

4.3.6 Troubleshooting





4.4 NMS INSTALLATION



Caution: Network security may be compromised when accessing external Internet connectivity. The use of established security software is recommended.

The NMS software is pre-installed on the Network Management Server and the NMS server arrives preinstalled in the optional Host Unit cabinet. This section provides instruction for installing the NMS software on a customer laptop or desktop and setting initial software parameters.



Figure 4-26. NMS Server

4.4.1 Installation Overview

The installation of the Network Management System consists of the following steps:

	Table	
Step	Operation Type	Operation Action
1	SYSTEM SET-UP	VERIFY SERVER SOFTWARE IS OPERATIONAL
2	SYSTEM SET-UP	INSTALL SYSTEM SOFTWARE ON TO CUSTOMER MONITORING EQUIPMENT
3	SYSTEM SET-UP	LAUNCH NMS SOFTWARE
4	CONFIGURE	CONFIGURE MANAGER ACCOUNT
5	CONFIGURE	SET-UP USER ACCOUNTS
6	CONFIGURE	SOFTWARE SYSTEM PARAMETERS
7	UPDATE/UPGRADE	SOFTWARE/FIRMWARE UPGRADE INSTALL
8	INITIAL SOFTWARE INSTALLATION REVIEW	CONFIRM SOFTWARE SET-UP INSTALLATION, TABLE 4-13 NMS INITIAL SOFTWARE INSTALLATION CHECKLIST
9	UPGRADE INSTALLATION REVIEW	CONFIRM FIRMWARE UPDATE AND SOFTWARE UPGRADE INSTALLATION, TABLE 4-14 NMS UPGRADE SOFTWARE INSTALLATION CHECKLIST
10	TROUBLESHOOTING	INSTALLATION TROUBLESHOOTING GUIDE

Table 4-11. NMS Installation Overview

4.4.2 Installation Hardware and Tools

The NMS server is shipped pre-installed in the optional Host Unit cabinet. **Table 4-12** lists the accessories provided by the manufacturer. Additional accessories may be needed, depending on the site requirements, and may be ordered through Customer Service (Section 6).

NMS ACCESSORY	Quantity	Received
SOFTWARE CD-ROM	1	

Table 4-12. NMS Cables and Accessories



NMS ACCESSORY	Quantity	Received
AC POWER CABLE	1	

The following is a list of tools and any additional materials required for NMS software installation:

- Laptop, Desktop PC and/or Terminal
- Crossover Cable
- Hub and/or Router

4.4.3 Unpacking And Inspection

This section provides the instructions for receiving the equipment shipment and verifying that no damage has occurred during shipping. The NMS software is pre-installed on the server which is shipped with the following:

- Optional cabinet with NMS server and Host Unit installed as shown in Figure 4-27.
- Installation cables and accessories as described in **Table 4-12**, **Section 4.4.2**.

Use the following procedure to unpack and inspect the NMS server and accessories:

- 1. Open the shipping packet and carefully unpack the cabinet from the protective packing material.
- 2. Verify receipt of accessories using Table 4-12
- 3. Check the server for visual damage. If there is any damage, contact BTI (Section 6) for further instructions including an RMA, if necessary.



Figure 4-27. NMS Server

4.4.4 Verify Server software



1. Connect the laptop, PC or terminal to the server through the hub using a crossover cable, **Figure 4-28**. The monitoring device may also be plugged directly into the server with a crossover cable.



Figure 4-28. Connecting the Monitoring Device to the Server

2. Locate the NMS icon on the screen of the monitoring device, Figure 4-29.



Figure 4-29. Locate NMS Icon

4.4.5 Initial System Setup

4.4.5.1 CD-ROM Install

The CD-ROM install is used to install NMS on to a Laptop or Desktop Computer. Use the following procedure to install the application on to the computer:

- 1. Open the CD drive on the machine.
- 2. Place the CD into the drive and close the drive.
- 3. The CD will begin the install wizard, Figure 4-30.
- 4. The wizard copies the files to the %ProgramFiles% folder. The default destination directory may be changed, if desired.



Choose	
Install to Hard Disk	C Run
Destination Directory:	
:\Program Files\	

Figure 4-30. DAS Setup Wizard

4.4.5.2 Launch NMS

- 1. After copying the files, the Wizard will ask to launch NMS, **Figure 4-31**.
- 2. Select Yes.
- 3. The Wizard simultaneously places a shortcut on to the desktop of the computer as shown in Figure 4-

Cho Pie	ase C	onfirm				×
Destir C:\Pro	?	Install	Finished	Launch [AS NMS?	
			Y	es	No	

32. Double clicking on the NMS icon on the desktop also launches the NMS Login screen.

Figure 4-31. NMS Launch from Wizard Installation





Figure 4-32. NMS Desktop Shortcut



NOTE: Occasionally, there are compatibility problems that cause a configuration conflict when setting up the NMS. Follow the steps shown in the Troubleshooting Guide. If this does not resolve the issue, contact Customer Service (Section 6).

- 4. Verify that the *Advance* box is checked and then click in the password field, **Figure 4-33**.
- 5. Enter the following default password: 1
- 6. Click on OK. The NMS Command Console is then launched.

- Login	
User :	Manager 💌
Password :	
Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø	Advance

Figure 4-33. NMS Login Screen

4.4.6 Initial Start-up Configuration

Once NMS is installed on the machine, the command console or main screen is used to navigate through various NMS menus to configure both the software system parameters and the DAS system parameters. This section covers the software system parameters needed to set-up an initial install.

Main access to the NMS software configuration is through the *System(S)* drop down on the Menu bar as shown in **Figure 4-34**. User accounts may also be accessed through the User Icon on the Command toolbar as shown in **Figure 4-35**. The software system configuration includes the ability to access the



following functions:

- Access and manage User Accounts and passwords (Add/Modify/Delete)
- Modify parameter defaults.

