# 13 Turn Up and Starting Initial Provisioning

## Introduction

The Mi7 can be turned up and provisioned with the Command Line Interface (CLI) and Transaction Language One (TL1). This chapter details the procedure for logging in to the Mi7 and changing to a secure password in CLI. It also begins the provisioning procedure with configuring the system number and configuring the IP address, both in TL1. Turn up and provisioning is then continued in "Chapter 14, Completing Initial Provisioning with TL1", and in "Chapter 15, Completing Initial Provisioning with Node Manager". After finishing the procedure described in this chapter, proceed to the chapter for the preferred interface.

## Toggling Between CLI and TL1

Once the initial login is done (see "Logging In" on page 97), it is possible to toggle between CLI and TL1. To get into TL1 from CLI, type `TL1` at the CLI prompt. To get into CLI from TL1, type `CLI;` at the TL1 prompt (`CLI` followed by a semicolon).

## TL1 Convention and Information

Following are select sections concerning TL1 syntax convention, and information that is pertinent in the turn up and initial provisioning process. See the *Mi7 TL1 Command Reference* for more information.

### The TL1 Prompt

The default TL1 prompt is `mahiMi7`. When a system identification (SID) is entered, the TL1 prompt changes to the newly provisioned SID. See "Configuring the System ID" on page 97. In the examples in this guide, all TL1 prompts are shown as `mahiMi7`.

# Command Structure

TL1 is not case sensitive. The TL1 command structure is:

`<Verb><-Modifier1>[-Modifier2]:`

- `Verb` defines the specific action to be performed
- `Modifier1` indicates the nature of the entity to be acted on.
- `Modifier2` can be used to further modify the entity.

# Key Descriptions

See Table 8 for key descriptions.

**Table 8** TL1 Key Descriptions

| Key | Description |
|---|---|
| < > | Mandatory field. Needs to be specified or filled |
| [ ] | Optional field. May or may not be specified |
| ; | TL1 message terminator |
| <SID> | Source ID. The name of the network element (Mi7) (as inputted) |
| <TID> | Target ID. The network element (Mi7's) name (as accessed) |
| <AID> | Access ID. Unique address of an entity within the network element |
| & | Operator for listing a group of specific AIDs |
| && | Operator for ranging a group of AIDs |
| <CTAG> | Correlation tag for individual input command message |
| ^ | Blank (space) |
| : | Colon. Used as a field separator in commands and responses |

# Aborting an Input Command

An input command can be aborted with the command ABT-CMD if the response message has not been generated. The input command cannot be aborted once the response message starts to generate, or a time-out message is sent for that input command.

# Response Message Time-Out

A time-out message is generated if the response message for an input command is not generated within one minute after the command is issued. An in progress (IP) code is generated every two seconds during the one-minute period, after which a repeat later (RL) message is generated with the input command.

## Context-Sensitive Help

Context-sensitive help can be invoked in two ways:

- Type help or ? on the command line to display all available TL1 commands.
- Type ? after an input command to display syntax information for that command.

  **EXAMPLE:** `mahiMi7>` RTRV-EQPT?

## TL1 Output

The following response identification gets returned (printed on the screen) for every non-retrieve command:

**mahiMi7><year><month><date> <hour><minute><second>**

**M CTAG1** <completion code>

**;**

**mahiMi7>**

Where **M^** (M followed by a space) indicates the message is a response to an input command message; **CTAG**, the correlation tag, is the same as that of the input command sequence; and the completion code is:

- **COMPLD** the input command was successfully executed
- **DENY** the input command execution was denied
- **PRTL** the partial input command execution was successful
- **RTRV** the retrieval was successfully executed

For retrieve commands, this response will include retrieved information in the line(s) between the completion code and the semicolon.

# Connecting the Craft Port Interface

The craft port interface may be connected only to the active NCC in the Primary Line Card Shelf (PLCS). The active NCC is indicated by the green LED (labeled ACT) on the faceplate. If the craft port interface is connected to the inactive NCC on the PLCS, or to an NCC on an Expansion Line Card Shelf (ELCS), the Mi7 will not respond.

The craft port interface is initially connected to the RS-232 connector (labeled *Craft Term*) on the faceplate of the NCC. The Ethernet connection (labeled *Craft ENet*) is active but may be used only after the local area network (LAN) is configured and the IP address is set. See "Configuring the IP Addresses" on page 98.

