Initial Configuration

This chapter describes the initial configuration of the ML-Series card and contains the following major sections:

Hardware Installation

This section lists hardware installation tasks, including booting up the ML-Series card. Because ONS 15454 SONET/SDH card slots can be preprovisioned for an ML-Series line card, the following physical operations can be performed before or after the provisioning of the slot has taken place.

1. Install the ML-Series card into the ONS 15454 SONET/SDH. See the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide* or the *Cisco ONS 15454 SDH Procedure Guide* for information.

2. Connect the cables to the front ports of the ML-Series card.

3. (Optional) Connect the console terminal to the ML-Series card.

Note   A NO-CONFIG condition is reported in the Cisco Transport Controller (CTC) under the Alarms tab when an ML-Series card is inserted and no valid Cisco IOS startup configuration file exists. Loading or creating this file clears the condition. See the "Startup Configuration File" section on page 5-7 for information on loading or creating the file.

Cisco IOS on the ML-Series Card

The Cisco IOS software image used by the ML-Series card is not permanently stored on the ML-Series card but in the flash memory of the TCC2/TCC2P card. During a hard reset, when a card is physically removed and reinserted or power is otherwise lost to the card, the Cisco IOS software image is downloaded from the flash memory of the TCC2/TCC2P to the memory cache of the ML-Series card. The cached image is then decompressed and initialized for use by the ML-Series card.

During a soft reset, when the ML-Series card is reset through CTC or the Cisco IOS command line interface (CLI) command **reload**, the ML-Series card checks its cache for a Cisco IOS image. If a valid and current Cisco IOS image exists, the ML-Series card decompresses and initializes the image. If the image does not exist, the ML-Series requests a new copy of the Cisco IOS image from the TCC2/TCC2P. Caching the Cisco IOS image provides a significant time savings when a warm reset is performed.

There are four ways to access the ML-Series card Cisco IOS configuration. The two out-of-band options are opening a Cisco IOS session on CTC and telnetting to the node IP address and slot number plus 2000. The two-in-band signalling options are telnetting to a configured management interface and directly connecting to the console port.

Opening a Cisco IOS Session Using CTC

Users can initiate a Cisco IOS CLI session for the ML-Series card using CTC. Click the **IOS** tab at the card-level CTC view, then click the **Open IOS Command Line Interface (CLI)** button (Figure 5-1). A window opens and a standard Cisco IOS CLI user EXEC command mode prompt appears.

Note   A Cisco IOS startup configuration file must be loaded and the ML-Series card must be installed and initialized prior to opening a Cisco IOS CLI session on CTC. See the "Startup Configuration File" section on page 5-7 for more information.

Figure 5-1   CTC IOS Window
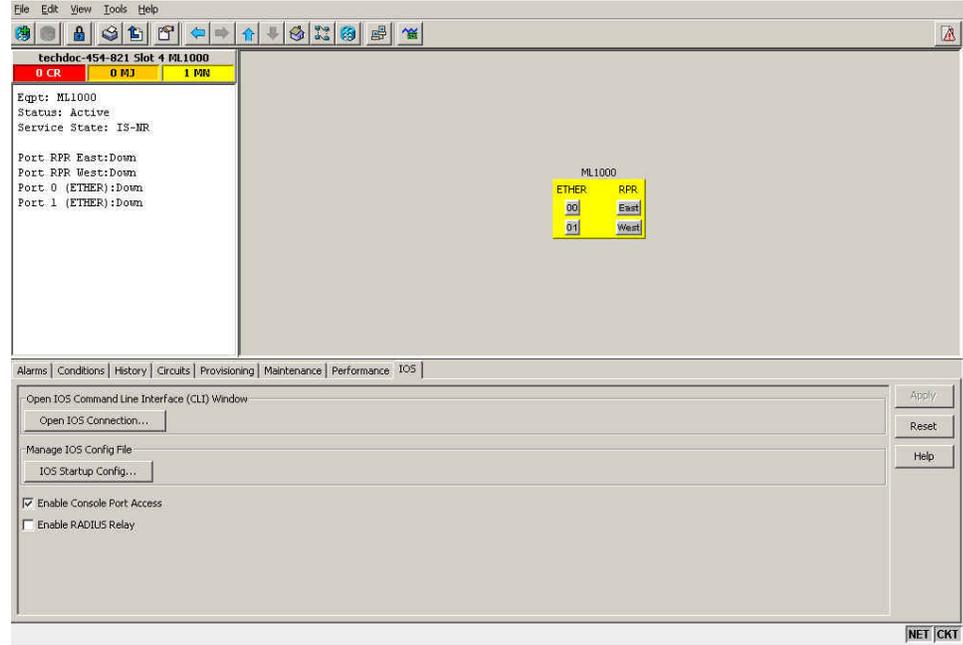
Telnetting to the Node IP Address and Slot Number

Users can telnet to the Cisco IOS CLI using the IP address and the slot number of the ONS 15454 SONET/SDH plus 2000.

> **Note**   A Cisco IOS startup configuration file must be loaded and the ML-Series card must be installed and initialized prior to telnetting to the IP address and slot number plus 2000. See the "Startup Configuration File" section on page 5-7 for more information.

