tait
communications

TN9400 Access P25 Trunked Network

Controller Installation and Configuration Manual

MNC-00006-01 · Issue 1 · April 2016

www.taitradio.com

Contact Information

Tait Communications
Corporate Head Office

Tait Limited
P.O. Box 1645
Christchurch
New Zealand

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

Copyright and Trademarks

Disclaimer

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

Enquiries and Comments

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

Updates of Manual and Equipment

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

Intellectual Property Rights

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

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

Environmental Responsibilities

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

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

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

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

Contents

Preface

Scope of Manual

This document describes procedures for the configuration of the operating system and software components that make up a TN9400 Access High Availability controller.

This document is limited to the operating system, software and configurable components of the TN9400 controller. It does not include maintenance of the hardware. For documentation and hardware support of Dell R620 servers, see http://www.dell.com/support/home/us/en/19/product-support/product/poweredge-r620/manuals

This manual presupposes a knowledge of how to carry out basic procedures, such as logging on, launching the desktop, accessing a command line prompt and opening a monit summary window

Document Conventions

“File > Open” means “click File on the menu bar, then click Open on the list of commands that pops up.” “Monitor > Interfaces > Channel Group” means for the CSS “click the Monitor icon on the tool bar, then in the left-hand navigation tree click Channel Group under the Interfaces heading.”

Alerts

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

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

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

Associated Documentation

The full customer documentation set for TN9400 P25 trunked networks is provided on a documentation CD supplied with the network. Updates may also be published on the Tait support website. Technical notes are published from time to time to describe applications for Tait products, to provide technical details not included in manuals, and to offer solutions for any problems that arise.

Publication Record

Issue	Publication Date	Description
1	April 2016	First release. Describes the version 1.90 network.

Terms and Abbreviations

Term	Definition
Active	An HA controller that is performing the role and function of an RFSS Controller, Site Controller or PSTN Gateway.
DRBD (Distributed Replicated Block Device)	A mechanism for replicating disk partition contents between different controllers via a network connection. Only used for HA controller configurations.
HA (High Availability)	A mode of operation where two controllers are available to perform the function of a single logical controller such that if one of the controller's hardware and/or software fails, the other controller will take over the role and function of the failed controller.
Controller A Controller B	One half of a HA controller pair.
ISSI	Project 25 Inter RF Subsystem Interface, a non-proprietary interface that enables RFSSs built by different manufacturers to be connected into wide area networks.
ITU	The International Telecommunication Union is a UN agency that coordinates the shared global use of the radio spectrum and assists in developing telecommunications standards and infrastructure.
Offline	In an HA setting, an offline controller is not available to operate as part of an HA controller pair. In a standalone setting, an offline controller is not able to perform the role and function of an RFSS Controller, Site Controller or PSTN Gateway.
Primary	DRBD disk partition that is in active use
Standalone	DRBD disk that is not available for network communications with other DRBD partitions.
Secondary	DRBD disk partition that is not in active use.
Standby	An HA controller that is able to take over the role of active controller to perform the role and function of an RFSS Controller, Site Controller or PSTN Gateway.
Takeover	The action of an HA controller to go into the online state.

1 Numbering for TN9400 Networks

This chapter is intended as a guide to assist in creating the IP addressing plan and P25 network identifiers for a TN9400 IP network and in configuring the network with them.

The section "Configuration Template" on page 14 contains a template in which you can enter information required by the configurations described in this document for use as a ready reference while undertaking the configurations.

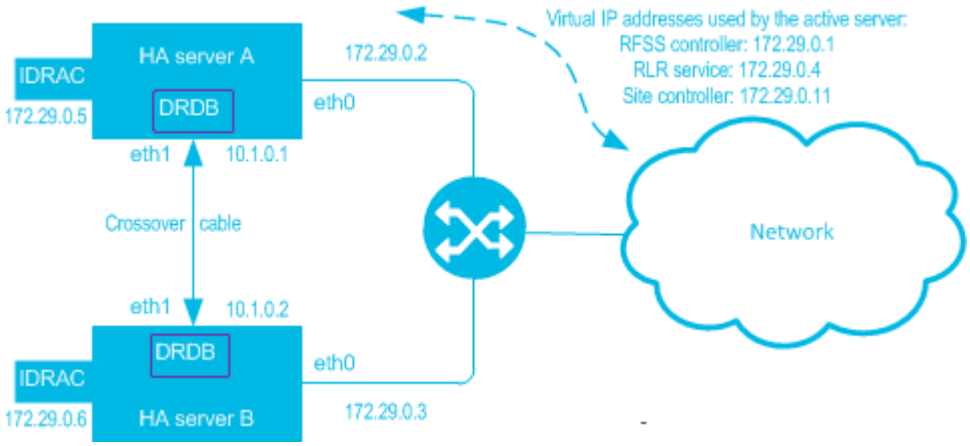
1.1 IP Addresses

Unless otherwise agreed with the customer, Tait builds TN9400 systems with the private class B network 172.29.0.0 mask 255.255.0.0. This class B block is split into ranges based on the third number of the IP address. The RFSS controller and its associated equipment is given 0 and each site is given a unique number.

1.1.1 Access System

All equipment associated with the RFSS controller is given IP addresses in the range 172.29.0.x. This is sufficient for most systems, though if there are many dispatch consoles, a custom scheme may be required.

The Access system runs on a cluster of two servers, with the RFSS application using a virtual IP address. If one server fails, the other server takes over the virtual IP address.



IP Address Scheme The following IP address scheme is used.