NMS Software V2.6	5.1.6	-	- and the second					
System(S)		99(L)	Help(H)					
System Parameter User Manager	Alarm	Log	Help	Exit				
Eet	Sie_Site		Alarm Status Selected	Config Sampi	ing]		Current Value	
			☐ Selec	t All	✓ Select	😹 Cancel	Del Read	
NMS Software V2.6.1.6	User: I	Manager	Network	128.0.0.15.81	92 Monitor Real-1	ime.No	Information	aravo Tech Inc

Figure 4-34. System (S) Drop Down Menu



NMS Software V2.6.1.6			
User NetConfig Alarm Log	Help Exit		
	Alarm Status Config Sampling	Current Value	1
NMS Software V2.6.1.5 User: Manager	C Select All ✓ Select Network 128.0.0.15.8192 Montor Real-	Cancel Cri Read	Intro Tech Inc

Figure 4-35. User Account Icon

4.4.6.1 Modify Default Accounts

The NMS User Manager comes with two default entries shown in the User list. For security reasons, changing the default manager account and password is highly recommended. The default User account may also be modified by overwriting the default information. The following procedure details the steps necessary to change the default accounts:

1. Using either the System(S), Figure 4-34 or the User icon, Figure 4-35, access the User Manager screen, Figure 4-36.



🖉 User Manager	×
User List	User Infomation
User	Login :
	Password :
	Type :
	Add 💽 Modify
	🗶 Delete 🔊 Return

Figure 4-36. User Manager Screen

2. Select Manager in the User List, Figure 4-37 to see the default information.



🖇 User Manager	×
User List Manager User	User Infomation User : Manager Password : 1
	Level : Supervisor
	X Delete S⇒ Return

Figure 4-37. Manager Default Information

3. Delete the default entries, Figure 4-38 and enter the new user name and password.



Note: There is a limit of 20 Alpha-Numeric characters for both User name and password entries. User names are selectable from the Login screen drop down menu, once entered into the system. Passwords are case sensitive.



🏂 User Manager	×
User List Manager User	User Infomation User : Mana
	Password : 1
	Add Add Add Carlot Modify Carlot Add Carlot Add

Figure 4-38. Edit Default Entries

- 4. Click *Modify* to update the User and Password.
- 5. Click *Return* to return to the NMS Command Console or continue to add or update User Accounts.

4.4.6.2 Set-up New User Accounts

Adding a New User is easily managed through the User Manager screen. Access the User Manager screen, then use the following procedure to add Users of various levels:

- 1. Currently, there are two levels available for User Accounts. Once the User Manager screen is up, select the User level, as shown in **Figure 4-39**.
 - **Supervisor**: This level acts as an administrator for the Network System. This level can make edits and set custom features.
 - **Observer**: This level is a monitoring functionality only. This level is most commonly used for users who will monitor the system and review alarm logs. At the Observer level, a user may only: modify their user name and password and; view, save and print Alarm information.





lear Liet	- User Infomation	
Manager		
User	User :	
	Password :	
	Level :	Observer 💌
		Supervisor
	Add	🛃 Modify
	X Delete	Return

Figure 4-39. Select a User Level

2. Enter a user name and password, Figure 4-40. Then click Add.



User Infomation
User
Password Type Password
Level : Observer
Add C Modify
X Delete Return

Figure 4-40. Enter User name and Password



Note: There is a limit of 20 Alpha-Numeric characters for both User name and password entries. User names are selectable from the Login screen drop down menu, once entered into the system. Passwords are case sensitive.

3. Additional detailed information for managing User accounts, including deleting and modifying User accounts is contained in the NMS User Manual.

4.4.6.3 Configure Software Parameters

The NMS system software parameter defaults allow the user to focus less on configuring the software system, **Figure 4-41**, and more on the critical functionality for the DAS system.

Detailed parameter information is available in the NMS User Manual.



🏭 System Parameter	
Parameter List Monitor Time	Parameter Information
SNMP Connecting Mode	Monitor Real-Time: No
	Apply Dr Return

Figure 4-41. System Parameter Screen

4.4.7 Firmware Update

DAS components periodically require firmware updates. The following list of components may require periodic firmware updates:

- BIU
- FIU
- PA
- RCU
- Remote Unit

A notification email is sent with the firmware update attached as a file to the email. The following procedures detail the firmware update process:

1. Verify the email is genuine and the file attachment is safe for download. The sent file will be named in the following manner and have a file extension of .s:

DAS8345_[Component]_[Version].s

2. Download the attached file to any chosen folder or the desktop. Note the folder name, if saved to a designated folder.



- 3. Log into the NMS System.
- 4. Click on NetConfig
- 5. Using the *RemoteSoftwareDownload* interface, **Figure 4-42**, Locate the file by clicking on the browse button.

/stem Net ⊕	Add/Remove Remot	eSoftwareDownload Current Version	1	Browse
	File Length: Package:	Vers Retry	ion: Status	

Figure 4-42. Remote Software Download Screen

- 6. Click Start Download. The firmware update may be paused if needed by clicking the Pause button.
- 7. Once the download is complete, click *Return*.

4.4.8 Software Upgrade Installation

4.4.8.1 CD-ROM Install

The CD-ROM Upgrade install is a quick and simple installation. Use the following procedure to install the application on to the computer:

- 1. Check that no instance of NMS is running.
- 2. Open the CD drive on the machine.
- 3. Place the CD into the drive and close the drive.
- 4. The CD will begin the install wizard and ask if the user would like to overwrite the older NMS version, Figure 4-43.