Required for this section:

- Serial cable ("straight through") with a female DB-9 connector on the end that is to be connected to the Mi7
- Craft computer with a terminal emulation software package installed

**Connect the craft computer to the craft port.**

1. Plug the serial cable into the serial port connector on the craft computer. The craft computer may be on or off.
2. Plug the other end of the serial cable into the RS-232 connector, labeled *Craft Term,* on the active NCC in the PLCS. See Figure 14.
3. Tighten the connector screws.

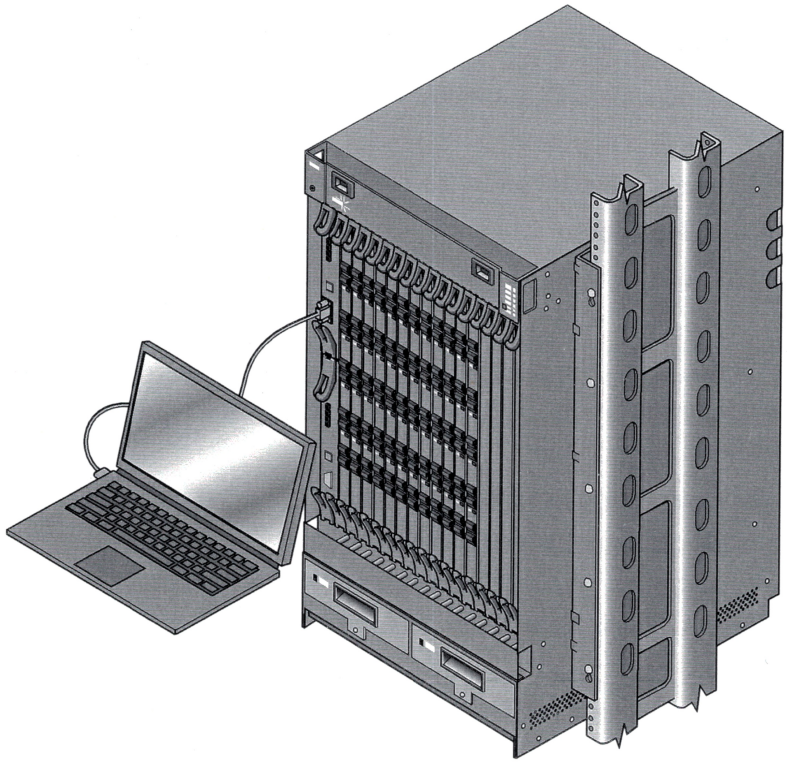

**Figure 14** Plug the Craft Interface Into the RS-232 Craft Terminal on the Active NCC

# Installing the Software

There is no need to load any software on the Mi7 at this time. The current software version (or a custom software configuration specified at the time of the order) has been factory-loaded on the network controller cards (NCC) which were installed in "Chapter 9, Installing the Cards".

System-wide upgrades and custom upgrades will be sent out on CD ROM, and instructions for installing new software is detailed in the *Mi7 CLI User Guide* and the *Mission7 User Guide*.

# System Administrator

The current factory-loaded software version includes one pre-provisioned user with system administrator rights. To add additional users, see "Chapter 14, Completing Initial Provisioning with TL1".

# Logging In

The login sequence detailed in this chapter is part of the turn up procedure, and is performed by the System Administrator. After the Mi7 is provisioned, a different login procedure is needed to access it, which is defined in the *Mi7 CLI User Guide* and the *Mi7 TL1 User Guide*.

### Log In

1. Press the enter key to get the login prompt.
2. Type the user name mahi and press return.

   **EXAMPLE:** `Login:` mahi
3. The Mi7 prompts for the default password:

   **EXAMPLE:** `password:`

   Type the default password, which is mahi.mi7, and press enter.

   **EXAMPLE:** `password:` mahi.mi7

# Configuring the System ID

Perform the following sequence to toggle to the TL1 prompt, and set the system identification (SID) code (which is the name of the network element).

### Toggle to the TL1 prompt.

4. Type `TL1` and press enter. The TL1 prompt appears.

### Set the system ID.

5. Check the installation order to find the SID designated for this network element. It is recommended the SID code be set to the Common Language Location Identifier (CLLI) code.
6. Use the following command to set the SID.

   `mahiMi7>` SET-SID:[TID]::[CTAG]:: <sid>;

   Where `TID` is the target ID (in this case, it is the default TID, MAHImi7), `CTAG` is the correlation tag, and sid is an alphanumeric string from 6 to 20 characters. The TL1 prompt changes to the newly provisioned SID, in all capital letters.

   See the *Mi7 TL1 Command Reference* for more information on the SET-SID command.

