# Performing Basic Configuration Tasks

SYSTEM ADMINISTRATOR GUIDE

6/1543-CRA 119 1170/1-V1 Uen G

### Copyright

### Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

### Trademark List

| | |
|---|---|
| **SmartEdge** | is a registered trademark of Telefonaktiebolaget LM Ericsson. |
| **NetOp** | is a trademark of Telefonaktiebolaget LM Ericsson. |

# Contents

# 1 Performing Basic Configuration Tasks

This document provides an overview of the command line interface (CLI). It describes the tasks used to initiate and navigate the CLI, manage database transactions, collect crash dump data, monitor the system, upload core dump files, configure system identity, set the system clock, and configure of TCP keepalive, administrator account, management port, and console setup.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **Product Overview** folder of this Customer Product Information library.

## 1.1 About Basic Configuration Tasks

The primary administrator interface to the operating system is the CLI. You access the CLI from the console port or through a remote session (for example, Telnet or Secure Shell [SSH]) to perform all configuration tasks and to monitor the operating system. To access the operating system software and its CLI, use either of the following methods:

- Connect to the console port—Located on the controller card and labeled *Craft 2*; you can connect a terminal to this port, either directly or through a terminal server.

- Connect to the Ethernet management port—Located on the controller card and labeled *ENET*; you can connect a terminal to the system over a LAN using this port if remote access using Telnet or SSH has been enabled. These services are enabled on local context by default.

If the console port has been secured or if the Ethernet management port has been configured, you are prompted to log on. If the console port has not been secured, you initiate your session by simply pressing **Enter**. In either case, your session begins in exec mode. To secure the console port and configure the Ethernet management port, see Accessing the CLI.

This section provides information about case sensitivity, partially typed commands and the no and default forms of commands.

### 1.1.1 Commands and Case-Sensitivity

Keywords in commands are not case-sensitive. For example, the `show version` command is accepted if entered in any of the following ways: `show version`, `SHOW VERSION`, or `Show Version`.

Arguments are case-sensitive. For example, if you supply **Customers** for the *`ctx-name`* argument in the `context` *`ctx-name`* command, the operating system software does not recognize the name **customers** as the same context.

### 1.1.2 Partially Typed Commands

In all modes, the system recognizes and accepts partially typed commands and keywords, provided that you have entered a sufficient text to be unique. For example, rather than typing `configure`, you can type `conf` and press `Enter` to enter configuration mode. However, if you enter the string `con`, an error is returned, because insufficient characters have been entered to distinguish between the `configure` command, and the `context` command.

### 1.1.3 No and Default Forms of Commands

Many configuration commands support the `no` keyword. Typing the `no` keyword in front of a command disables the function, removes a command from the configuration, or sets a command to its default state. For example, to enable the Routing Information Protocol (RIP), enter the `router rip` command (in context configuration mode). To subsequently disable the RIP process and remove the command from the configuration, enter the `no router rip` command (in context configuration mode).

Many configuration commands support the `default` keyword. Typing the `default` keyword in front of a command returns a parameter or feature to the default state.

## 1.2 Log On and Initiate the CLI

To initiate a CLI session, you log on to the SmartEdge router, either remotely connected to the Ethernet management port or directly connected to the console port; upon successful log on, the CLI is set to exec mode, by default.

**Note:** You must have an administrator account to log on. To configure the initial administrator account in the local context for a new system, see Accessing the CLI; to configure additional administrator accounts in any context, see *Configuring Contexts*.

To log on to the system using SSH:

- If you are logging on to a router for which the IP address and SSH service are configured in a context different from that of the administrator, enter the administrator name in the following format:

***admin-name@ctx-name***

Replace the ***ctx-name*** argument with the name of the context in which the user is configured for authentication.

- If you are logging on to a router for which the IP address and SSH service are configured in the same context as the administrator, enter the administrator name in the following format:

  ***admin-name***

To log on to the system using Telnet:

- If you are logging on to a router that has the administrator configured in a nonlocal context, enter the administrator name in the following format when prompted:

  ***admin-name@ctx-name***

- If you are logging on to a router that has the administrator configured in a local context, enter the administrator name in the following format when prompted:

  ***admin-name@***[***ctx-name***]

  **Note:** In this situation, the ***ctx-name*** argument is optional.

**Note:** The separator character between the ***admin-name*** and the ***ctx-name*** or ***ip-address*** arguments is configurable and can be any of %, -, @, _, \\, #, and /. For information about configuring the separator character, see *Command List*. The default character is @, which is used throughout this document.