> **Note**   If the ONS 15454 SONET/SDH node is set up as a proxy server, where one ONS 15454 SONET/SDH node in the ring acts as a gateway network element (GNE) for the other nodes in the ring, telnetting over the GNE firewall to the IP address and slot number of a non-GNE or end network element (ENE) requires the user's Telnet client to be SOCKS v5 aware (RFC 1928). Configure the Telnet client to recognize the GNE as the Socks v5 proxy for the Telnet session and to recognize the ENE as the host.

Step 1   Obtain the node IP address from the LCD on the front of the physical ONS 15454 SONET/SDH or the IP Addr field shown at the CTC node view (Figure 5-2).

Step 2   Identify the slot number containing the targeted ML-Series card from either the physical ONS 15454 SONET/SDH or the CTC node view (Figure 5-2). For example, Slot 13.

Figure 5-2   CTC Node View Showing IP Address and Slot Number
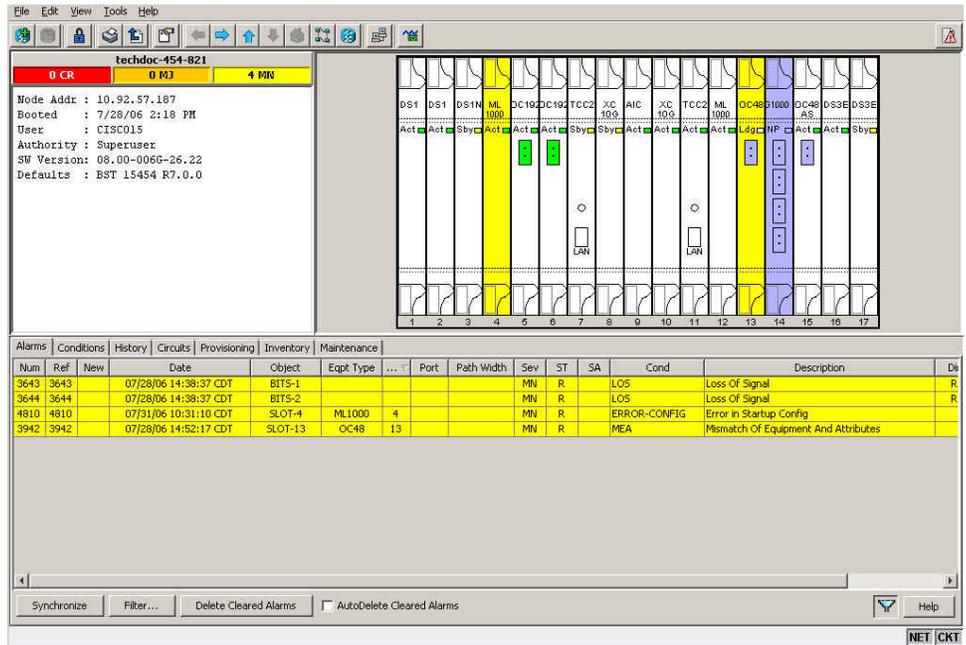
Step 3   Use the IP address and the total of the slot number plus 2000 as the Telnet address in your preferred communication program. For example, for an IP address of 10.92.57.187 and Slot 13, you would enter or telnet `10.92.57.187 2013`.

Telnetting to a Management Port

Users can access the ML-Series through a standard Cisco IOS management port in the same manner as other Cisco IOS platforms. For further details about configuring ports and lines for management access, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

As a security measure, the vty lines used for Telnet access are not fully configured. In order to gain Telnet access to the ML-Series card, you must configure the vty lines via the serial console connection or preload a startup-configuration file that configures the vty lines. A port on the ML-Series must first be configured as the management port; see the "Configuring the Management Port" section on page 5-8.

ML-Series IOS CLI Console Port

The ML-Series card has an RJ-11 serial console port on the card faceplate labeled CONSOLE. The console port is wired as data circuit-terminating equipment (DCE). It enables communication from the serial port of a PC or workstation running terminal emulation software to the Cisco IOS CLI on a specific ML-Series card.

RJ-11 to RJ-45 Console Cable Adapter

Due to space limitations on the ML-Series card faceplate, the console port is an RJ-11 modular jack instead of the more common RJ-45 modular jack. Cisco supplies an RJ-11 to RJ-45 console cable adapter (P/N 15454-CONSOLE-02) with each ML-Series card. After connecting the adapter, the console port functions like the standard Cisco RJ-45 console port. Figure 5-3 shows the RJ-11 to RJ-45 console cable adapter.
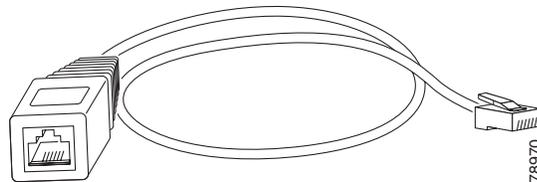
Figure 5-3   Console Cable Adapter

Table 5-1 shows the mapping of the RJ-11 pins to the RJ-45 pins.

Table 5-1   RJ-11 to RJ-45 Pin Mapping

RJ-11 Pin	RJ-45 Pin
1	1
2	2
3	3
4	4
None	5
5	6
None	7
6	8

## Connecting a PC or Terminal to the Console Port

Use the supplied cable, an RJ-11 to RJ-45 console cable adapter, and a DB-9 adapter to connect a PC to the ML-Series console port.