Host	IP	Description
RFSS	172.29.0.1	HA cluster: The (virtual) IP address used by the active RFSS controller application (defined in RFSS Manager) Single server: Physical IP address of the RFSS server.
High Availability (HA) RFSS A	172.29.0.2	Physical IP address of the Primary HA RFSS (defined in the server itself).
HA RFSS B	172.29.0.3	Physical IP address of the Secondary HA RFSS.
Fleet Manager (RLR)	172.29.0.4	(virtual) IP address of the Fleet Manager application (defined in RFSS Manager).
Access A IDRAC	172.29.0.5	Physical IP address of the Primary Access IDRAC
Access B IDRAC	172.29.0.6	Physical IP address of the Secondary Access IDRAC
PSTN Gateway	172.29.0.7	Physical address of the PSTN Gateway
PSTN Gateway IDRAC	172.29.0.8	Physical address of the PSTN Gateway IDRAC
Enable Monitor	172.29.0.9	Physical address of Enable Monitor
Enable Monitor IDRAC	172.29.0.10	Physical address of Enable Monitor IDRAC
Site Controller	172.29.0.11	Virtual IP address of the site controller
Frequency Reference	172.29.0.17	Physical IP address of the frequency reference if connected to the LAN
Voice Recorder	172.29.0.20 (and 21)	Physical IP address(es) of the voice recorder system
Local PC	172.29.0.22	Physical IP address of the Local PC
Dispatch console system	172.29.0.23 to 39	IP address range reserved for the dispatch console system
TB9x00 Base Station	172.29.0.<Channel ID + 40>	E.g. Channel 1 is 172.29.0.41 and Channel 10 is 172.29.0.50
Miscellaneous equipment	172.29.0.201 to 172.29.0.249	If miscellaneous or third party equipment is used then assign it an address in this range
Technician PC	172.29.0.250	Physical IP address reserved for use by a technician when connecting a laptop during a site visit.
Switch	172.29.0.252	Physical IP address of the local switch, that is separate from the router
Router Switch Module	172.29.0.253	Physical IP address of switch that is in the Router.

Host	IP	Description
Router (Default Gateway)	172.29.0.254	LAN IP address for the default router used by all equipment on this network.
	xxx.xxx.xxx.xxx	The customer will need to provide the IP address for the router's WAN port.
HA eth1 port on RFSS A	10.1.0.1	IP address used for the HA cable between servers
HA eth1 port on RFSS B	10.1.0.2	IP address used for the HA cable between servers

1.1.2 Simulcast Equipment

The following address scheme can be used for simulcast networks that only have one site controller (cluster), at the same location as the RFSS controller. Larger simulcast networks require a custom scheme. The third number of the IP address is assigned to base stations based on the radio area instead of the site. (The radio area is the simulcast equivalent of a site, but the radio areas together form a logical site from the perspective of the core network.)

Host	IP	Description
Frequency Reference	172.29.<radio area ID>.17	Physical IP address of the frequency reference if connected to the LAN.
TB9x00 Base Station	172.29.<radio area ID>.<Channel ID + 30>	E.g. Site 1, Channel 1 is 172.29.1.31 and Site 2 Channel 10 is 172.29.2.40
Miscellaneous equipment	172.29.<radio area ID>.201 to 172.29.<radio area ID>.249	If miscellaneous or third party equipment is used then assign it an address in this range
Technician PC	172.29.<radio area ID>.250	Physical IP address reserved for use by a technician when connecting a laptop during a radio area visit.
Switch	172.29.<radio area ID>.252	Physical IP address of the local switch, that is separate from the router
Router Switch Module	172.29.<radio area ID>.253	Physical IP address of switch that is in the Router.
Channel group multicast address	239.0.0.*n*	This address is used for voting in channel groups. *n*=channel group number. Any IP address in the range 239.0.0.0/8 can be assigned. These are Administratively Scoped IPv4 Multicast addresses defined in RFC 2365. Addresses in the range 224.0.0.0 should not be used as most of them are reserved for various well-known protocols. This address is part of the channel group configuration, defined using the CSS (TB9100) or web interface (TB9400).

1.2 P25 Identifiers

P25 works with the following hierarchy of identifiers.

Item	Example	Description
WACN ID	A4397	5 hexadecimal characters
System ID	2cc	3 hexadecimal characters
RFSS ID	01	2 hexadecimal characters (4 are used for dispatch consoles)
Site ID	72	2 hexadecimal characters

Applications that participate in the TN9400 network are identified using ISSI domain names with the following format:

```
<site ID>.<RFSS ID>.<system ID>.<WACN ID>.p25dr.
```

P25 identities are defined in RFSS Manager, which generates hosts files that contain the mappings of IP addresses to P25 identifiers for all the elements in the network. Applications use the hosts files to convert between the P25 identifiers and IP addresses. P25 identifiers appear as locations in Fleet Manager. Some elements also require a SUID, so must be declared to Fleet Manager on the Subscribers page.

The WACN ID and System ID of a network require approval or assignment by the regulatory authority. The document Project 25 Guidelines to Assign Wide Area Communication Network and System Identities (available from www.taitonline.org) provides a standardized way of deriving these identifiers from the call signs for each country that have been adopted by the ITU.

1.2.1 RFSS IDs

The RFSS is given the RFSS ID 01, unless there are other RFSSs to be connected to it using ISSI, now or in the future. These are given IDs starting at the bottom of the range.

Dispatch consoles and voice recorders function like RFSSs and so need their own RFSS ID. They are given IDs from the top of the range.

Item	Example	Description
RFSS	1	
Dispatch console	13FE	Dispatch equipment connected by CSSI is effectively its own RFSS, so needs an RFSS ID
Voice recorder	FD	The voice recorder connected by ISSI is effectively its own RFSS, so needs an RFSS ID.

1.2.2 Site IDs

Several network elements apart from site controllers function as virtual sites and so need their own site ID. Tait recommends numbering site controllers from the beginning of the number range, and numbering other equipment from the top of the range down.

Item	Default Site ID	Description
Site controllers	1	One site per system.
Fleet Manager	FE	The Fleet Manager needs a site ID. It operates as a virtual site, with a single virtual SUID.
PSTN Gateway	FD	A PSTN gateway operates as a virtual site.

1.2.3 Subscriber Unit and Group IDs

SUIDs and Group IDs must be unique for each RFSS. The following address ranges will need to be subdivided if the network has more than one RFSS. Address ranges are assigned using Fleet Manager.