5. Select Yes.

Please (Confirm		×
?	DAS NMS alrea	dy exists, Overwr	te Database?
	Yes	No	Cancel

Figure 4-43. Replace NMS File

- 5. An error dialog box will appear, **Figure 4-44**, if the older version of NMS is open and running.
- 6. Close NMS and click Try Again.

File In U	se		×
	The action can't be con Close the file and try ag	npleted because the file is open in another program Jain.	
	2	NMS_TestN File version: 2.5.2.1 Date created: 7/22/2011 3:54 PM Size: 2.25 MB	
	Do this for all curren	Try Again Skip Cancel	

Figure 4-44. NMS Update Fail Error Box

4.4.9 NMS Upgrade Installation Review



Table 4-13. NMS Initial Installation Checklist

Items	Description
1	Verify that the CD is undamaged and the server software is installed.
2	Confirm that the version number once the set-up Wizard launches NMS.
3	Verify that the shortcut launches the NMS Login.
4	Check that the default Manager Account and password have been updated.
5	Confirm that new User accounts and passwords have been added.

Table 4-14. NMS Firmware Update and Software Upgrade Checklist

Items	Description
1	Verify that the email and attachment. are genuine.
2	Confirm that the firmware update is downloaded to the appropriate folder on the computer.
3	Verify that firmware update was complete from the RemoteSoftwareDownload interface.
4	Confirm that no instance of NMS is running before beginning Upgrade installation.
5	Check the version number to verify upgrade once the set-up Wizard has launched NMS.



4.4.10 Troubleshooting



5 mBSC DAS SYSTEM START-UP

When the system component installations are complete, the system must be configured. Please refer to the applicable System Operation and User Manual for detailed system configurations, operations, and troubleshooting/test procedures

5.1 SYSTEM COMMUNICATION

Once the components have been installed, the system should be activated by establishing communication through the Host Unit and configuring the system to the network through the NMS.

5.1.1 Establishing a Host Unit communication

The Host Unit hardware default IP address must be updated with the customer's network IP address. This is accomplished by first establishing a communication link, setting up the initial base system and configuring the IP Address parameter. Use the following procedure to establish communication with the Host Unit :

- 1. Connect the NMS installed Laptop ethernet port to the RCU front ethernet port with a cross or null modem cable.
- 2. From the Laptop, click the Start Button, then Settings and Network Connections, Figure 5-1.

Figure 5-1. Open Network Connections

3. Select the LAN Icon and click on *File* then *Properties*, **Figure 5-2**.

Sharing Using: Using: Using: Corrigu Inection uses the following items: Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Realtke RilProt WLAN Utility Protocol Driver Internet Protocol Version 6 (TCP/IPv6) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder Unik-Layer Topology Re	cal Area Connection Properties	elp
using: ealtek Configu nection uses the following items: Client for Microsoft Networks GOS Packet Scheduler File and Printer Sharing for Microsoft Networks Realtke RtProt WLAN Utility Protocol Driver Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 6 (TCP/IPv6) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder stall Uninstall Properti ption s your computer to access resources on a Microsoft rick.	working Sharing	
Configu nection uses the following items: Client for Microsoft Networks GoS Packet Scheduler File and Printer Sharing for Microsoft Networks Realtke RiProt WLAN Utilty Protocol Driver Internet Protocol Version 6 (TCP//Pv6) Internet Protocol Version 6 (TCP//Pv6) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder istall	nnect using:	
Configu nection uses the following items: Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Realtke RilProt WLAN Utilty Protocol Driver Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 7 (TCP/IPv6) Internet Protoc	Realtek ·	
Conigu nection uses the following items: Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Realtke RilProt WLAN Utilty Protocol Driver Intermet Protocol Version 6 (TCP/IPv6) Intermet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 7 (TCP/IPv6) Internet Protoco		Configure
Client for Microsoft Networks GloS Packet Scheduler File and Printer Sharing for Microsoft Networks Realtke RiProt WLAN Utilty Protocol Driver Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder istall Uninstall Properti ption s your computer to access resources on a Microsoft rk.	is connection uses the following items	Coninguio
Quicari for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Realtke RiProt WLAN Utility Protocol Driver Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 6 (TCP/IPv6) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder istall Uninstall ption syour computer to access resources on a Microsoft rik.	s connection uses the rollowing items	•C:
Jubs Fracket Scheduler File and Printer Sharing for Microsoft Networks Realtke RtIProt WLAN Utility Protocol Driver Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 6 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder Istall Uninstall Propertion syour computer to access resources on a Microsoft rick.	Client for Microsoft Networks	
International Control South Resolution (CPU) (CP	Gos Facket Scheduler Ele and Printer Sharing for Mar	man Maturada
Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder Install	Realtice BtiProt WI AN Litity Pr	rotocol Driver
Internet Protocol Version 4 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder istall Uninstall Properti ption s your computer to access resources on a Microsoft rfk.	Internet Protocol Version 6 (TC)	P/1Pv6)
Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder Istall Uninstall Properti ption s your computer to access resources on a Microsoft rik.	Internet Protocol Version 4 (TC)	P/IPv4)
Link-Layer Topology Discovery Responder Istall Uninstall Property ption s your computer to access resources on a Microsoft rk.	Link-Layer Topology Discovery	Mapper I/O Driver
InstallUninstall Properti ption s your computer to access resources on a Microsoft vfk.	Link-Layer Topology Discovery	Responder
ption s your computer to access resources on a Microsoft rk.	Install Uninstall	Properties
s your computer to access resources on a Microsoft ork.	Description	
nk.	Allows your computer to access resou	irces on a Microsoft
	network.	

Figure 5-2. LAN Properties

4. Click on Internet Version Protocol (TCP/IPv4) and then click on Properties, Figure 5-3.

Figure 5-3. Select Internet Protocol Version 4

5. Click on the second option, *Use the Following IP Address:*, **Figure 5-4**, and manually enter the IP Address: 128.0.2.30. The Subnet mask will automatically default to 255.255.0.0.