The PC must support VT100 terminal emulation. The terminal-emulation software—frequently a PC application such as HyperTerminal or Procomm Plus—makes communication between the ML-Series and your PC or terminal possible during the setup program.

Step 1   Configure the data rate and character format of the PC or terminal to match these console port default settings:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

Step 2   Insert the RJ-45 connector of the supplied cable into the female end of the supplied console cable adapter.

Step 3   Insert the RJ-11 modular plug end of the supplied console cable adapter into the RJ-11 serial console port, labeled CONSOLE, on the ML-Series card faceplate. Figure 5-4 shows the ML1000-2 faceplate with console port. For the ML100T-12 and ML100X-8, the console port is at the bottom of the card faceplate.

Figure 5-4   Connecting to the Console Port
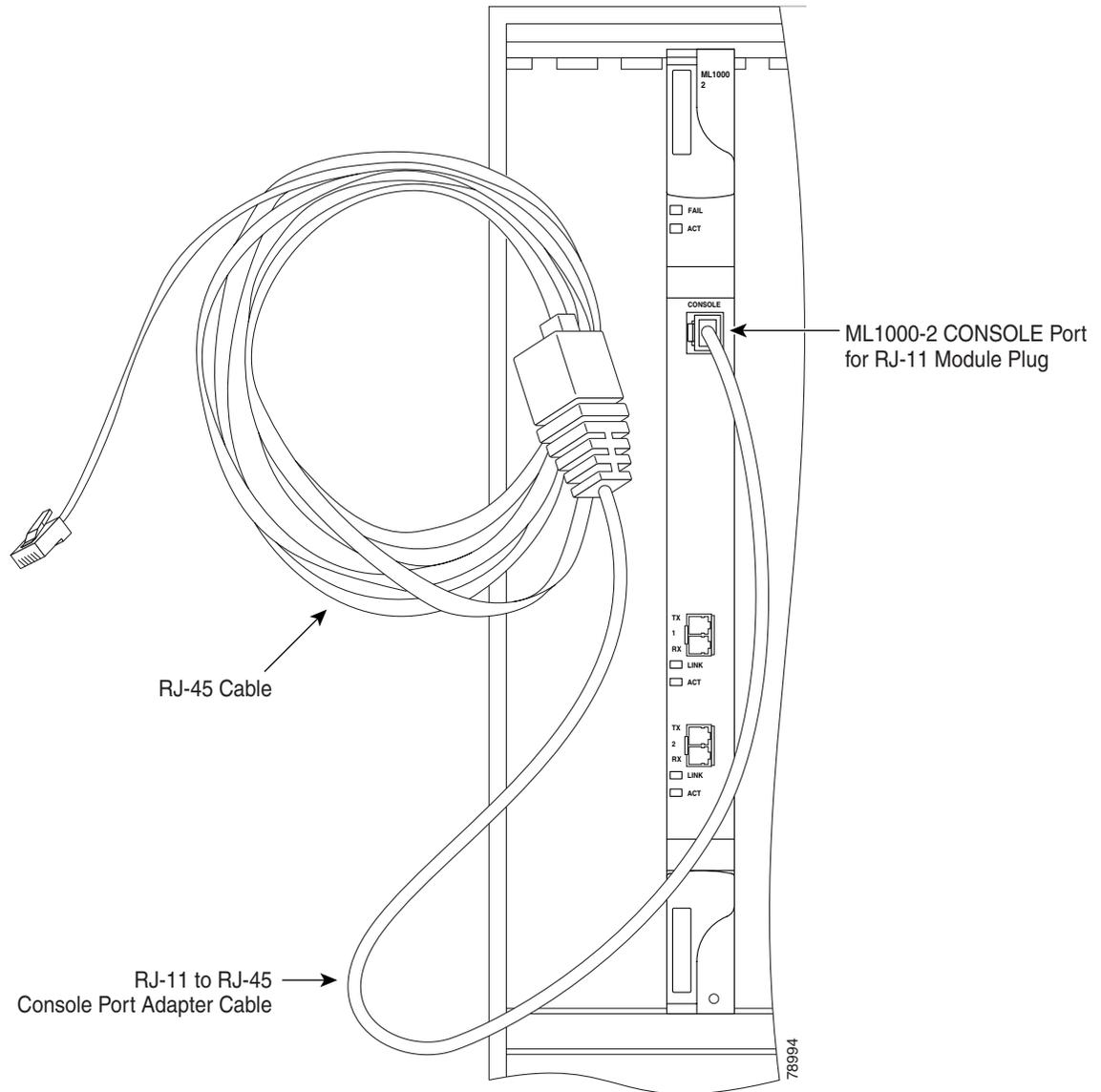
Step 4   Attach the supplied RJ-45-to-DB-9 female DTE adapter to the nine-pin DB-9 serial port on the PC.

Step 5   Insert the other end of the supplied cable in the attached adapter.