# Configuring the IP Addresses

Use the following command in TL1 to set the internet protocol (IP) address (IP service parameters) of the Mi7. This will enable the Ethernet management and craft ports to become active. Check the installation order to find the IP address designated for this network element.

`mahiMi7>` SET-IP:[TID]:<aid>:[CTAG]::[<ipaddr>][,<networkmask>];

Where TID is the target ID, and aid is the access identifier of NCCA or NCCB of the network element (valid values are 1-NCCA, 1-NCCB). CTAG is the correlation tag.

The fields with ipaddr (layer 3 IP address) and networkmask (network mask) each contain a string with a maximum of 15 characters in the format n.n.n.n. where n is a number between 0 and 255 decimal. Enter the strings with double quotes. Null defaults to 0.0.0.0.

See the *Mi7 TL1 Command Reference* for more information on the SET-IP command.

# Continuing Initial Provisioning

After completing the procedure described in this chapter, proceed to the chapter detailing the process for completing the initial provisioning on your preferred interface. This is either "Chapter 14, Completing Initial Provisioning with TL1", or "Chapter 15, Completing Initial Provisioning with Node Manager".

# 15 Completing Initial Provisioning with Node Manager

## Introduction

This chapter details the procedure for using the Web GUI to complete the initial provisioning that began in "Chapter 13, Turn Up and Starting Initial Provisioning". Procedures for changing the system configuration after initial turn up can be found in *Mission 7 Node Manager User Guide*.

## Connecting to the Mi7

Follow the procedure in this section to gain access to the Web GUI through your computer.

**Connect to the Mi7.**

1. Configure your computer to receive its IP address from a dynamic host configuration protocol (DHCP) server. The NCC has a DHCP server, and will assign the computer the IP address 192.168.1.2.
2. Enter the IP address 192.168.1.1 in your Web browser to connect to the Mi7. The Mi7 *Log In* screen opens.

## Logging in to the Mi7

Node Manager security is enforced by requiring the operator to log in. The Mi7 references user profiles during each login session. The login validates the operator's login and access privilege. The Mi7 maintains a list of user profiles, defining access privileges for each operator with a login account.

The *Log In* screen is the first screen a user sees when accessing a Mi7 through the Node Manager. It contains text boxes to input the following information:

- *User Name* - Operator's user name.
- *Password* - The operator password.

The *Log In* screen also has a *Light View* check box. The light view disables the alarm summary, face views, and real-time alarm view. Use the light view for faster screen loading when you are not using the alarm summary, face views, or real-time alarm view.

### Log in to the Mi7

1. Enter your user name in the *User Name* text box and your password in the *Password* text box. Your Mahi Networks representative will provide you with the initial user name/password combination. The user ID and password are case insensitive.
2. To load the light view, select the *Light View* check box.
3. Click *LOG IN*.

**NOTE:** You should create a new system administrator user for the Node Manager during your first Node Manager session. Create a user with in the group MNE with the role mneadmin. As soon as a user is defined with these resources, the default username/password combination is disabled. See "Adding the First User" on page 140 for information on how to create users.

# Configuring the Initial Mi7 System

After a successful login, the *Welcome* screen opens. Navigate to the *General System Configuration* screen to set initial system configuration. This screen must be completed to turn up the Mi7.

## Setting Initial Mi7 System Configuration

**FIND IT:** Provisioning >> System >> General

### Set initial system configuration settings

1. Click *EDIT*. The *Edit General System Configuration* screen opens.
2. Add or edit the following system configuration information:

- IP addresses for NCC-A and NCC-B. Use IPv4 format, Class A, B, or C.
- Subnet masks for NCC-A and NCC-B. Use a defined or configured subnet.
- Static Route - Prefix for NCC-A and NCC-B. Use a valid IP network address.
- Static Route - Mask for NCC-A and NCC-B. Use IPv4 format, Class A, B, or C.
- Static Route - Gateway for NCC-A and NCC-B. Use IPv4 format, Class A, B, or C.
- Host Name / System ID. Valid options are 1 to 20 alphanumeric characters, plus the hyphen ( - ). The node name is case sensitive. The first and last characters cannot be a hyphen.
- System Number. 1-254. (See note below.)
- Location. Alphanumeric text string.
- Contact. Alphanumeric text string.