Network	rk Connections	
00	Control Panel + Network Connections	
File Edit	t View Tools Advanced Help	
Loc.	cal Area Connection Properties	ectio
Na Netwo	rorking Sharing)evic
a -	nternet Protocol Version 4 (TCP/IPv4) Properties	
	General	
r]	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	
	Obtain an IP address automatically	
	• Use the following IP address:	
	IP address: 128.0.2.30	
	Subnet mask: 255 . 255 . 0 . 0	
	Default gateway:	
-	O Obtain DNS server address automatically	
	Use the following DNS server addresses:	
	Preferred DNS server:	
L.	Alternate DNS server:	
	Advanced	
	OK Cancel	

Figure 5-4. Manually Enter the IP Address

6. Click OK.

5.2 INITIAL NETWORK CONFIGURATION

This section details the initial functions necessary for a basic system activation through the NMS. Access to the DAS system configuration is through the *Network(N)* menu bar drop-down or the Net Config Command bar button, **Figure 5-5**. The DAS *Network(N)* drop-down includes the ability to access the following functions:

- Add/Modify/Delete Sites
- Add/Modify/Delete the Host Unit(s)
- Add/Modify/Delete the Remote Unit(s)

NMS S	oftware V2.6.1.6							
System(S)	Network:(N)	<u>.</u>	leip(H)					
User	NetConfig A	arm Log	O Help	Exit				
	et ETT_Exomple		Alarm Status Selected	Config Sampling Item	Select	<u>te</u> Cancel	Current Value	
NMS Softw	are V2.5.1.5	User: Manager	Network	128.0.0.15.8192	Monitor Real-Time	No	Infomation	Iravo Tech Inc

Figure 5-5. Accessing the Network Configuration screen

The NMS software provides an example configuration as shown in **Figures 5-5** and 5-6. The example may be deleted or the example information may be overwritten with customer specific information and then saved by clicking the **Modify** button. For the purposes of this installation manual, the example has been deleted to provide the most accurate details.

Figure 5-6. BTI Example System Configuration

5.2.1 Add a Site

The highest level of system configuration is defined by adding a Site Caption and a Site Code. The alphanumeric text fields accept any user-defined descriptive name (30 alpha-numeric character limit) and site code (1 through 9999 numeric limit). The following steps are used to add the Site Caption and Site code:

- 1. Access the *Network Config* screen, **Figure 5-5**, via the NetConfig Command bar button or the *Network(N)* menu drop-down.
- 2. Click on the Site button in the Select Information field, Figure 5-7.
- 3. Enter the Site name and the Site code. The example, BTI_Example_Cypress_Site is shown in **Figure 5-8**.
- 4. Click Add to save the Site Caption and Site Code.

mBSC DAS System Installation Manual Issue 3

stem Net	\	
	Add/Remove RemoteSoftwareDownload	
	Information	
	Select item	
	C Site C Equipment	
	Site Caption :	
	Site Code :	
		🖹 Add
		🏹 Modify
		Y Delete
		Delete
		De Return

Figure 5-7. Add a Site

mBSC DAS System Installation Manual Issue 3

twork Config	
twork Config	Add/Remove RemoteSoftwareDownload

Figure 5-8 Adding a Site

5.2.2 Add a Host Unit

Once the Site Caption and Site Code have been configured, the Host Unit should be added to the system. The alpha-numeric text fields accept any user-defined descriptive *HU Caption* (20 alpha-numeric character limit) and *HU No.* (1 through 9999 numeric limit). The following steps provide the Host Unit configuration:

- 1. Click on *Equipment* to bring up the new information section for the DAS System equipment.
- 2. Click on *HU* in the *Select Equipment* section. Verify that the Site Caption and Site Code are correct for the Host Unit being added.
- 3. Add the customer designated Host Unit Caption and Host Unit No. as shown in Figure 5-9.

BTI_EXAMPLE_CYPRESS_SITE	Add/Remove RemoteSoftwareDownload	
	Information	
	Select item	
	C Site Equipment	
	Site Caption : BTI_EXAMPLE_CYPRE	
	She Carlas 2	
	Site Code .	
	Select Equipment	
	C HU C RU equipped	Add
	HU Caption :	The same of the
	HU NO. :	Modily
	Slot: Fiber: Type:	
	Equipment Address : 0 Default	X Delete
	IP Address(HU): 128.0.2.28	-
	10 Det	
	1P Port : [8192	CP Return

Figure 5-9. Adding a Host Unit

4. Verify that all changes have been correctly entered and click Add, Figure 5-10.

n Net BTI_Example_Cypress_Site	Add/Remove RemoteSoftwareDownload
🗟 👼 HU_30	Information
	Select item
	C Site C Equipment
	Site Caption : BTI_Example_Cypress_
	Site Code : 2
	Select Equipment
	CRU CRU equipped
	HU Caption : HU_30
	Slot: Fiber: Type: 0 - RCU
	Equipment Address : 0
	IP Address(HU) : 128.0.2.28
	IP Port : 8192 IP Re

Figure 5-10. Configured Host Unit

5.2.3 Configuring the Host Unit Hardware Card

Once the Host Unit has been added to the system, the IP address for the Host Unit must be changed from the default to the designated network IP address in the Host Unit Hardware Card. Configuring the IP Address is done from the Main Command Screen. The following procedures outline the steps necessary to change the Host Unit IP Address:

- 1. From the Main Command Screen, Select the added HU.
- 2. Select the RCU Module, Figure 5-11.
- 3. Select Config.