Startup Configuration File

The ML-Series card needs a startup configuration file in order to configure itself beyond the default configuration when the card is reset. If no startup configuration file exists in the TCC2/TCC2P flash memory, then the card boots up to a default configuration. Users can manually set up the startup configuration file through the serial console port and the Cisco IOS CLI configuration mode or load a Cisco IOS supplied sample startup configuration file through CTC. A running configuration becomes a startup configuration file when saved with a **copy running-config startup-config** command.

It is not possible to establish a Telnet connection to the ML-Series card until a startup configuration file is loaded onto the ML-Series card. Access is available through the console port.

⚠
Caution   The **copy running-config startup-config** command saves a startup configuration file to the flash memory on the ML-Series card. This operation is confirmed by the appearance of [OK] in the Cisco IOS CLI session. The startup configuration file is also saved to the ONS node's database restoration file after approximately 30 additional seconds.

⚠
Caution   Accessing the read-only memory monitor mode (ROMMON) on the ML-Series card without the assistance of Cisco personnel is not recommended. This mode allows actions that can render the ML-Series card inoperable. The ML-Series card ROMMON is preconfigured to boot the correct Cisco IOS software image for the ML-Series card.

⚠
Caution   The maximum size of the startup configuration file is 98356 bytes (characters).

✎
Note   When the running configuration file is altered, a RUNCFG-SAVENEED condition appears in CTC. This condition is a reminder to enter a **copy running-config startup-config** command in the Cisco IOS CLI, or the changes will be lost when the ML-Series card reboots.

Manually Creating a Startup Configuration File Through the Serial Console Port

Configuration through the serial console port is familiar to those who have worked with other products using Cisco IOS. At the end of the configuration procedure, the **copy running-config startup-config** command saves a startup configuration file.

The serial console port gives the user visibility to the entire booting process of the ML-Series card. During initialization, the ML-Series card first checks for a local, valid cached copy of Cisco IOS. It then either downloads the Cisco IOS software image from the TCC2/TCC2P or proceeds directly to decompressing and initializing the image. Following Cisco IOS initialization the CLI prompt appears, at which time the user can enter the Cisco IOS CLI configuration mode and setup the basic ML-Series configuration.

Passwords

There are two types of passwords that you can configure for an ML-Series card: an enable password and an enable secret password. For maximum security, make the enable password different from the enable secret password.

- Enable password—The enable password is a non-encrypted password. It can contain any number of uppercase and lowercase alphanumeric characters. Give the enable password only to users permitted to make configuration changes to the ML-Series card.

- Enable secret password—The enable secret password is a secure, encrypted password. By setting an encrypted password, you can prevent unauthorized configuration changes. On systems running Cisco IOS software, you must enter the enable secret password before you can access global configuration mode.

  An enable secret password can contain from 1 to 25 uppercase and lowercase alphanumeric characters. The first character cannot be a number. Spaces are valid password characters. Leading spaces are ignored; trailing spaces are recognized.

Passwords are configured in the "Configuring the Management Port" section on page 5-8.

Configuring the Management Port

Because there is no separate management port on ML-Series cards, any Fast Ethernet interface (0 to 11 on the ML100T-12 card and 0 to 7 on the ML100X-8), any Gigabit Ethernet interface (0 to 1 on the ML1000-2 card), or any POS interface (0 to 1 on any ML-Series card) can be configured as a management port. For the packet over SONET (POS) interface to exist, a synchronous transport signal (STS) or synchronous transport module (STM) circuit must first be created through CTC or translation language 1 (TL1).

You can remotely configure the ML-Series card through the management port, but first you must configure an IP address so that the ML-Series card is reachable or load a startup configuration file. You can manually configure the management port interface from the Cisco IOS CLI through the serial console connection.

To configure Telnet for remote management access, perform the following procedure, beginning in user EXEC mode:

	Command	Purpose
Step 1	`Router> enable` `Router#`	Activates user EXEC (or enable) mode. The # prompt indicates enable mode.
Step 2	`Router# configure terminal` `Router(config)#`	Activates global configuration mode. You can abbreviate the command to **config t**. The Router(config)# prompt indicates that you are in global configuration mode.
Step 3	`Router(config)# enable password` `password`	Sets the enable password. See the "Passwords" section on page 5-8.
Step 4	`Router(config)# enable secret password`	Allows you to set an enable secret password. See the "Passwords" section on page 5-8. A user must enter the enable secret password to gain access to global configuration mode.
Step 5	`Router(config)# interface type number` `Router(config-if)#`	Activates interface configuration mode on the interface.

	Command	Purpose
Step 6	`Router(config-if)# ip address` `ip-address subnetmask`	Allows you to enter the IP address and IP subnet mask for the interface specified in Step 5.
Step 7	`Router(config-if)# no shutdown`	Enables the interface.
Step 8	`Router(config-if)# exit` `Router(config)#`	Returns to global configuration mode.
Step 9	`Router(config)# line vty line-number` `Router(config-line)#`	Activates line configuration mode for virtual terminal connections. Commands entered in this mode control the operation of Telnet sessions to the ML-Series card.
Step 10	`Router(config-line)# password password`	Allows you to set a password for Telnet sessions.
Step 11	`Router(config-line)# end` `Router#`	Returns to privileged EXEC mode.
Step 12	`Router# copy running-config` `startup-config`	(Optional) Saves your configuration changes to NVRAM.