3. To save the new configuration, click *SAVE*. To cancel the operation, click *CANCEL*.

**NOTE:** System numbers are arbitrary. They can range from 1-254, with one caveat. The system number is used internally for IP addresses, and thus dictates what addresses are accessible on the management ports. Basically any IP address "10.system.x.x" will not be accessible on the management interface. So if the management LAN is using 10.x.x.x addressing, the customer will need to set our system address so that the addresses do not conflict with this.

The following table shows the general system configuration elements and valid options:

**Table 60** General System Screen Elements

| Element | Description | Valid Options |
|---|---|---|
| IP Address - NCC-A | Active IP address | IPv4 format, Class A, B, or C |
| IP Address - NCC-B | Standby IP address | IPv4 format, Class A, B, or C |
| Subnet Mask - NCC-A | Active subnet mask | Defined or configured subnet |
| Subnet Mask - NCC-B | Standby subnet mask | Defined or configured subnet |
| Static Route - Prefix NCC-A | Active static route prefix | Valid IP network address |
| Static Route - Prefix NCC-B | Standby static route prefix | Valid IP network address |
| Static Route - Mask NCC-A | Active static route mask | Valid IP network address |
| Static Route - Mask NCC-B | Standby static route mask | Valid IP network address |
| Static Route - Gateway NCC-A | Active static route gateway | Valid IP network address |
| Static Route - Gateway NCC-B | Standby static route gateway | Valid IP network address |
| Host Name/SID | Name or system ID of node | 1 to 20 alphanumeric characters, plus the hyphen ( - ). The node name is case sensitive. The first and last characters cannot be a hyphen. |
| System No. | Number of system | 1-254 (see note below) |
| Location | Location of node | Alphanumeric text string |
| Contact | Node administrative contact | Alphanumeric text string |

# Setting Clock Information

Initial clock information for the Mi7 comes from the internal system clock on the Network Controller Card (NCC). The system clock is powered from the -48V office feed. The clock will maintain time for a very limited period without office power, and thus is fully discharged before the NCC is installed in the Mi7. Consequently, the system clock needs to be reset when the Mi7 is turned up for the first time.

## Editing Clock Parameters

Timing can come from either the system clock, or from a network timing source. When the timing source is *System Clock* the date and time can be edited. When the timing source is *NTP*, these fields are defined by the network timing source, and are not editable.

**FIND IT:** Provisioning >> System >> Clock

**Edit the system clock parameters**

1. Click *EDIT*. The *Edit System Clock* screen opens.
2. For system clock, edit date and time fields as needed. Format: hh:mm:ss.

   **NOTE:** System uses military (24 hour) time format.
3. Select time source radio button. Options are *System Clock* or *NTP*.
4. Click *SAVE* to apply the settings. Click *CANCEL* to cancel the operation.

The following table shows the attributes of the system clock:

**Table 61** System Clock Attributes

| Element | Description | Valid Entries |
|---|---|---|
| Date | Current date | Format: mm/dd/yyyy |
| Time | Current time | Format: hh:mm:ss<br>**Note**: System uses military (24 hour) time format |
| Time Zone | Displays the system time zone. The time zone cannot be edited from this screen. | EDT - Eastern Daylight Time<br>EST - Eastern Standard Time<br>CDT - Central Daylight Time<br>CST - Central Standard Time<br>PST - Pacific Standard Time<br>PDT- Pacific Daylight Time<br>MST - Mountain Standard Time<br>MDT- Mountain Daylight Time<br>GMT - Greenwich Mean Time |
| Time Source | Displays the timing source | System Clock or NTP |

**NOTE:** The Time Zone is not an editable field.

# Provisioning NTP

You can elect to receive timing from an outside network timing protocol (NTP) server instead of the Mi7 system clock. If NTP is selected as the timing source, it is not possible to edit the clock manually. You can enforce authentication of NTP timing sources through use of a specified authentication key. The Mi7 supports MD5 authentication.