Image: Selected Item Current Value Image: Selected Item Image: Selected Image: Selected	NUAS Software V2.6.1.6 (stem(5) Network(N) Alarm Manager(A) Log(L)	lb(H)	
NMS List 1 2 3 4 5 6 7 8 9 MU: HU_30 NU: B F I	ି କିଛି ୬ହି ା ା User NetConfig Alarm Log	elp Exit	
Selected Item Current Value Total Alarm Level Item RCU +5V Alarm Item POI Fan1 Alarm Item POI Fan2 Alarm Item Expanded Alarm Input 1 Item Expanded Alarm Input 2 Item Expanded Alarm Input 3 Item	NMS List BTLEXAMPLE_CYPRESS_S T	2 3 4 5 6 7 8 9 B F I I U U S Sampling MU: HU_30 RU: Time: 2011-07-13/14:16:04 m Status Config Sampling	8
Total Alarm Level RCU +5V Alarm RCU +9V Alarm POI Fan1 Alarm POI Fan2 Alarm Expanded Alarm Input 1 Expanded Alarm Input 2 Expanded Alarm Input 3	-	ielected Item	Current Value
RCU +5V Alarm RCU +9V Alarm POI Fan1 Alarm POI Fan2 Alarm Expanded Alarm Input 1 Expanded Alarm Input 2 Expanded Alarm Input 3		Total Alarm Level	
RCU +9V Alarm POI Fan1 Alarm POI Fan2 Alarm Expanded Alarm Input 1 Expanded Alarm Input 2 Expanded Alarm Input 3		RCU +5V Alarm	
POI Fan1 Alarm POI Fan2 Alarm Expanded Alarm Input 1 Expanded Alarm Input 2 Expanded Alarm Input 3		RCU +9V Alarm	
POI Fan2 Alarm Expanded Alarm Input 1 Expanded Alarm Input 2 Expanded Alarm Input 3		POI Fan1 Alarm	
Expanded Alarm Input 1 Expanded Alarm Input 2 Expanded Alarm Input 3		POI Fan2 Alarm	
Expanded Alarm Input 2 Expanded Alarm Input 3		Expanded Alarm Input 1	
Expanded Alarm Input 3		Expanded Alarm Input 2	
		Expanded Alarm Input 3	
Expanded Alarm Input 4		Expanded Alarm Input 4	
Cancel	 A (1) 	□ Select All Select	17 Read

Figure 5-11. Select the HU

- 4. Click on Parameter List. Then click Select All.
- 5. Click on *Read*, Figure 5-12.

m(5) Network(N) Alarm Mai	nager(A) Log(L)	Help(H)								Constant Providence
er NetConfig Alarm	Log	⊘ Help	Exit							
IS List	PRESS_S	1 2	3 4 B F I I U U	5	6 7 R U	8 0 0 0	9 P RU : 5 U Time: 201	J_30 11-07-13/14:43:26	Reading (Config: Success
Alarm Sta	Alarm Statu	s Config) Sam	ipling		1	In second		Parameter List	
		Selected	Item				Current Value	Edit V	lue	Edit Rule
		P	Device	Mode			DAS Remote C	tri Unit		
		11.	Device	S/N			BII-RC0-110310			
		1	Longitu	de			E103.12345678			Character ShortString
		1	Latitud	e			N103.12345678	•		Character ShortString
		1	Softwar	re Vers	ion		RCU_1.0.1.0_20	0110526		
		1	Site No	1.			00020002			Number , 0 <= X <= 1
		jÌ.	Device	No			0			Number , 0 <= X <= 2
		1	Monito	r centre	IP add	ress	128.0.0.20			128.0.0.15
		p)	Monitor	r centre	IP port		8192			Number , 0 <= X <= 8
		ji .	Site IP	addres	s		128.0.5.27			128.0.2.28
		jî.	Site IP	port			8192			Number , 0 <= X <= 6
			Site De	escriptio	on					Character ShortString
		Select		🖌 Se	lect	à	Cancel		>c>] Read	Set Set

Figure 5-12. View the Current Values

- 6. Confirm Select All is unchecked. Click on Site IP Address in the Parameter List.
- 7. Click Edit.
- 8. Enter the new IP Address in the Edit Value Column, **Figure 5-13**.
- 9. Click Set, Figure 5-14.

	a martin		1						
er NetConfig Alarm Log	Help	Exit							
S List	1 2 Alarm Statu	3 4 B F I U U S Conf	5 ig Sa	6 mplin	7 RCU	8 0.00	9 MU : HU_30 RU : U Time: 2011-07-13/	14:48:39	
									Parameter List
Set	Selected	Item					Current Value	Edit Value	Edit Rule
		Device	Mode)			DAS Remote Ctrl Unit		1
		Device	SIN				BTI-RCU-11031015		
		Longit	ude				E103.12345678 '		Character ShortString
		Latitude					N103.12345678 '		Character ShortString
		Softwa	are Ve	rsion			RCU_1.0.1.0_20110526		
	Site No.						00020002		Number , 0 <= X <= 4
							0		Number , 0 <= X <= 2
		Monito	or cent	re IP	addre	55	128.0.0.20		128.0.0.15
		Monito	or cent	re IP	P port 8192	8192		Number , 0 <= X <= E	
	ji .	Site IF	addr				128.0.5.27	128.0.5.30	128.0.2.28
		Site IF	port o				8192		Number , 0 <= X <= 6
	<	Site D	escrip	tion					Character ShortString
	☐ Select	All	√ 5	Select		2	Can Edi	t Read	Set