After you have completed configuring remote management on the management port, you can use Telnet to remotely assign and verify configurations.

Configuring the Hostname

In addition to the system passwords and enable password, your initial configuration should include a hostname to easily identify your ML-Series card. To configure the hostname, perform the following task, beginning in enable mode:

	Command	Purpose
Step 1	`Router# configure terminal` `Router(config)#`	Activates global configuration mode.
Step 2	`Router<config)# hostname name-string`	Allows you to enter a system name. In this example, we set the hostname to "Router."
Step 3	`name-string(config)# end` `name-string#`	Returns to privileged EXEC mode.
Step 4	`name-string# copy running-config` `startup-config`	(Optional) Copies your configuration changes to NVRAM.

CTC and the Startup Configuration File

CTC allows a user to load the startup configuration file required by the ML-Series card. A Cisco-supplied sample Cisco IOS startup configuration file, named **Basic-IOS-startup-config.txt**, is available on the Cisco ONS 15454 SONET/SDH software CD. CISCO15 is the Cisco IOS CLI default line password and the enable password for this configuration. Users can also create their own startup configuration file; see the "Manually Creating a Startup Configuration File Through the Serial Console Port" section on page 5-7.

CTC can load a Cisco IOS startup configuration file into the TCC2/TCC2P card flash before the ML-Series card is physically installed in the slot. When installed, the ML-Series card downloads and applies the Cisco IOS software image and the preloaded Cisco IOS startup-configuration file. Preloading the startup configuration file allows an ML-Series card to immediately operate as a fully configured card when inserted into the ONS 15454 SONET/SDH.

If the ML-Series card is booted up prior to the loading of the Cisco IOS startup configuration file into TCC2/TCC2P card flash, then the ML-Series card must be reset to use the Cisco IOS startup configuration file. The user can also issue the command **copy start run** at the Cisco IOS CLI to configure the ML-Series card to use the Cisco IOS startup configuration file.

Loading a Cisco IOS Startup Configuration File Through CTC

This procedure details the initial loading of a Cisco IOS Startup Configuration file through CTC.

Step 1   At the card-level view of the ML-Series card, click the **IOS** tab. The CTC IOS window appears.

Step 2   Click the **IOS Startup Config** button.

The config file dialog box appears.

Step 3   Click the **Local -> TCC** button.

Step 4   The sample Cisco IOS startup configuration file can be installed from either the ONS 15454 SONET/SDH software CD or from a PC or network folder:

- To install the Cisco supplied startup config file from the ONS 15454 SONET/SDH software CD, insert the CD into the CD drive of the PC or workstation. Using the CTC config file dialog, navigate to the CD drive of the PC or workstation and double-click the **Basic-IOS-startup-config.txt** file.

- To install the Cisco supplied config file from a PC or network folder, navigate to the folder containing the desired Cisco IOS startup config file and double-click the desired Cisco IOS startup config file.

Step 5   In the Are you sure? dialog box, click the **Yes** button.

The Directory and Filename fields on the configuration file dialog box update to reflect that the Cisco IOS startup config file is loaded onto the TCC2/TCC2P.

Step 6   Load the Cisco IOS startup config file from the TCC2/TCC2P to the ML-Series card:

a.   If the ML-Series card has already been installed, right-click on the ML-Series card at the node level or card level CTC view and select **Reset Card**.

After the reset, the ML-Series card runs under the newly loaded Cisco IOS startup configuration file.

b.   If the ML-Series card is not yet installed, installing the ML-Series card into the slot loads and runs the newly loaded Cisco IOS startup configuration on the ML-Series card.

✎
Note   When the Cisco IOS startup configuration file is downloaded and parsed at initialization, if there is an error in the parsing of this file, an ERROR-CONFIG alarm is reported and appears under the CTC Alarms tab or in TL1. No other Cisco IOS error messages regarding the parsing of text are reported to the CTC or in TL1. An experienced Cisco IOS user can locate and troubleshoot the line in the startup configuration file that produced the parsing error by opening the Cisco IOS CLI and entering a **copy start run** command.

> **Note**   A standard ONS 15454 SONET/SDH database restore reinstalls the Cisco IOS startup config file on the TCC2/TCC2P, but does not implement the Cisco IOS startup config on the ML-Series. See the "Database Restore of the Startup Configuration File" section on page 5-11 for additional information.

Database Restore of the Startup Configuration File

The ONS 15454 SONET/SDH includes a database restoration feature. Restoring the database will reconfigure a node and the installed line cards to the saved provisioning, except for the ML-Series card. The ML-Series card does not automatically restore the startup configuration file saved in the TCC2/TCC2P database.

A user can load the saved startup configuration file onto the ML-Series card in two ways. He can revert completely to the saved startup configuration and lose any additional provisioning in the unsaved running configuration, which is a restoration scheme similar to other ONS cards, or he can install the saved startup configuration file on top of the current running configuration, which is a merging restoration scheme used by many Cisco Catalyst devices.

To revert completely to the startup configuration file saved in the restored database, the user needs to reset the ML-Series card. Right-click the ML-Series card in CTC and choose **Reset** or use the Cisco IOS CLI **reload** command to reset the ML-Series card.