Item	ID Range	Description
Groups	1-65535	Reserved for group addresses. The number range needs to be separate from SUIDs, so that telephone calls can be made to groups.
Dispatch consoles and voice recorders	65537-65999	Reserved for FNE. Each console position needs its own SUID.
Fleet Manager	0x0000FE	Fleet Manager operates with a virtual SUID, which it uses for operations such as radio check. Use the same number as Fleet Manager's site ID.
SUs	66000-9999999	Each SU needs its own SUID.

1.3 Defining Identifiers

Defining IP addresses and P25 IDs is a four-stage process (described in Chapters 6 and 7):

1. Assign an IP address and basic Internet identity to the server itself.
2. In the RFSS Manager, enter other IP addresses and P25 identifiers for all network elements with P25 software.
3. Using command line scripts, propagate RFSS Manager settings to the hosts files and configuration files of the network elements.
4. In the Fleet Manager, P25 IDs appear automatically on the Locations page when the network elements communicate with the RFSS manager. For each location, you need to specify the location type and manually enter a suitable (human-readable) alias, such as Site 1 or RFSS North. You also need to declare the SUIDs that network elements will use.

1.4 Configuration Template

Before configuring Taitnet CentOS and the RFSS Manager the following parameters should be defined. You can write them on this template as a ready reference.

It is important to ensure that each hostname and IP address is consistent across all fields. Problems during configuration often arise due to a hostname or IP address being entered in different ways in different RFSS elements.

Network (RFSS)	
The name of the RFSS	
The IP address of the application used by the controller servers	
The RFSS ID (hex identifier) Appended by `/WebUI` for the RFSS Manager and `/RLR` for the Fleet Manager	
The system ID of the system to which the RFSS belongs	
WACN ID (the hex identifier of the WACN to which this system belongs)	
The addresses of the NTP server(s) used for time synchronization	
The IP address of the manager to which SNMP traps are sent	
The community string to include in SNMP v2c or SNMP v1 GET requests (supplied by Tait)	
Controller(s)	
Your organization's name(s) for the controller(s)	
Controller A hostname (the name of the controller A server in High Availability)	
Controller A IP address	
Controller A DRBD address	
Controller A iDRAC IP address	
Controller B hostname	
Controller B IP address	
Controller B DRBD address	
Controller B iDRAC IP address	

Controller Netmask	
Controller Gateway (router) - or ‘Network check device IP address’ in the RFSS Manager	
Fleet Manager	
Your organization’s name for the Fleet Manager	
The Fleet Manager’s IP address	
The Fleet Manager’s site ID	
The Fleet Manager’s SUID	
PSTN Gateway	
Your organization’s name for the PSTN Gateway	
The RFSS controller with which the Gateway is associated	
The IP address of the server	
Hostname (the network name for the server running the application)	
The PSTN Gateway’s site ID	
The IP address of the PSTN router	
The Site	
Your organization’s name for the site	
IP address	
Site ID (the two-hex digit by which the site is known to the RFSS)	
Hostname (the network name for the server)	
The LRA (Location Registration Area)	
The site’s NAC (the system ID)	
First Frequency Plan	
Your organization’s name for the frequency plan	
The plan’s ID (a unique number between 1 and 16)	
Channel type (FDMA or TDMA)	
The base frequency (Hz)	

The transmit offset (Hz)	
The offset sign	
The channel bandwidth (Hz)	
The channel spacing (Hz)	
Second Frequency Plan (for TDMA)	
Your organization's name for the frequency plan	
The plan's ID (a unique number between 1 and 16)	
Channel type (FDMA or TDMA)	
The base frequency (Hz)	
The transmit offset (Hz)	
The offset sign	
The channel bandwidth (Hz)	
The channel spacing (Hz)	
A Channel	
Your organization's name for the channel	
Control channel (primary or backup)	
Traffic channel usage (voice only, data only, or voice or data)	
Channel transmit frequency (Hz)	
Channel receive frequency (Hz)	
Transmit frequency calculation method (implicit or explicit)	
A Transceiver	
Your organization's name for the transceiver	
Transceiver type (TB9100 or TB9400)	
IP address	
Control port	
Voice port	
Whether primary, secondary or satellite	
Whether or not TDMA capable	

2 Configuring BIOS and iDRAC

The TN9400 Access High Availability controller can be built on either a Dell R220 or R630 server.

This chapter covers Dell R220 and Dell R630 Server BIOS and iDRAC. TN9400 controllers are normally shipped with BIOS and iDRAC configured. In this case all the settings below should be correct except for step 2 in "Configuring iDRAC Options" on page 18. It is part of the IP plan outlined in "Numbering for TN9400 Networks".

BIOS and iDRAC will need to be reconfigured in the wake of a major system failure that requires a controller to be configured from scratch.

2.1 Prerequisites

The following items are required before commencing the configuration of the BIOS and iDRAC:

- IP Address for remote access.
- Subnet mask for remote access.
- IP address for the servers' gateway.
- VGA (DB15) monitor, USB keyboard and USB mouse.

2.2 Configuring BIOS Options

1. Connect a monitor, keyboard and mouse to the front of the Dell server being configured.
2. Boot server and wait for the Dell logo screen during early boot then press the F2 key when 4 options appear in the top right corner of the Dell logo screen.

   After a period of approximately 1 minute, the 'System Setup' screen appears.
3. Select 'System BIOS'.
4. Click 'Memory Settings' and set the 'System Memory Testing' to 'Enabled'.
5. Click the 'BACK' button (to return to 'System Bios Settings').
6. Click 'Boot Settings' → 'BIOS Boot Settings' → 'Boot Sequence'; click the 'Hard Drive C' and click the '+' sign to move the item to the top of the list. Click 'OK'.