Figure 5-13. Enter the New IP Address

x NMS Software V2.6.1.6 ystem(5) Network(N) Alarm Manager(A) Log0	.) Heb(H)					
San	⊘ Help	Exit				
MMS_List BT_EXAMPLE_CYPRESS_S B- & HU_30		3 4 5 B F I U U	6 7 8 R P C U U	9 MU : HU_30 RU : U Time: 2011-07-13/1	4.49.24	Config: Success
	Autor Statu	s cound los	surburg [Parameter List
	Selected	Item		Current Value	Edit Value	Edit Rule
	-	Device Mod	e	DAS Remote Ctrl Unit		
		Device S/N		BTI-RCU-11031015		
		Longitude		E103.12345678 '		Character ShortString
		Latitude		N103.12345678 1		Character ShortString
		Software Ve	rsion	RCU_1.0.1.0_20110526		
		Site No.		00020002		Number , 0 <= X <= 2
		Device No.		0		Number , 0 <= X <= 2
		Monitor cent	tre IP address	128.0.0.20		128.0.0.15
		Monitor cent	tre IP port	8192		Number , 0 <= X <= 8
		Site IP addr	ess	128.0.5.30		128.0.2.28
		Site IP port		8192	1	Number , 0 <= X <= 6
	<	Site Descrip	tion			Character ShortString
s	□ Select	All 🖌 S	Select	🚀 Cancel 🛃 Edit	rr] Read	Set]
Software V2.6.1.6 User: Manager	Network Srm	128.0.5.2	27:8192 M	onitor Real-Time:Pause	00020002:0 Success	kavo Tech

Figure 5-14. IP Address Update Setting

5.2.4 Map the IP Address to the NMS Software

- 1. Click the Netconfig button.
- 2. Select the Host Unit. Figure 5-15.
- 3. Change the *IP Address(HU)* from the default value to the designated network IP address. This will map the IP Address in the NMS System to the HU hardware card.
- 4. Then Click Modify. Click Return
- 5. Restart NMS to set the new parameters.

RTI Example Site	Add/Remove RemoteSoftwareDownload
⊕ ⊕ HU_30	Information Select item C Site C Equipment
	Site Caption : BTI_Example_Site Site Code : 2
	Select Equipment
	HU Caption : HU_30 HU NO. : 1
	Slot: Fiber: Type: 0 - RCU Equipment Address : 0
L	IP Port : 8192

Figure 5-15. Modify IP Address(HU)

From the Main Command Screen:

- 1. Select the updated Host Unit.
- 2. Click on Parameter List. Then click Select All.
- 3. Click on *Read*, Figure 5-16.
- 4. Confirm that the HU Hardware Card IP Address matches.

NMS Software ¥2.6.1.6				
Rem(S) Network(N) Hiarm Hanager(H) Log(L	() Help(h)			
Ser NetConfig Alarm Log	Help Exit			
MS List 금- III EXAMPLE_CYPRESS_S 금- 중 HU_30 원 S4F2_RU650	1 2 3 4 5 6 7 8 B F I I 0 0 0 0 0 Alarm Status Config Sameline 1 0 0 0 0 0	9 MU: HU_30 RU: U Time: 2011-07-13/14:	Reading 51:07) Config: Success
	Seemi oraça a see a l'oanikinik l			Parameter List
	Selected Item	Current Value	Edit Value	Edit Rule 🙆
	Device Mode	DAS Remote Ctrl Unit		
	Device S/N	BTI-RCU-11031015		
	Longitude	E103.12345578 *		Character ShortString
	Latitude	N103.12345678 *		Character ShortString
	Software Version	RCU_1.0.1.0_20110526		
	Site No.	00020002		Number , 0 <= X <= 4
	Device No.	0		Number , 0 <= X <= 2
	Monitor centre IP address	128.0.0.20		128.0.0.15
	Monitor centre IP port	8192		Number , 0 <= X <= £
	Site IP address	128.0.5.30		128.0.2.28
	Site IP port	8192		Number , 0 <= X <= 6
	Site Description			Character ShortString
	□ Select All	Cancel 👸 Edit	P] Read	😫 Set
tware V2.6.1.6 User: Manager	Network Snmp 128.0.5.30:8192 Mor	itor Real-Time:Pause	00020002:0 Success	Iravo Te

Figure 5-16. Confirm IP Address Update Accepted.

5.2.5 Add a Master Remote

Once the Site Caption, Site Code, and Host Unit have been configured, the Master Remote Unit should be added to the system. The alpha-numeric text fields accept any user-defined descriptive R*U Caption* (20 alpha-numeric character limit) and R*U No.* (1 through 9999 numeric limit). The following steps provide the Remote Unit configuration:

- 1. Click on the new HU in the System Net section.
- 2. Click on Equipment to bring up the new information section for the DAS System equipment.
- 3. Click on *RU* in the Select Equipment section.
- 4. Select the Slot No. for the Master Remote Unit. (This is generally Slot 2).
- 5. Select the Fiber value.
- 6. Select the Type of Remote Unit.
- 7. NMS creates a default name based on the chosen slot, fiber and type values selected as shown in **Figure 5-17**. Modify the Remote Unit Caption with a customer designated name, if desired.
- 8. Verify that the Site Caption, Site Code and HU No. are correct for the Remote Unit being added
- 9. Click Add.

■ THU_30	 Add/Remove RemoteSoftwareDownload Information Select item Site © Equipment Site Caption : BTI_Example_Cypress_ Site Code : 2 Select Equipme RU RU equipped RU Caption : S2F1_RU1900 HU NO. : 1 Slot 2 Fiber: 1 Type: 2 - 1900 F Equipment Address : 66 IP Address(HU) : 128.0.2.30 IP Port : 8192 	C Add C Modify X Delete Return
----------	--	---

Figure 5-17 Adding Master Remote Unit

5.2.6 Add a Slave Remote

To complete the system activation, Slave Remote Units should be added to the system. The alphanumeric text fields accept any user-defined descriptive R*U Caption* (20 alpha-numeric character limit) and R*U No.* (1 through 9999 numeric limit). The following steps provide the Remote Unit configuration:

- 7. Click on the new HU in the System Net section.
- 8. Click on Equipment to bring up the new information section for the DAS System equipment.
- 9. Click on RU in the Select Equipment section.
- 10. Select the Slot No. for the Slave Remote Unit. (This should match the Master RU configuration).
- 11.Select the Fiber value.
- 12. Select the Type of Remote Unit.
- 13.NMS creates a default name based on the chosen slot, fiber and type values selected as shown in **Figure 5-18**. Modify the Remote Unit Caption with a customer designated name, if desired.
- 14. Verify that the Site Caption, Site Code and HU No. are correct for the Remote Unit being added.

