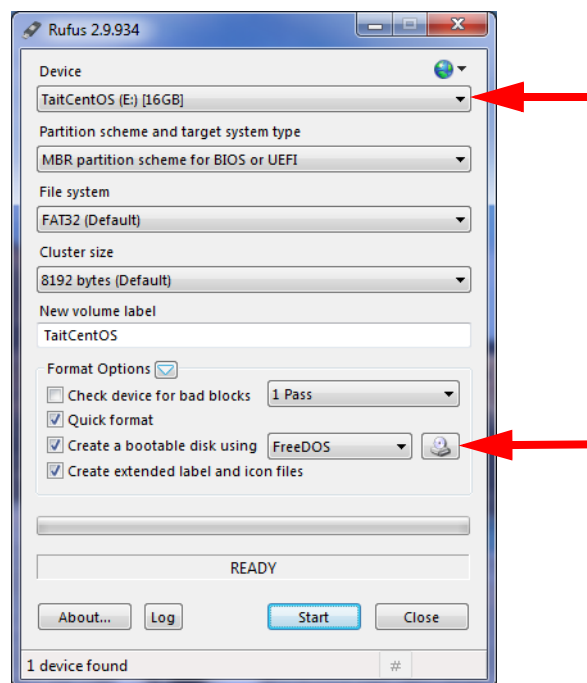
The advantage of Rufus over Win32DiskImager is that when the USB flash drive has been written to, the USB flash drive is still able to be read from and written to under Windows. This allows the user to add any additional scripts, configuration files etc. to the USB flash drive.

1.1 Using Rufus

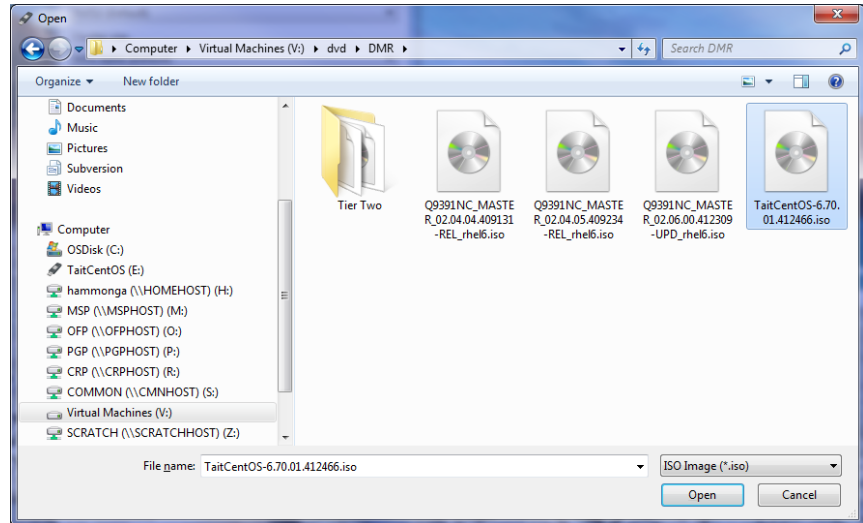
1. To create a bootable USB flash drive with TaitCentOS, first download and install the Rufus application. Note that Rufus cannot be used to write non-bootable ISO images, such as the TaitNet installation software.

Notice Only install the TaitCentOS version supplied by Tait, to ensure that the correct configuration settings are installed.

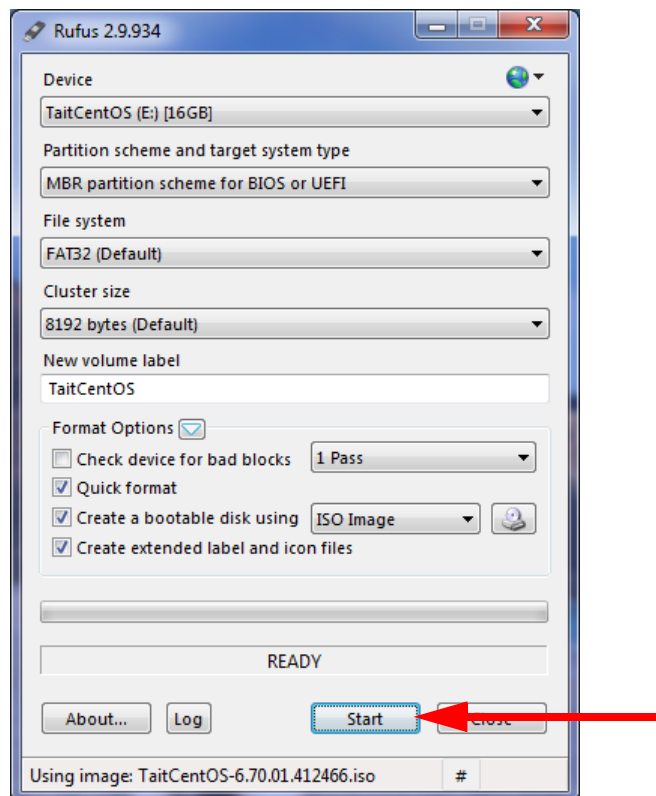
2. Insert a suitably sized USB flash drive into one of the PC's USB ports. (TaitCentOS will require at least an 8GB flash drive.)
3. Run the Rufus program.