7. Click the ‘BACK’ button twice to return to 'System BIOS Settings'.
8. Click 'System Security'.
9. Set the passwords.
10. Set 'AC Power Recovery' to 'On'
11. Set 'AC Power Recovery delay' if deemed appropriate.
    (Set to 60 seconds for HA controller B.)
12. Click the ‘BACK’ button to return to 'System Bios Settings'
13. Click 'Miscellaneous Settings'.
14. Set ‘System Time’ and ‘System Date’ to UTC.
    Tait recommends the use of UTC. If local time is used, time changes around daylight saving could cause issues.
15. Set ‘Asset Tag’ if deemed appropriate.
16. Set ‘Report Keyboard Errors’ to ‘Do Not Report’. (This step doesn’t appear in the R630.)
17. Set 'F1/F2 Prompt on Error' to 'Disabled'.
18. Click the ‘BACK’ button to return to 'System BIOS Settings'
19. Click the ‘Finish’ button.
20. Click the ‘Yes’ button to save the changes.
21. Click the ‘OK’ button.

2.3 Configuring iDRAC Options

1. Click 'iDRAC Settings'.
2. Click 'Network' and set up the appropriate IP V4 network settings for remote access. Click the ‘Back’ button when done.
3. Click 'Alerts' to set up any alerting options as appropriate.
4. Set the SNMP community string. The default is `tait_p25`.
5. Click the ‘Back’ button when done.
6. Click ‘User Configuration’, change the user name (default is `admin`) and the password (default is `k1w1`).
7. Click the ‘Back’ button when done.
8. Click the ‘Finish’ button.

9. Click the ‘Yes’ button and confirm reboot.

3 Installing the CentOS Operating System

TN9400 controllers are normally shipped with the TaitNet CentOS operating system already installed. (This is a Linux operating system configured for TN9400 controllers.) The procedures in this chapter are only necessary in the wake of a major system failure that requires a controller to be configured from scratch.

As the web browser and iDRAC do not always work smoothly together, some troubleshooting tips are included at the end.

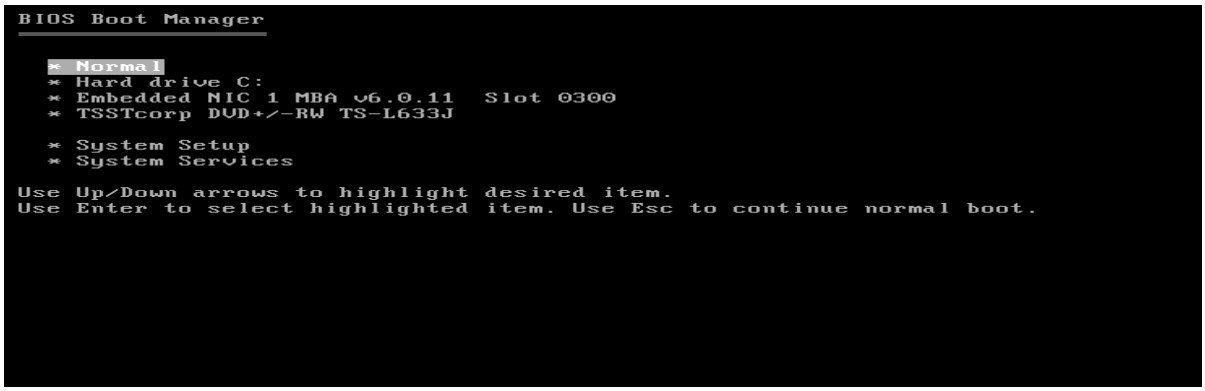
Prerequisites

- The TN9400 Controller doesn't have an OS installed or is being reinstalled with a new, clean OS installation.
- BIOS and iDRAC have been configured
- 406-00083-XX DVD Tait CentOS media

This procedure will overwrite any existing operating system on the controller.

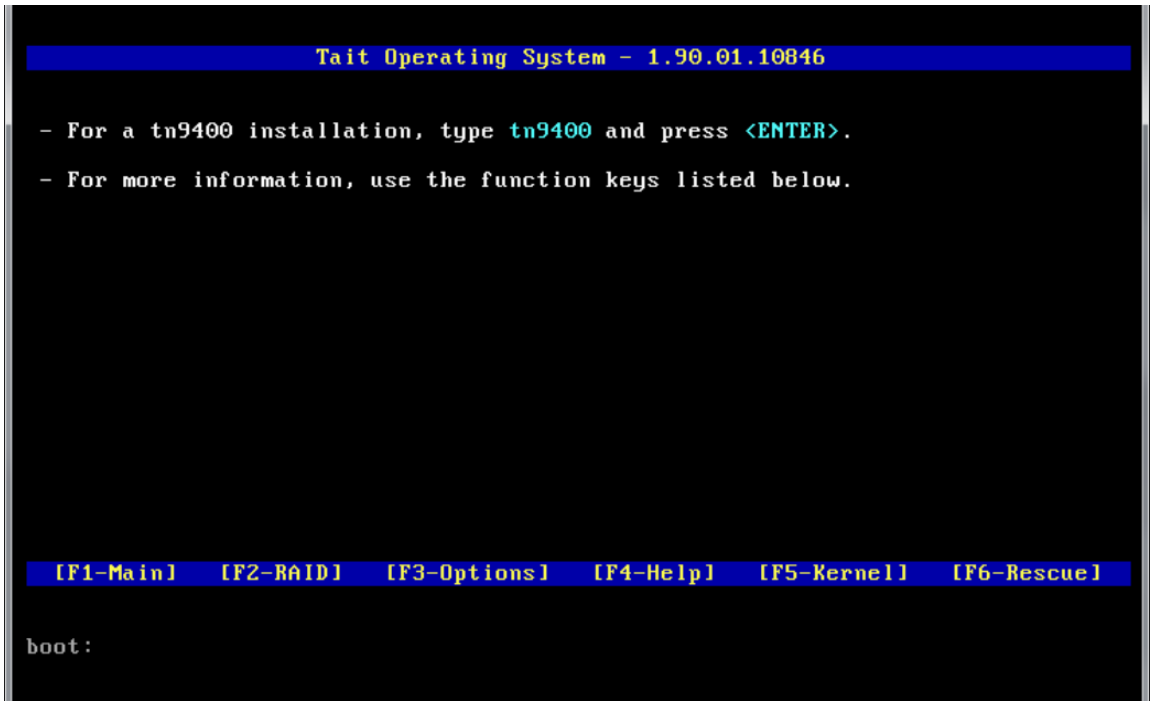
Procedure

1. Power up the server.
2. Either connect a monitor, keyboard and mouse to the front of the Dell server being configured, or establish an IP connection to the iDRAC virtual console on the server.
3. Insert the 406-00083-XX DVD Tait CentOS media in the server's DVD drive.
4. Wait for the Dell logo screen to appear during early boot. As soon as it appears, press F11 to select the Bios Boot Manager option. The display of this option changes to Entering BIOS Boot Manager, confirming that the selection was successful. After a time, the graphical BIOS Boot Manager screen appears.
5. Scroll down to the BIOS Boot Manager option and select it. The text-based BIOS Boot Manager menu appears.