**FIND IT:** Provisioning >> System >> NTP

### Provision NTP

1. Authentication can be set to either *ENABLE* or *DISABLE* through the button toggle. Click the button toggle to change the option if necessary. Once disabled, users cannot view or edit authentication keys.
2. To set authentication keys, click the *AUTHENTICATION KEYS* button. The *Authentication Keys* screen opens.
3. Click *CREATE*. The *Create Authentication Keys* screen opens.
4. Add the *Key* and *Value* information. The key is an integer from 1 through 2,147,483,647, the value is an arbitrary string up to eight characters.
5. To set this key as trusted, check the *Trusted* check box.
6. Click *CREATE* to create the authentication key. Click *CREATE & DUPLICATE* to create the authentication key, and open a new *Create Authentication Keys* screen with the same options preselected. Click *CANCEL* to cancel the operation.
7. To set NTP associations, click *ASSOCIATIONS*. The *NTP Associations* screen opens.
8. Click *CREATE*. The *Create Associations* screen opens.
9. Enter the IP address of the node to associate with. Use IPv4 format, Class A, B, or C.
10. Select *Peer* or *Server* from the drop-down list.
11. Select the NTP version number from the drop-down list. Options are 1 through 4.
12. If needed, enter the authentication key of the associated node. The key is an integer from 1 through 2,147,483,647. A key must be created before it is used in an association.
13. If this node is to be preferred over other nodes, click the *Preferred* check box. If not, clear this check box.
14. Click *CREATE* to create the association. Click *CREATE & DUPLICATE* to create the association, and open a new *Create Associations* screen with the same options preselected. Click *CANCEL* to cancel the operation.

The following table shows the NTP attributes:

**Table 62** NTP Provisioning Attributes

| Element | Description | Valid Entries |
|---|---|---|
| Authentication Key | Defines the authentication key used by NTP. If set, uses authentication key for synchronization. Disables peer and server information based on synchronization. | Integer from 1 through 2,147,483,647 |
| Value | For identification purposes | Arbitrary string up to 8 characters |
| Version No. | NTP version number | 1 through 4 |
| Peer | If set, system synchronizes with peer and vice versa. Disables authentication key and server information based synchronization. | Peer or Server |
| Server | If set, system synchronizes with NTP server. Disables authentication and peer information based synchronization. | Peer or Server |
| Trusted Key | Specifies trusted key used by authentication key based synchronization | Integer from 1 through 2,147,483,647 |
| Prefer | Defines the preferred peer | Boolean check box |

# Adding the First User

**FIND IT:** Administration >> Security >> Users

### Add the first user

1. Click *CREATE*. The *Create New User* screen opens.
2. Enter user ID. The ID must contain between 1 to 10 alphanumeric characters. The user ID is case insensitive.
3. Enter password. The password must contain between 8 - 10 alphanumeric characters, plus special characters ( ., +, -, #, %, (, ), *, [, ], {, }, @, !, <, >, ^, $, _ ). There must be at least one each alphabetic, numeric, and special character. The password is case insensitive, and cannot contain the user ID.
4. Re-enter the password.

   **NOTE:** Steps 5 through 11 are optional. If no entry is made, the default is used.
5. Select the time zone from the drop-down list. Valid options are Pacific-Time, Mountain-Time, Central-Time, Eastern-Time, Arizona, Hawaii, and GMT (Greenwich Mean Time).
6. Enter password expiration. Valid options are 1 through 999. Default is 45.
7. Enter user ID expiration. Valid options are 1 through 999. Default is 45.

8. Enter the number of passwords retained. Valid options are 1 through 10. Default is 5.
9. Enter password update times duration. Valid options are 1 through 999. Default is 7.
10. Enter password update duration. Valid options are 1 through 999. Default is 3.
11. Enter account update wait time. Valid options are 1 through 60 days. Default is 20.
12. Click *NEXT*. The *User Group* screen opens.
13. Select the group *MNE* from the radio buttons on the left, and click *NEXT*. The *User Roles* screen opens.
14. Select the role to *mneadmin*, and click *NEXT*. The *Information* screen opens with the group name and role or roles displayed.
15. Click *SAVE*.

# Resetting the System

You can reset the system at one of three levels:

- **L1 - APPLICATION RESTART** - The NCC will take down all Application Layer processes and threads and then restart them. First performed on the standby, active-standby switchover, then on the new standby.
- **L2 - NCC RESTART** - The standby is rebooted, active-standby switchover, the new standby is rebooted.
- **L3 - FULL SYSTEM RESTART** - The standby is rebooted, active-standby switchover, the new standby is rebooted. All provisioned cards are reset and restarted.

When resetting, a warning message opens, explaining that this operation will disconnect the browser from the Mi7, and the operator will need to re-login into the system.

**NOTE:** Resetting the system re-synchronizes alarms and the system clock (when the clock source is defined as NTP).

**FIND IT:** Provisioning >> System >> Reset

### Reset the system

1. Select initialization level from the drop-down list. Options are L1 (level 1), L2 (level 2), or L3 (level 3).
2. Click *RESET*. A confirmation screen opens. To cancel the operation, click *CANCEL*.
3. To rest the system, click *RESET*. To cancel the operation, click *CANCEL*.