When you connect to the system either directly to the console, or remotely to the management port, the password you enter is not echoed. In addition, passwords are stored in the configuration file in encrypted format.

If you have configured the management port, you can establish a Telnet or SSH session to the system. There are many tools that provide Telnet and SSH access to remote systems. These tools are beyond the scope of this document. In general, you must provide the system name (the hostname configured for the system) or IP address (the IP address configured for the system management port), as well as an administrator name and password.

If you forget a password, you must delete the administrator account and create a new one; there is no way to modify the password for an administrator account.

If you forget all passwords on the system, you must perform the password discovery procedure described in *Recovering Passwords*.

The operating system provides default settings for local console sessions. You can customize these settings for the duration of the current session. To change the settings, see *Performing Basic System Tasks*.

After you are logged on to the system, you have access to the CLI, based on the context to which you are logged on and the privilege level of your account.

**Note:** If you are using Telnet to access the system, to enter the Telnet shell (with the Telnet prompt), enter the `^]` characters. The **se_telnet** prompt is displayed.

## 1.3 Navigate the CLI

To navigate the CLI, perform the tasks described in Table 1.

*Table 1 Navigate the CLI*

| Task | Root Command | Notes |
|---|---|---|
| Return the privilege level for the current exec session to the initial privilege level configured for the current administrator account. | *disable* | When you create the account, the initial privilege level is specified.<br>Enter this command in exec mode. |
| Change the current privilege level for an exec session while in exec mode. | *enable* | You can specify a level up to the level specified for your account.<br>Enter this command in exec mode. |
| Return to exec mode while in any configuration mode. | *end* | Enter this command in any configuration mode. |
| Terminate the current CLI session while in exec mode. | *exit* | Enter this command in exec mode. |
| Move up one level in the configuration mode hierarchy while in a configuration mode; return to exec mode while in global configuration mode. | *exit* | Enter this command in any configuration mode. |
| Enter global configuration mode. | *configure* | Enter this command in exec mode. |
| Display the current configuration of the SmartEdge router or the contents of a previously saved configuration file on the local file system. | *show configuration* | Enter this command in any configuration mode |
| Display the command history for the current session. | *show history* | Enter this command in any configuration mode |
| Display outstanding transactions for other administrators or for internal processes. | *show transaction* | Enter this command in any configuration mode |
| Enter a configuration mode from another configuration mode. | See Table 7 for the command to enter the mode. | |

**Note:** Within any configuration mode, you can enter commands that are available at the one level higher than the current configuration mode without first entering the `exit` command to return to the higher-level configuration mode. For example, within interface configuration mode, you can type any of the commands in that mode and any commands in the context configuration mode—the next highest mode in the hierarchy.

## 1.4 Manage Database Transactions

Every configuration command that you enter becomes part of a database transaction, which has a transaction ID associated with it. Commands in a transaction are not incorporated into the database until you commit the transaction. To manage database transactions, perform the tasks described in Table 2.

*Table 2 Manage Database Transactions*

| Task | Root Command | Notes |
|---|---|---|
| Begin a transaction and enter global configuration mode. | *configure* | Enter this command in exec mode. |
| Erase the current transaction and begin a new one. | *abort* | Enter this command in any configuration mode. |
| Assign a comment to the current configuration database transaction. The description can only be viewed with the **show transaction** command. | *comment* | Enter this command in any configuration mode.<br>For more information on the **show transaction** command, see *Command List*. |
| Save the current transaction and begin a new one. | *commit* | Enter this command in any configuration mode. |
| Save the current transaction, exit the current configuration mode, and return to exec mode. | *end* | Enter this command in any mode. |
| Neither save nor delete the current transaction when returning to the next highest level configuration mode; commit the transaction when exiting global configuration mode and returning to exec mode. | *exit* | Enter this command in any mode. |

# 1.5 Work with Commands

## 1.5.1 Display Help for a Command

You can access the online Help for the CLI in the following ways:

- Use the `?` command when entering a command to display the options available at the current state of the command syntax.
- Use the **`help`** command to display how to use the ? character to obtain help.

Table 3 lists these commands; enter either command in any mode.

*Table 3 Access Online Help*

| **Task** | **Root Command** |
|---|---|
| Obtain help for the current command. | *?* |
| Obtain help for using the `?` command. | *help* |

**Note:** To enter the `?` character as part of a command, when it is not a request for online Help, enter the `Esc` key followed by the `?` character.