6. Select the item describing the DVD drive and press <enter>. (You may need to press the tab key before the arrow keys move the highlight.) This instructs the server to boot from the DVD.

7. When CentOS boots, the installation will pause at the following screen.

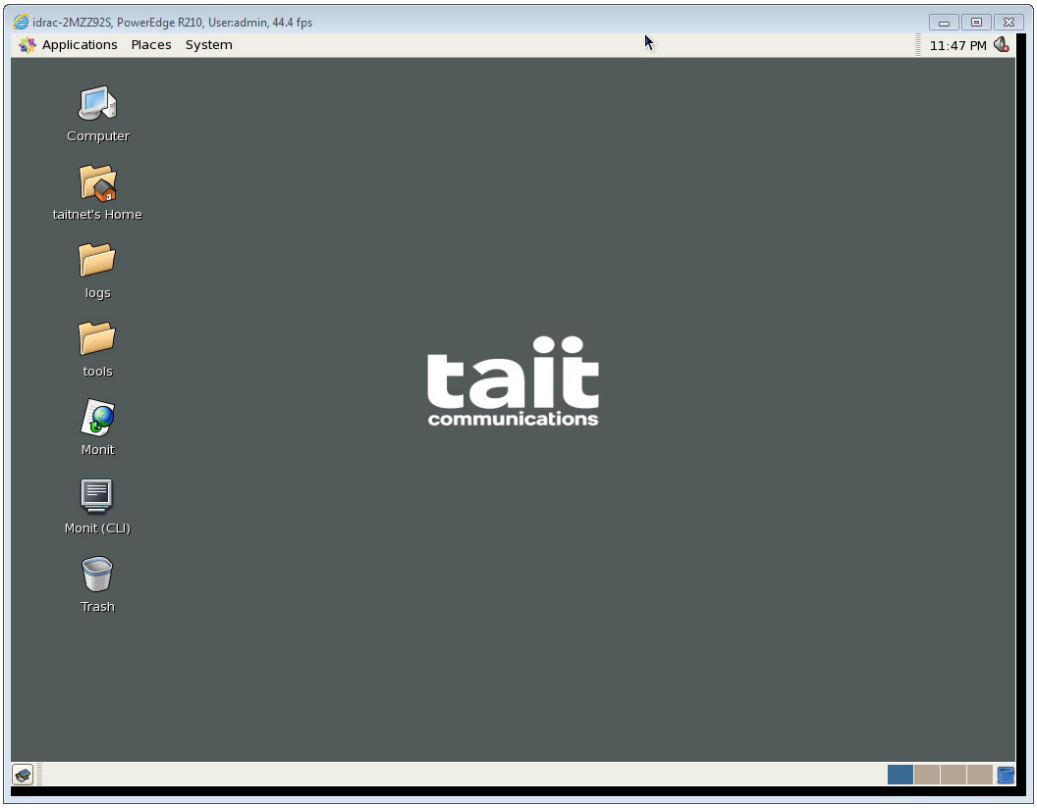


8. To initiate the operating system installation enter:

   `tn9400`

   The process will take up to 30 minutes during which time no human intervention is required. In particular, “Running post-install scripts” can take a long time. During this process the system is configured with default network parameters and user accounts, and then automatically restarts.

9. When the restart is completed, the white TN9400 Login screen appears. Log on with username `taitnet` and password `tait`. The desktop appears (as shown next page). You can now eject the DVD by right-clicking its icon and selecting Eject.



Troubleshooting

- When reinstalling the operating system on a TN9400 server, for example after hardware failure, it is good practice to remove locally stored SSH keys, i.e. SSH keys for the TN9400 server on any servers or PCs that have previously communicated with that server via SSH. You can do this as the RmUser or taitnet user by using the command:

  ```
  ssh-keygen -R <IP address of the remote host>
  ```

- You may experience difficulty logging on to the iDRAC or launching the virtual console. Try the following:
- Use Internet Explorer as your web browser. When you are asked to add the Dell ActiveX control to enable the Virtual Console, enter, `yes`.
- If the iDRAC web page is empty, in Internet Explorer select Tools > Compatibility View Settings and add the iDRAC website to the list of websites.