15.Click Add.

罪 Network Config	×
System Net Add/Remove RemoteSoftwareDownload Information Select item Select item Site Equipment Site Code : 2 Select Equipment Select Equipment Information Select Equipment Site Code : 2 Select Equipment Select Equipment Information Select Equipment Site Code : 2 Select Equipment Select Equipment Site Code : 2 Select Equipment Select Equipment Site Code : 2 Select Equipment Select Equipment Site Code : 1 Site Caption : Select Equipment Site Caption : Select Equipment Site Caption : Select Equipment Address : Site Prot : B192	Add Carlot Modify Carlot Delete Return
S2E1_RU2100.2.1.67:128.0.2.30	

Figure 5-18. Adding a Slave Remote Unit

Table 5-2. Slots, Fiber and Type Values				
Name	Configuration Value			
Slot	Represents the slots on the HU from Left to Right that can be assigned to various equipment. Slots 1-6 are reserved for the FIU and BIU. Designating a slot number maps the RU to an FIU.			
Fiber	Maps the RU to the Fiber connection on the Host Unit to the associated FIU.			
Туре	Defines the frequency used and must match the RU type installed. There are currently four different types of Remote Units. 700 MHz, 850 MHz, 1900 MHz, and 2100 MHz.			

5.2.7 Connect Host Unit to Server

With the IP address updated, the Host Unit must be connected the server, **Figure 5-19**, for communication information to function. The Host Unit is connected from the Network port on the back interface through the hub to the server as shown in **Figure 5-20** or may be directly connected from the back interface port to the server. The Host Unit may also be connected to the server from the RCU network port on the front interface, either directly or through the hub to the server. Only one network port connection may be used at a time.

Figure 19. Connect Host Unit to Server

Only one port may be connected to the server at a time, as both front interface and back interface network ports are the same port.

Figure 5-20. HU Back Interface Network Connection

5.3 MANAGING AND MONITORING ALARMS

5.3.1 Alarm Manager

The NMS is also the means for managing and monitoring the DAS systems through the *Alarm Manager(A)* menu or the Alarm Icon on the Menu bar. The managing and monitoring of the DAS system is more completely detailed in the BTI NMS User Manual.

NMS Software V2.6.	1.6						
System(IC)	Nam Manager(A)	Log(L) Help(H)					
User NetConfig	Alarm L	og Help	Exit				
MS List							
		Alarm Status	Config Sampling	S.			
		Selected	ltem			Current Value	
		Г					
		F Selec	All	Select	# Cancel	tr] Read	
NMS Software V2.6.1.6	User: Mana	ger Network	128.0.0 15-8192	Monitor Real-Time No	irfo	mation	Iravo Tech inc

Figure 5-21. Alarm Manager

5.3.2 Configuring Standard Alarm Defaults

Configuring NMS is easily accomplished through the Custom Alarm tab, **Figure 5-21**. Select the alarm type and click the *Select* button for the appropriate category. **Table 5-3** provides a recommended list of alarms by category that may be selected to create a custom alarm configuration.

mBSC DAS System Installation Manual Issue 3

🕈 Alarm Manager			×
✓ Alarm Manager Active Alarm Cleared Alarm Query Alarm Cu Alarm List Slot1 FIU Fiber1 Light Rx alarm Slot1 FIU Fiber1 Light Rx alarm Slot1 FIU Fiber2 Light Rx alarm Slot1 FIU Fiber2 Light Rx alarm Slot2 FIU Fiber1 Light Tx alarm Slot3 FIU Fiber1 Light Rx alarm Slot3 FIU Fiber1 Light Rx alarm Slot3 FIU Fiber2 Light Rx alarm Slot3 FIU Fiber1 Light Rx alarm Slot3 FIU Fiber2 Light Rx alarm Slot4 FIU Fiber2 Light Rx alarm Slot4 FIU Fiber2 Light Rx alarm Slot5 FIU Fiber2 Light Rx alarm Slot5 FIU Fiber1 Light Rx alarm Slot5 FIU Fiber2 Light Rx alarm Slot6 FIU Fiber1 Light Rx alarm Slot6 FIU Fiber2 Light Rx alarm Slot6 FIU Fiber1 Light Rx alarm Slot6 FIU Fiber2 Light Rx alarm Sl	stom Alarm Select Delete Select	Critical Alarm mRU and sRU(LTE) communication Alarm mRU and sRU(AWS) communication Alar mRU and sRU(CELL) communication Alar mRU and sRU(PCS) communication Alar Downlink OverPower alarm Downlink VSWR alarm Downlink LoopFail Alarm Downlink LoopFail Alarm Downlink Over Voltace alarm Major Alarm RU Fan1 Alarm RU Fan2 Alarm RCU +5V Alarm RCU +5V Alarm POI Fan1 Alarm POI Fan1 Alarm RCU ver Voltace alarm POI Fan1 Alarm RCU ver Voltace alarm POI Fan1 Alarm POI Fan2 Alarm RCU No communication Alarm FIU No communication Alarm BIU No communication Alarm	
Slot5 FIU Fiber1 Light Rx alarm Slot5 FIU Fiber1 Light Tx alarm Slot5 FIU Fiber2 Light Tx alarm Slot5 FIU Fiber2 Light Tx alarm Slot6 FIU Fiber1 Light Tx alarm Slot6 FIU Fiber2 Light Tx alarm Slot6 FIU Fiber2 Light Tx alarm Slot6 FIU Fiber2 Light Tx alarm RCU No communication Alarm FIU No communication Alarm BIU No communication Alarm	Content Co	RCU +9V Alarm POI Fan1 Alarm POI Fan2 Alarm RCU No communication Alarm FIU No communication Alarm BIU No communication Alarm Winor Alarm Uplink Pilot Power Expanded Alarm Input 1 Expanded Alarm Input 2 Expanded Alarm Input 3 Expanded Alarm Input 4	