4. Check that the Device in the first drop down list is the same as the USB flash drive.
5. Click on the CD icon next to the drop down list containing 'FreeDOS'. This will open a dialog box to enable the selection of the ISO file to be written to the USB flash drive.
6. Select the ISO file and click Open, which takes you back to Rufus.



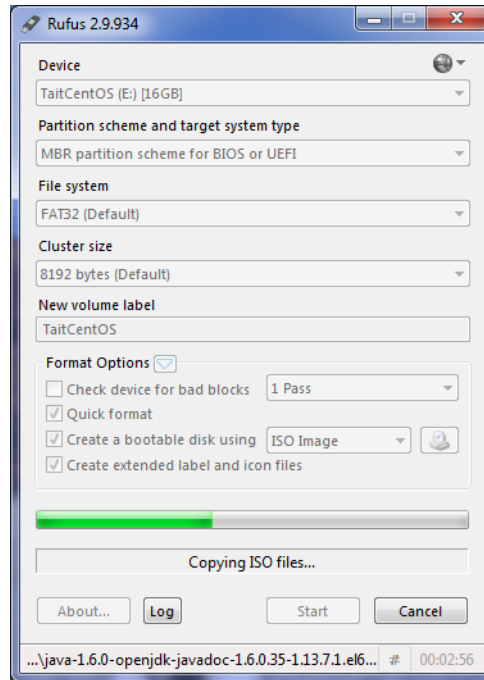
7. When ready to start the writing process, click Start.



8. A dialog box will appear to confirm that a write operation is to be carried out. At this point double check that the correct device is being written to and then click OK.

Depending on how large the ISO file is and the write speed of the USB flash drive, it could take from less than a minute to half an hour or more to complete the write process.

9. The progress of the USB flash drive write is displayed as follows:



10. When the USB flash drive write has finished, the Cancel button will change to a Close button. Click Close to complete the process.
11. Remember to safely eject the USB flash drive before physically removing it from the PC.

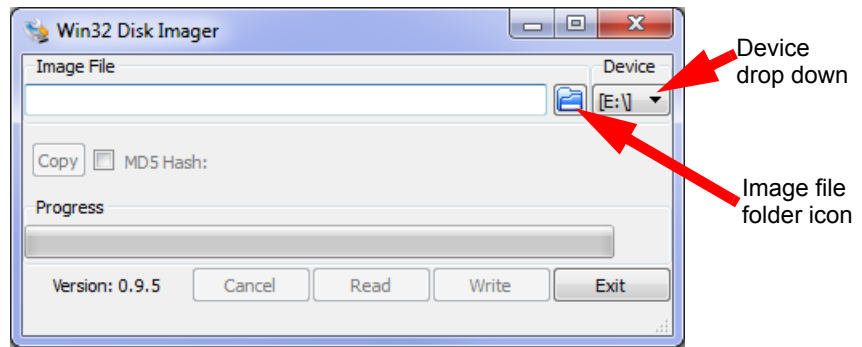
1.2 Using Win32DiskImager

1. To create a USB flash drive with TaitCentOS or node controller software, first download and install the Win32DiskImager application.

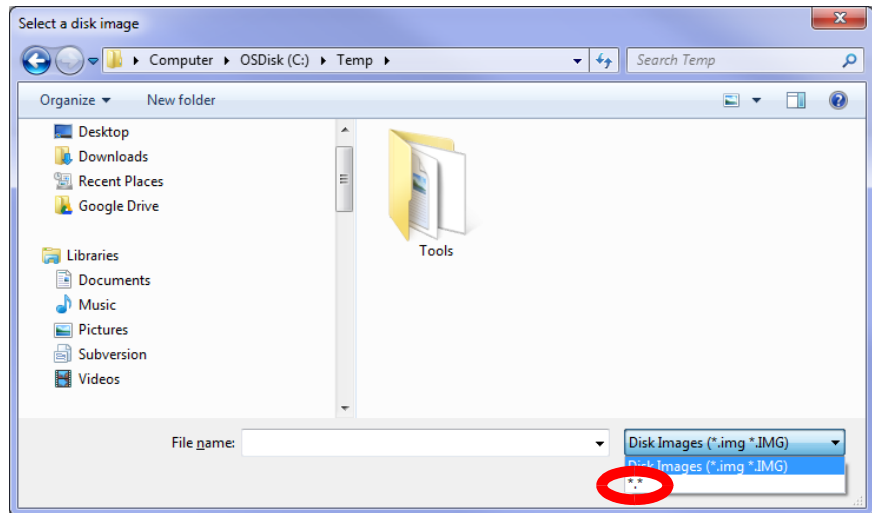
Notice Only install the TaitCentOS version supplied by Tait, to ensure that the correct configuration settings are installed.