4 Installing the Controller Software

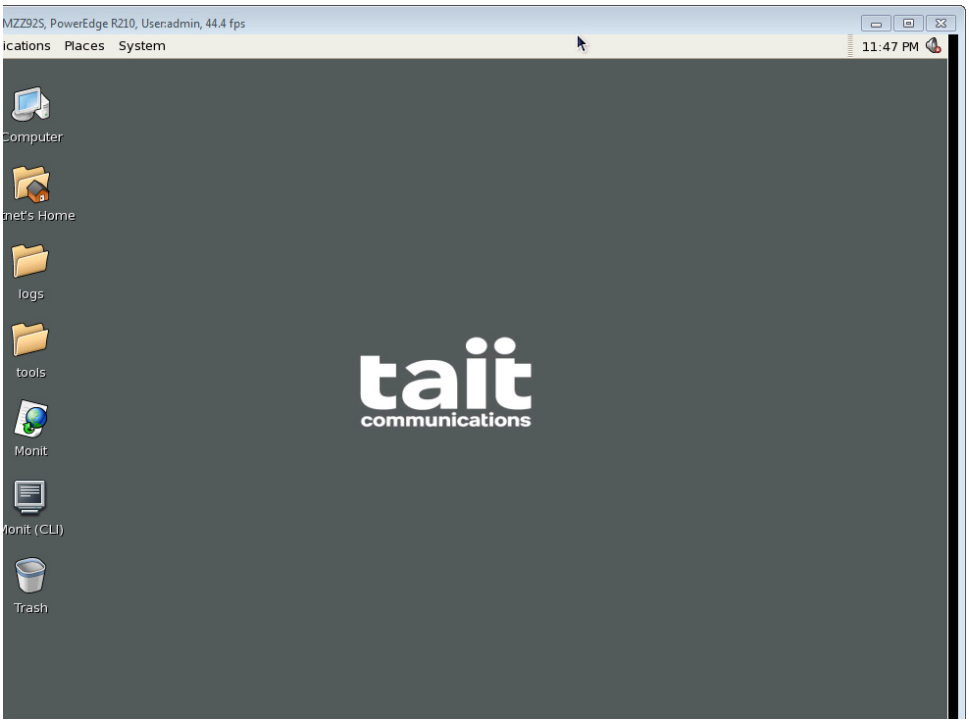
This chapter marks where a normal configuration begins — other than entering the iDRAC IP address (see "Configuring iDRAC Options" on page 18). Controller software is only installed, and network settings configured, after the controller has had its BIOS and iDRAC configured and the TaitNet CentOS operating system installed. Tait normally ships controllers with these procedures already carried out.

Prerequisites

- TaitCentOS has been installed on the controller and the DVD removed.
- TN9400 Software DVD (406-00084-XX).

Procedure

1. On a locally connected keyboard, log in to the controller as the `taitnet` user, password `tait`. The desktop appears.



2. Insert the TN9400 software DVD in the DVD drive.
3. On the desktop, open a terminal window by double-clicking the Tait logo and selecting ‘Open Terminal’.
4. Install the Access software for the controller by entering the following commands:

```
sudo service mysqld start
package install access
sudo service mysqld stop
```

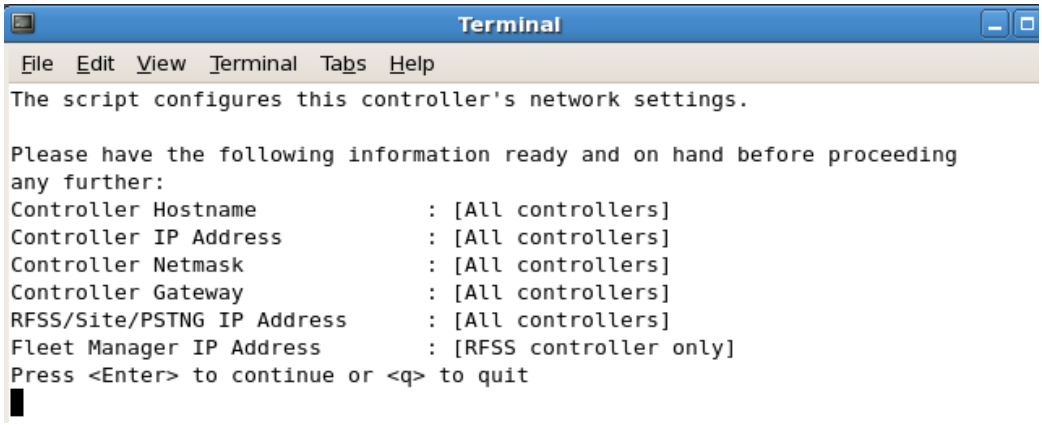
5. Eject the DVD when completed:

   `eject`

6. Enter the following command:

   `sudo access_config.sh`

   The following screen should appear.



   This is where you define the controller A network settings. The template in Section 1.4 of this manual may be useful here.

7. Press <Enter> to display the current settings. These are defaults set during the installation of the operating system.

8. Press <Enter> again. You can now define the first item, the hostname.

9. Press <Enter> to confirm your entry and move to the next item, the controller IP address.

   After entering the RFSS Manager address ('RFSS/Site/PSTNG IP Address') you are asked if the controller will be configured as an RFSS Manager. Enter <y>.

   If a mistake is made in a setting, press <q> to quit the script and then rerun it to make any corrections. The script can be rerun at any time.

10. Once all the settings have been correctly entered, press <enter> to apply them. A successful execution of the script will give a screen indicating which files have been changed and requesting a controller reboot.

11. Enter:

    `reboot`

5 Installing High Availability Software

Prerequisite

The controller A software has been installed and the controller A network settings have been defined. The controller has just been rebooted (see step 11 page 24).

Procedure

1. Log in to the controller as the `taitnet` user, password `tait`. The desktop. will appear.
2. On the desktop, open a terminal window by double-clicking the Tait logo and selecting ‘Open Terminal’.
3. Enter the following command to install the HA package:

   ```
   package install ha
   ```

   This creates the following:

   The ‘HA Takeover,’ ‘HA Standby’ and ‘HA Status’ shortcuts appear on the desktop.

   The ‘Start HA’ and ‘Stop HA’ shortcuts appear in the desktop folder ‘tools:’.

   The ‘Live HA Log’ shortcut appears in the desktop folder ‘logs:’
4. Configure controller B. This is a repeat of the procedure already followed for controller A, described in the previous chapter.

6 Configuring the HA Access Controller

Prerequisites

- Taitnet CentOS has been installed and configured on both Access controllers.
- High Availability, RFSS and site controller software has been installed on both Access controllers.
- The network settings have been defined on both Access controllers.
- All the relevant network IP information is at hand. This is where the template in "Configuration Template" on page 14 may be useful.