Figure 5-22. Configuring Custom Alarm Levels

Figure 5-23 shows an active alarm.

🕈 Alarm Manager	X
Active Alarm Cleared Alarm Query Alarm	
Active Alarm Cleared Alarm Query Alarm	First Index: Date Second Index: 7/18/2011 Alarm Total: 1 Alarm Total: Print Print Image: History

Figure 5-23. Active Alarm Screen

The **Table5-3** provides alarm indicator descriptions for the mBSC DAS system. Alarm types for the Host Unit and Remote Unit monitored by the NMS are included as well as optional components such as the POI. The recommended category for the alarm indicator is included in column 3 of the table along with the affected component. Critical alarms indicate system failures that disable the uplink or downlink operation. Other categories, such as Major, may indicate impaired performance, but not the catastrophic system failure or a specific RU node failure.

Alarm Indicator	Description	Category	Component
Downlink OverPower	Transmit Power exceeds rated output	Critical	PA
Downlink VSWR	Antenna system VSWR exceeds preset level	Critical	PA
Downlink OverVoltage	PA Power supply over voltage	Critical	PA
Downlink DeviceFail	Downlink system critical failure	Critical	PA
Downlink LoopFail	Downlink MCPA IM cancellation not functioning	Critical	Fiber Module PA
Downlink	MCPA is operating at an unsafe	Critical	Fiber Module PA

Alarm Indicator	Description	Catagory	Component
	temperature	Calegory	Component
	Di Liber DV feilure	Critical	Domoto Linit
Fiber Light RX			Remote Unit
	Iber Light Ix RU fiber TX failure		Remote Unit
mRU and sRU1(LTE) comm	Master to Slave communications failed	Critical	Remote Unit
mRU and sRU2(AWS) comm	Master to Slave communications failed	Critical	Remote Unit
mRU and sRU2(Cell) comm	Master to Slave communications failed	Critical	Remote Unit
mRU and sRU2(PCS) comm	Master to Slave communications failed	Critical	Remote Unit
RU Fan1	RU Fan failure	Major	Remote Unit
RU Fan2	RU Fan failure	Major	Remote Unit
LNA	RU Receive LNA failure	Critical	Remote Unit
RU/PA communication	RU Internal PA to CPU comm failure	Major	Remote Unit
Uplink Pilot Power	Uplink Pilot Power Failure	Minor	Remote Unit
RCU No Communication	NMS to RCU comm failure	Major	Host Unit
FIU No Communication	FIU to RCU comm failure	Major	Host Unit
BIU No Communication	BIU to RCU comm failure	Major	Host Unit
Fiber1 Light RX	FIU Fiber1 port RX light fail	Critical	Host Unit FIU
Fiber1 Light TX	FIU Fiber1 port TX light fail	Critical	Host Unit FIU
Fiber2 Light RX	FIU Fiber2 port RX light fail	Critical	Host Unit FIU
Fiber2 Light TX	FIU Fiber2 port TX light fail	Critical	Host Unit FIU
RCU +5V	Host Unit RCU power supply alarm	Major	Host Unit RCU
RCU +9V	Host Unit RCU power supply alarm	Major	Host Unit RCU
POI Fan1	POI Fan1 failure	Major	Host Unit POI
POI Fan2	POI Fan2 failure	Major	Host Unit POI
Expanded Alarm Input 1	Expansion	User Defined	Third Party Component
Expanded Alarm Input 2	Expansion	User Defined	Third Party Component
Expanded Alarm Input 3	Expansion	User Defined	Third Party Component

Alarm Indicator	Description	Category	Component
Expanded Alarm Input 4	Expansion	User Defined	Third Party Component

5.3.3 System Activation Review

Table	5-4.	System	Start-up	Review
-------	------	--------	----------	--------

Items	Description
1	Verify that the Host Unit communication was established.
2	Confirm that at least one Site has been added.
3	Verify that the Host Unit Hardware card IP address has been configured.
4	Check that the Remote Unit is communicating with the Host Unit
5	Confirm that the Host Unit is connected to the Server.

5.3.4 Troubleshooting

6 CUSTOMER SERVICE CONTACT INFORMATION

USA

BTI 6185 Phyllis Dr. Unit D. Cypress, CA 90630, USA Tel: +1 714-230-8333 Fax: +1 714-230-8341 E-mail: Customer Service: <u>CustomerService@bravotechinc.com</u> Sales: <u>sales@bravotechinc.com</u>

China

BTI (Shenzhen) Co., Ltd. No.8 Building, Zone #3, Tangtou Industrial Park, Shiyan, Baoan District, Shenzhen, Guangdong P.R.China 518102 Tel: +86 755-2951-2233 Fax: +86 755-2951-2299 E-mail: chinasales@bravotechinc.com This device complies with part 15 of the FCC Rules. Operation is subject to the

following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.

-- Increase the separation between the equipment and receiver.

-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 400cm between the radiator & your body.