> **Caution**   Resetting the ONS 15454 ML-Series card causes a loss of traffic and closes any Telnet sessions to the card.

To merge the saved startup configuration file with the running configuration, use the Cisco IOS CLI **copy startup-config running-config** command. This restoration scheme should only be used by experienced users with an understanding of the current running configuration and the Cisco IOS **copy** command. The **copy startup-config running-config** command will not reset the ML-Series card. The user also needs to use the Cisco IOS CLI **copy running-config startup-config** command to save the new merged running configuration to the startup configuration file.

Multiple Microcode Images

The primary packet processing and forwarding on the ML-Series card is done by the network processor, which is controlled by microcode. This microcode is a set of instructions (software) loaded into the network processor and executed at high speed. The network processor has limited microcode storage space.

Some of the ML-Series card features require significant amounts of microcode, and this additional microcode exceeds the storage capacity of the network processor. These features are added as new microcode images (separate microcode programs). The network processor can only hold one microcode image at a time, and changing the loaded microcode image requires resetting the network processor.

The user can choose from several microcode images for the ML-Series card. Table 5-2 compares the features available with the different microcode images.

Caution   Configuring topology discovery or shortest path load balancing on an ML-Series card with the SW-RPR microcode image disables support for Cisco proprietary resilient packet ring (RPR) and dual RPR interconnect (DRPRI).

Table 5-2   Microcode Image Feature Comparison

Features	Base	Enhanced	EoMPLS[1]	SW-RPR	802.17
Packet Classification	Yes	Yes	Yes	Yes	Yes
Policing and Quality of Service (QoS)	Yes	Yes	Yes	Yes	Yes
Layer 2 Bridging	Yes	Yes	Yes	Yes	Yes
IP Unicast Switching	Yes	Yes	Yes	Yes	No
IP Fragmentation	Yes	No	No	No	No
IP Multicast Switching	Yes	No	No	No	No
EoMPLS	No	No	Yes	No	Future
Cisco Proprietary RPR Encapsulation	Yes	Yes	Yes	Yes	No
Cisco Proprietary RPR Resiliency Enhancements: • Cisco Proprietary RPR Keep Alive • Cisco Proprietary RPR CRC Threshold Configuration, Detection, and Wrap • Cisco Proprietary RPR Customer Ethernet FCS Preservation • Cisco Proprietary RPR CRC Error Alarm Generation • Cisco Proprietary RPR Shortest Path Determination and Topology Discovery	No	No	Yes	Yes	No
PPP/HDLC[2]/LEX[3]Encapsulation Support	Yes	Yes	Yes	No	No
IEEE 802.17b	No	No	No	No	Yes
Enhanced Performance Monitoring	No	Yes	No	Yes	Yes
Redundant Interconnect	No	No	Yes	Yes	Yes

1. Ethernet over multiprotocol label switching

2. high-level data link control

3. Ethernet over GFP-F according to ITU-T G.7041

Changing the Working Microcode Image

The user can change the microcode image using Cisco IOS CLI configuration and a reset of the ML-Series card. Using this configuration method, you can load any microcode image except 802.17. To automatically download and enable the 802.17 microcode image, use CTC to set the card mode to 802.17. For more information, see the

To configure a working microcode image, perform the following procedure, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# *microcode* {**base** | **enhanced** | **fail** | **mpls** | **spr**}	Configures the ML-Series card with the selected microcode image: **base**—(Default) Enables base features only. Base features include Multicast routing and IP fragmentation. **enhanced**—Enables ERMS, enhanced packet statistics, and enhanced DRPRI. Disables multicast routing and IP fragmentation. **fail**—This command and feature are specific to ML-Series cards. In the event of a microcode failure, it configures the ML-Series card to save information to the flash memory and then reboot. The information is saved for use by the Cisco Technical Assistance Center (Cisco TAC). To contact Cisco TAC, see Appendix C, "Using Technical Support.". **mpls**—Enables MPLS. Disables IP multicast, IP fragmentation, and Ethernet relay multipoint service (ERMS) support. **spr**—Enables Cisco proprietary RPR encapsulation, Enhanced Packet Statistics, DRPRI, and Keepalives. Disables Multicast routing or IP fragmentation.
Step 2	Router(config)# **exit**	Exits global configuration mode.
Step 3	Router# **copy running-config startup-config**	Saves the configuration changes to flash memory. The running configuration file configured with the new microcode image choice must be saved as a startup configuration file for the ML-Series card to reboot with the new microcode image choice.
Step 4	Router# **reload**	Resets the ML-Series card and loads the new microcode image. ⚠ **Caution** Resetting the ML-Series card causes a loss of traffic and closes any Telnet sessions to the card.
Step 5	Router# **show microcode**	Shows the microcode image currently loaded and the microcode image that loads when the ML-Series card resets.

Version Up Software Upgrade

The Version Up software upgrade feature allows users to independently upgrade ML-Series cards and the ML-MR-10 card as part of an overall software upgrade process. With this feature enabled, the user first upgrades all the cards in the node that are not ML-Series cards or ML-MR-10 card, then in a second pass updates the ML-Series cards or ML-MR-10 card. Version Up is disabled by default.