6.1 Configure Access Controller A

Procedure

1. Log in to controller A, which is used for distributing configuration information as the `taitnet` user, password `tait`. The desktop will appear.
2. Open a terminal window by double-clicking the Tait logo and selecting ‘Open Terminal’.
3. Restart the system services and start the RFSS Manager service by typing:
   ```
   restart services
   start rm
   ```
4. Open the web browser and enter the RFSS Manager IP address followed by `/WebUI` — for example, `https://172.29.0.1/WebUI`
   Continue through the routine warning message and enter the default password and username:
   ```
   administrator
   taitadmin
   ```
5. The RFSS Manager will appear, which must now be configured. As part of the configuration, a site needs to be defined, with a channel and transceiver, which requires a frequency plan to be configured.
   Depending on the network, fields on all the screens under ‘Configure’ in the left-hand menu will need to be filled out, with the exception of ‘External RFSSs’, ‘Packet data’ and ‘PSTNG’. The site is configured in ‘Sites’. Many fields in these screens have default settings that can be left as is.

Use the Help of the RFSS Manager for more information.

6. Return to the terminal window of controller A. Deploy the TN9400 configuration files, host files and optionally the NTP and SNMP configuration files to the controller by entering the following commands.

   If the RmCli command is not found, log out and re-log in as the `taitnet` user.

   ```
   RmCli share_key
   ```

   (The second command should only need to be run the first time configuration files are deployed, or if a controller has been replaced, or a new controller added to the system.)

   ```
   RmCli send_all
   ```

   ```
   RmCli update_ntp
   ```

   (This is an optional step.)

   ```
   RmCli update_snmp
   ```

   (This is an optional step.)

7. Copy the Access license file to the controller. This is done in the RFSS Manager. In the ‘RFSS’ screen under ‘Configure’ (the first screen that appears), click ‘Edit’ and scroll down to ‘License’. Click ‘Upload’ for controller A and select and Apply the license file (its name includes `QNB20RNC` followed by the host ID). The controller B license can be uploaded now also.

8. (Optional) Copy the site controller license file to the controller if the Access controller is to be configured for Phase 2 functionality. This is also done in the RFSS Manager. Under ‘Sites’ select the site, click ‘Edit’ and scroll down to ‘License’. Click ‘Upload’ for controller A and select and Apply the license file (its name includes QNB20SC followed by the host ID). The controller B license can be uploaded now also.

9. Reset the file permissions, start the Access controller and check to see if the controller is behaving as expected:

   ```
   set_permissions
   ```

   ```
   start access
   ```

10. Restart the controller to confirm the controller starts up with the RFSS and site running:

    ```
    reboot
    ```

11. Configure the HA package:

    ```
    ha_config --force primary
    ```

    Wait for 30 seconds after the completion of the ha_config script, at which point controller A should become the active controller in the cluster.

12. Stop the HA service and reboot the controller to confirm the controller starts as the active controller in the cluster:

    ```
    stop ha
    ```

    ```
    reboot
    ```

6.2 Configure Access Controller B

Prerequisites

As for Controller A, with the addition of:

- Controller A has been installed and configured as the active HA controller.
- The configuration files have been deployed.

Procedure

1. Log in to controller B as the `taitnet` user, password `tait`. The desktop will appear.
2. Copy the Access license file to the controller by navigating in the RFSS Manager, ‘RFSS’ > ‘Configure’ > ‘Edit’ > ‘License’.
3. (Optional) Copy the site controller license file to the controller if the site is to be configured for Phase 2 functionality by navigating in the RFSS Manager, ‘Sites’ > the site > ‘Edit’ > ‘License’.
4. Reset the file permissions and configure the HA package:

   ```
   set_permissions
   ha_config --force secondary
   ```

   Wait for 30 seconds after the completion of the ha_config script, at which point controller B should become the standby controller in the cluster.
5. Close the terminal window and open a new one. Monitor the status of the HA cluster:

   ```
   ha_status –t 5
   ```
6. Observe the HA status on controller B to confirm that the DRBD partitions are synchronizing. Wait until the synchronization has completed.
7. Close the ha_status window:

   ```
   q
   exit
   ```
8. Open another terminal window. Stop the HA service and reboot the controller to confirm the controller starts as the standby controller in the cluster.

   ```
   stop ha
   reboot
   ```

After the reboot, both controllers should be operating as a normal HA cluster. It is recommended that testing of the ‘standby’ and ‘takeover’ commands is carried out to ensure correct operation of the HA cluster.

6 Configuring the Fleet Manager

The final stage to having a basic RFSS up and running is to configure the Fleet Manager (in IP addresses it is called the RLR).

Prerequisites

- Access Controller A and Access Controller B have been installed and configured.

Procedure

1. Open the web browser and enter the Fleet Manager IP address followed by `/RLR` — for example, `https://172.29.0.4/RLR`
2. Continue through the routine warning message and enter the default password and username:

   `administrator`

   `taitadmin`

   The Fleet Manager will appear, which must now be configured. There is an online help for guidance.
3. Enter the ‘Locations’ screen, then click on ‘Add a New Location’ to configure the Fleet Manager as a location. A warning message is displayed that the Fleet Manager’s location ID cannot be resolved, and the ID shown in the message can be copied and pasted to the first field. The location type is RLR. Click Add to add it to the Locations table.
4. Remaining in ‘Add a New Location’, configure the site as a location and click Add.
5. Still in ‘Add a New Location’, configure the RFSS as a location and click Add.
6. Enter ‘Groups’ > ‘Home RFSS Map’ to assign the range of group ID numbers that will be associated with the RFSS.
7. In ‘Groups’ > ‘Groups’ > ‘Add a New Group’ create a group for the subscribers you are about to define to affiliate to.
8. Enter ‘Subscribers’ > ‘Home RFSS Map’ to assign the range of subscriber ID numbers that will be associated with the RFSS.
9. In ‘Subscribers’ > ‘Subscribers’ > ‘Add a New Subscriber’ to configure the Fleet Manager as a subscriber of the type FNE. A warning message that the Fleet Manager’s unit ID has not been entered, enables you to copy and paste the ID shown in the message to the first field. Click Add to add it to the Subscriber List.
10. Still in ‘Add a New Subscriber’, configure radios (SUs) for use in testing.