2. Insert a suitably sized USB flash drive into one of the PC's USB ports. (TaitCentOS will require at least an 8GB flash drive, and for the node controller application 1GB or greater is required.)

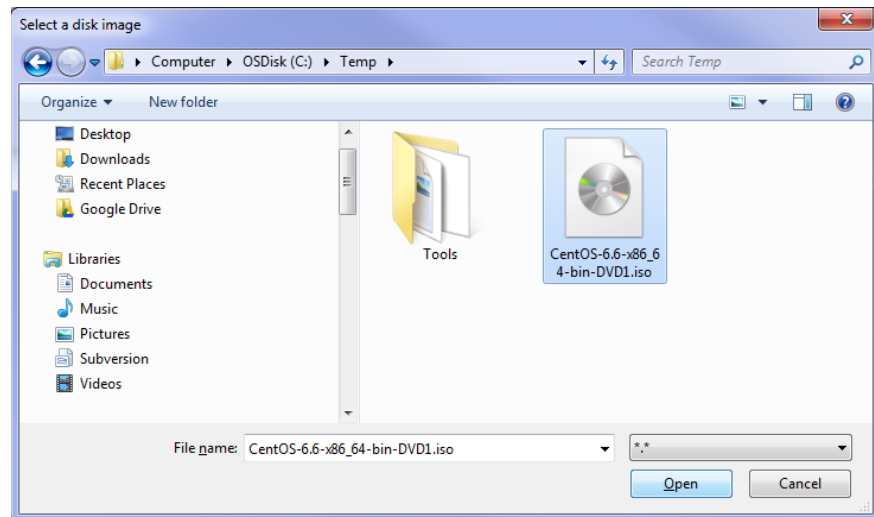
3. Run the Win32DiskImager program.



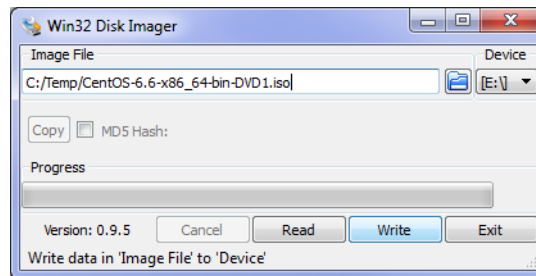
4. Check that the drive letter in the Device drop down list is the same as the USB flash drive. If you get this wrong, you could erase the wrong disk.
5. Click on the folder icon for the Image file.
6. Change the file filter from Disk Images (*.img *.IMG) to *.*



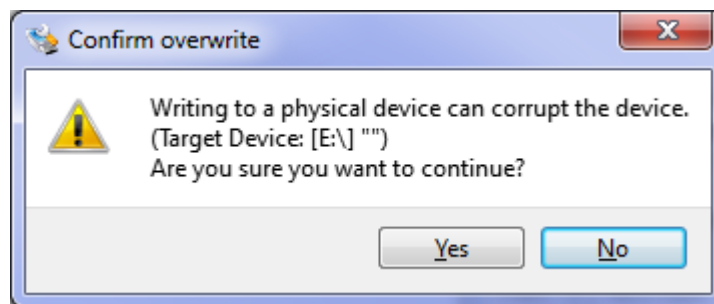
7. Select the desired iso file and click Open.



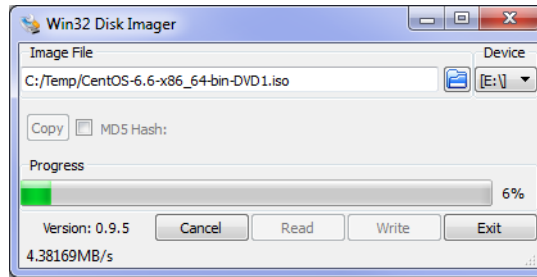
8. When ready to proceed, click Write.



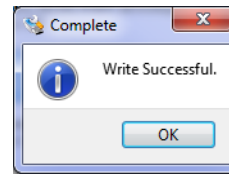
9. A Confirm overwrite dialog will appear which gives you a last chance to abort the process. Click Yes to continue.



10. The writing to the USB flash drive will begin and, depending on the quality/speed of the USB flash drive, this could take some time.



11. When the write has completed, a completion dialog will appear. Click OK.



12. Close the Win32DiskImager program.
13. Eject the USB flash drive by clicking the Safely Remove Hardware and Remove Media icon in the notification area, then clicking on the USB flash drive device.
14. Remove the USB flash drive from the PC.

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 Licensee'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.