The user can initiate individual upgrades for each ML-Series cards or ML-MR-10 card or upgrade all the ML-Series cards or ML-MR-10 card at the same time. In the case of redundant ML-Series cards or ML-MR-10 card, individual upgrades allow time to verify the proper operation of the first card before the second card is upgraded. No ML-Series cards or ML-MR-10 card is updated until the user specifically requests it.

The user can perform a Version Up upgrade with CTC or Cisco Transport Manager (CTM). The Version Up feature is only supported on the ONS 15454 and SDH platforms. TL1 does not support the Version Up feature, and you cannot enter TL1 commands during the Version Up process.

Node and Card Behavior During Version Up

Between the upgrade of the non-ML-Series cards or ML-MR-10 card and the upgrade of the ML-Series cards or ML-MR-10 card, the node functions normally with regards to existing circuits but does not allow new provisioning or software downloads. Alarms still operate even with the ML-Series cards or ML-MR-10 card that are not yet upgraded.

The ML-Series cards or ML-MR-10 card also continues to carry data traffic in the time span between the upgrade of the non-ML-Series cards or ML-MR-10 card and the upgrade of the ML-Series cards or ML-MR-10 card, although this traffic drops when the ML-Series card or ML-MR-10 card resets to load the new software. You can telnet to the ML-Series card or ML-MR-10 card and configure the card using the Cisco IOS CLI, but the new configuration only exists in the running configuration file and cannot be saved to the startup configuration file.

During the Version Up upgrade, a SwMismatch condition appears for any cards running a different software version, even for non-ML-Series cards or ML-MR-10 card awaiting their turn to reset. When the card resets and loads the new software, the condition clears. The SwMismatch condition disappears on the ML-Series cards or ML-MR-10 card as they finish resetting and loading the new software. You can use the SwMismatch condition to keep track of ML-Series cards or ML-MR-10 card that still need upgrading. A SysBoot alarm is also raised during the upgrade. This alarm does not clear until all the ML-Series cards or ML-MR-10 card is upgraded.

## Enabling and Completing Version Up

The default software upgrade behavior for the node is fully automatic. To enable Version Up, the NE defaults must be changed by a Superuser.

This procedure details enabling the Version Up feature through NE Defaults and completing the Version Up process.

Step 1   At the node view, click the **Provisioning > Defaults** tabs.

The Node Defaults window appears (Figure 5-5).

Figure 5-5   Node Defaults Delayed Upgrade Settings
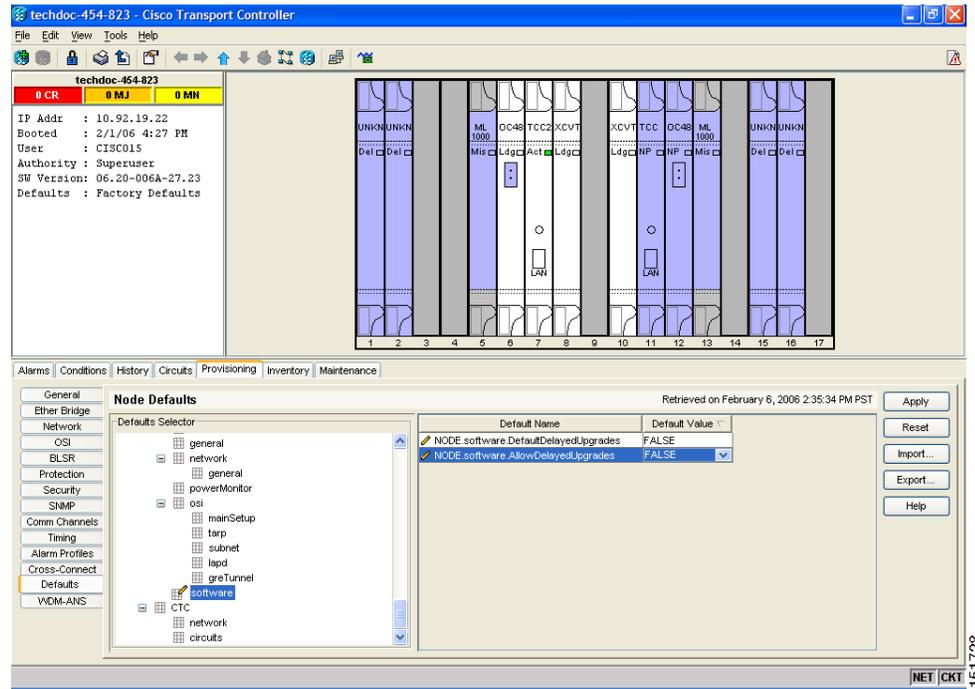
Step 2   In the Defaults Selector field, click **NODE** and then click **software.**

In the Default Name column, the *Node.Software.DefaultDelayedUpgrades* row and the *Node.Software.AllowDelayedUpgrades* row appear (Figure 5-5).

Step 3   Change the Default Value of the *Node.Software.AllowDelayedUpgrades* row to TRUE.

Step 4   Change the Default Value of the *Node.Software.DefaultDelayedUpgrades* row to TRUE.

Step 5   Click **Apply**.

The NE default is now set to enable Version Up.

Step 6   Begin the standard upgrade procedure for the node. Refer to the release-specific software upgrade document.