Appendix A – TN9400 Tools

The Tait TN9400 Tools package installs a number of scripts to the 'taitnet' users folder `/home/taitnet/bin`. These scripts are used for maintenance and support activities and when run, display information about the TN9400 controller. The Tait Technical Support team may ask for one or more of these scripts to be run to assist in resolving service requests.

The scripts normally require root access to operate. Prefix the scripts with '`sudo`' to run the scripts with root privileges.

TN9400 Info Script

The TN9400 info script is a meta-script that calls other TN9400 Tools scripts in addition to displaying information itself. The following information is displayed:

- TaitCentOS version information.
- IP configuration checks.
- Result of network connectivity tests (ping tests).
- Firewall status and configuration checks.
- TN9400 package checks.
- NTP configuration checks.
- Summary of monit processes.
- Process information for specific processes.
- DRBD status for HA systems.
- Disk space usage.
- If there are any errors detected, the script will display the errors as the script runs and will display at the end, a message to say that errors have been found.

  To see only the errors, run the script again with the '`-q`' parameter, i.e., '`sudo TN9400_info.sh -q`'.

It is recommended that the script be run in the following circumstances:

- after commissioning of the system.
- after configuration changes to the system.
- before and after software upgrades.
- before and after networking infrastructure changes.
- prior to contacting Tait Technical Support

Script Usage

Usage:

```
TN9400_info.sh [--help|-h] [--quiet|-q] [--no-ping|-np]
[--full_ping|-fp]
```

Parameters:

`--help or -h:`

Displays this usage message.

`--quiet or -q:`

Quiet mode. Turns off progress and debug messages to stdout. This does not affect error messages which continue to be sent to stderr.

`--no-ping or -np:`

Disables the ping tests.

`--full-ping or -fp:`

Displays full ping test results instead of the default of a summary of the ping test results.

This script is a meta-script that will provide information on the current settings and status of a TN9400 system. This script will call the following scripts as part of information gathering process:

- `TN9400_IP_check.sh`
- `TN9400_package_check.sh`
- `TN9400_ntp_check.sh`
- `TN9400_ping_test.sh`

Note:
This script must be run as the root user. It will terminate with an exit code of 1 if any errors have been found.

TN9400 IP Check

The TN9400 IP check script checks the status of the IP network settings. It performs the following in the process:

- Scans active ethernet ports and display the ports' IP address details.
- Checks to see if the IP address of the active ethernet port is in the `/etc/hosts` file and displays any found entries.
- Checks each active ethernet port to see if it is using factory default IP addresses. If so, an error message is sent to stderr.
- Checks each active ethernet port to see if the link is up. If not, an error message is sent to stderr.

Script Usage

Usage:

```
TN9400_IP_check.sh [--help|-h] [--quiet|-q]
```

Parameters:

`--help or -h:`

Displays this usage message.

`--quiet or -q:`

Quiet mode. Turns off progress and debug messages to stdout. This does not affect error messages which continue to be sent to stderr.

This script will check the status of the IP network settings. It will perform the following in the process:

- Scans active ethernet ports and display the port's IP address details.
- Checks to see if the IP address of the active ethernet port is in the /etc/hosts file and displays any found entries.
- Checks each active ethernet port to see if it is using factory default IP addresses. If so, an error message is sent to stderr.
- Checks each active ethernet port to see if the link is up. If not, an error message is sent to stderr.

TN9400 NTP Check

This script will check the status of the NTP client. It will perform the following in the process:

- Displays the NTP server IP address.
- Checks the stratum, offset, reach and drift values and compares them against Tait recommended limits.

Script Usage

Usage:

```
TN9400_ntp_check.sh [--help|-h] [--quiet|-q]
```

Parameters:

`--help or -h:`

Displays this usage message.

`--quiet or -q:`

Quiet mode. Turns off progress and debug messages to stdout. This does not affect error messages which continue to be sent to stderr.

This script will check the status of the NTP client. It will perform the following in the process:

- Display the NTP server IP address.
- Check the stratum, offset, reach and drift values and compare them against Tait recommended limits.

Note:
This script must be run as the root user. It will terminate with an exit code of 1 if any errors have been found.

TN9400 Package Check

This script will check the status of TN9400 packages. It will perform the following in the process:

- Displays package names and version numbers.
- Displays version numbers as reported from service binary files.
- Displays version numbers from log files.
- Displays version numbers from Web UI applications.
- Compares version numbers and reports errors where there are discrepancies in the version numbers.

Script Usage

Usage:

```
TN9400_package_check.sh [--help|-h] [--quiet|-q]
```

Parameters:

`--help or -h:`

Displays this usage message.

`--quiet or -q:`

Quiet mode. Turns off progress and debug messages to stdout. This does not affect error messages which continue to be sent to stderr.

This script will check the status of TN9400 packages. It will perform the following in the process:

- Display package names and version numbers.
- Display version numbers as reported from service binary files.
- Display version numbers from log files.
- Display version numbers from Web UI applications.
- Compare version numbers and report errors where there are discrepancies in the version numbers.

Note:
This script must be run as the root user. It will terminate with an exit code of 1 if any errors have been found.

TN9400 Ping Test

This script will ping IP addresses from TN9400 configuration files for the checking of connectivity to the various controllers in a TN9400 system.

Script Usage

Usage:

```
TN9400_ping_test.sh [--help|-h] [--quiet|-q] [--full-
ping|-fp]
```

Parameters:

`--help or -h:`

Displays this usage message.

`--quiet or -q:`

Quiet mode. Turns off progress and debug messages to stdout. This does not affect error messages which continue to be sent to stderr.

`--full-ping or -fp:`

Displays full ping test results instead of the default of a summary of the ping test results.

This script will ping IP addresses from TN9400 configuration files for the checking of connectivity to the various controllers in a TN9400 system.

Note:
This script must be run as the root user. It will terminate with an exit code of 1 if any errors have been found.

Tait Software License 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 Soft-

ware.
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.