After clicking **Activate**, the Software Activation dialog box appears.

Step 7   Select the Delay automatic activation on the Software Activation dialog check box and click **OK**

Step 8   Accept the confirmation prompt to begin the Version Up activation.

✎

Note   Clearing the Delay automatic activation on the ML-Series cards or ML-MR-10 card check box and clicking OK begins normal activation and upgrades all the cards in the node, including the ML-Series cards or the ML-MR-10 card.

Step 9   After the new software load is activated on the node and all the non-ML-Series cards or ML-MR-10 card, you can activate this load on the ML-Series cards or ML-MR-10 card by resetting the ML-Series cards or the ML-MR-10 card.

⚠

Caution   Resetting the ML-Series card or ML-MR-10 card causes a loss of traffic and closes any Telnet sessions to the card.

To reset the ML-Series card or ML-MR-10 card through CTC, go to node view and click the ML-Series or ML-MR-10 card card to reveal a short cut menu, click **Reset Card**.

Step 10   After the ML-Series card or ML-MR-10 card reloads, verify that the correct software build is on the card using the Cisco IOS CLI privilege level **show version** command.

Example 5-1 shows a partial example of the **show version** command output with the Cisco IOS software version in bold.

Example 5-1   Output from show version Command

```
ML_Series# show version

Cisco IOS Software, ONS M-Series Software (DAYTONA-I7K91-M), Experimental Version
12.2(20050912:041138) [BLD-IOS_MARINER_MARINER_BF5_BUILD_6.amoayedi 105]
```

Cisco IOS Command Modes

The Cisco IOS user interface has several different modes. The commands available to you depend on which mode you are in. To get a list of the commands available in a given mode, type a question mark (?) at the system prompt.

Table 5-3 describes the most commonly used modes, how to enter the modes, and the resulting system prompts. The system prompt helps you identify which mode you are in and, therefore, which commands are available to you.

✎

Note   When a process makes unusually heavy demands on the CPU of the ML-Series card, it could impair CPU response time and cause a CPUHOG error message to appear on the console. This message indicates which process used a large number of CPU cycles, such as the updating of the routing table with a large number of routes due to an event. Seeing this message as a result of card reset or other infrequent events should not be a cause for concern.

Table 5-3   Cisco IOS Command Modes

Mode	What You Use It For	How to Access	Prompt
User EXEC	Connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and display system information.	Log in.	`Router>`
Privileged EXEC (also called Enable mode)	Set operating parameters. The privileged command set includes the commands in user EXEC mode, as well as the **configure** command. Use this command mode to access the other command modes.	From user EXEC mode, enter the **enable** command and the enable password.	`Router#`
Global configuration	Configure features that affect the system as a whole.	From privileged EXEC mode, enter the **configure terminal** command.	`Router(config)#`
Interface configuration	Enable features for a particular interface. Interface commands enable or modify the operation of a Fast Ethernet, Gigabit Ethernet, or POS port.	From global configuration mode, enter the **interface** *type number* command. For example, enter **interface fastethernet 0** for Fast Ethernet, **interface gigabitethernet 0** for Gigabit Ethernet interfaces, or **interface pos 0** for **POS** interfaces.	`Router(config-if)#`
Line configuration	Configure the console port or vty line from the directly connected console or the virtual terminal used with Telnet.	From global configuration mode, enter the **line console 0** command to configure the console port or the **line vty** *line-number* command to configure a vty line.	`Router(config-line)#`

When you start a session on the ML-Series card, you begin in user EXEC mode. Only a small subset of the commands are available in user EXEC mode. To have access to all commands, you must enter privileged EXEC mode, also called Enable mode. From privileged EXEC mode, you can type in any EXEC command or access global configuration mode. Most of the EXEC commands are single-use commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the ML-Series card.

The configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across ML-Series card reboots. You must start in global configuration mode. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and a variety of protocol-specific modes.

ROM monitor (ROMMON) mode is a separate mode used when the ML-Series card cannot boot properly. For example, your ML-Series card might enter ROM monitor mode if it does not find a valid system image when it is booting, or if its configuration file is corrupted at startup.

Using the Command Modes

The Cisco IOS command interpreter, called the EXEC, interprets and executes the commands you enter. You can abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh** and the **configure terminal** command to **config t**.

Exit

When you type **exit**, the ML-Series card backs out one level. In general, typing **exit** returns you to global configuration mode. Enter **end** to exit configuration mode completely and return to privileged EXEC mode.

Getting Help

In any command mode, you can get a list of available commands by entering a question mark (?).

```
Router> ?
```

To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is called word help, because it completes a word for you.

```
Router# co?
configure
```

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you have already entered.

```
Router#configure ?
  memory              Configure from NV memory
  network             Configure from a TFTP network host
  overwrite-network   Overwrite NV memory from TFTP network host
  terminal            Configure from the terminal
  <cr>
```

To redisplay a command you previously entered, press the Up Arrow key. You can continue to press the Up Arrow key to see more of the previously issued commands.

Tip If you are having trouble entering a command, check the system prompt, and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

You can press **Ctrl-Z** or type **end** in any mode to immediately return to privileged EXEC (enable) mode, instead of entering **exit**, which returns you to the previous mode.