## 1.5.2 Recall Previous Command Entries

Table 4 lists two Emacs-style command keyboard sequences that allow you to step through previously entered commands.

*Table 4 Recall Previously Entered Commands*

| **Keyboard** | **Description** |
|---|---|
| `Ctrl+p` or up arrow | Recalls previous command in the command history |
| `Ctrl+n` or down arrow | Recalls next command in the command history |

## 1.5.3 Edit Command Entries

Table 5 lists additional Emacs-style command keyboard sequences.

*Table 5 Additional Emacs-Style Keyboard Sequences*

| **Keyboard** | **Description** |
|---|---|
| `Ctrl+f` or right arrow | Moves cursor forward one character |
| `Ctrl+b` or left arrow | Moves cursor backward one character |
| `Esc+f` | Moves cursor forward one word |
| `Esc+b` | Moves cursor backward one word |

*Table 5 Additional Emacs-Style Keyboard Sequences*

| Keyboard | Description |
|---|---|
| `Ctrl+a` | Moves cursor to beginning of line |
| `Ctrl+e` | Moves cursor to end of line |
| `Ctrl+k` | Deletes to end of line |
| `Ctrl+u` | Deletes to beginning of line |
| `Ctrl+d` | Deletes character |
| `Esc+d` | Deletes word |
| `Ctrl+c` | Quits editing the current line |
| `Ctrl+l` | Refreshes (redraws) the current line |
| `Ctrl+t` | Transposes current character with previous |

### 1.5.4 Complete a Command

You can use the **`Tab`** key in any mode to complete a command. Partially typing a command name and pressing the **`Tab`** key causes the command to be displayed in full to the point where a further choice has to be made.

## 1.6 Navigate CLI Output

The CLI automatically pages output for console, Telnet, and SSH sessions. The operating system prints “--more--” to indicate the presence of more output. To navigate command output, use the keyboard sequences described in Table 6.

*Table 6 Auto-More Keys and Functions*

| Key | Function |
|---|---|
| `q` | Skips all remaining output and returns to the CLI prompt |
| `Enter` | Displays one additional line of output |
| `Space` | Displays the next page of output |
| `b` | Displays the previous page of output |

**Note:** You can use the **`terminal length`** and **`terminal width`** commands (in exec mode) to specify a terminal size to correctly paginate the output. For more information, see *Performing Basic System Tasks*.

## 1.7 Exit Command Modes

The following example exits global configuration mode and returns to exec mode:

```
[local]Redback(config)#exit
[local]Redback#
```

The following example exits a CLI session:

```
[local]Redback#exit
```

The following example exits context configuration mode and returns to exec mode:

```
[local]Redback(config-ctx)#end
[local]Redback#
```

## 1.8 Display Available Commands, Keywords, and Arguments

The following output displays the first few commands available for an administrator with a default privilege level of 6 (> prompt):

```
[local]Redback>?
  bulkstats     Manage bulk statistics collection file
  disable       Drop into disable administrator mode
  enable        Modify command mode privilege
  exit          Exit exec mode
  help          Description of the interactive help system
  modify        Modify condition action for ACL rule
  monitor       Monitor information
  more          Display the contents of a file
  mrinfo        Request multicast router information
  mtrace        Trace reverse multicast path from source to receiver
  no            Disable an interactive option
  ping          Packet Internet Groper Command
  reauthorize   Reauthorize subscriber using RADIUS
  show          Show running system information
  ssh           Execute SSH/SSHD commands
  talk          talk to administrator
  telnet        Telnet to a host
  terminal      Modify terminal settings
  traceroute    Trace route to destination
```

The following example uses partial help to display all commands (in global configuration mode) that begin with the character sequence **cl:**

```
[local]Redback(config)#cl?
  clock    clock-source
```

The following example uses full help to display the next argument of a partially complete `clock` command in global configuration mode:

```
[local]Redback(config)#system clock ?


  summer-time   Configure summer (daylight savings) time
  timezone      Configure time zone
```

## 1.9 Manage Database Transactions

This section provides examples for database commit and delete transactions and providing comments for transactions.

### 1.9.1 Commit Transactions

The following example commits the current database transaction in **60** minutes, and includes the comment, **Cfg BGP in local ctx**, to help identify the commit:

```
[local]Redback(config)#commit in 60 Cfg BGP in local ctx
```

The following example, by another administrator logged on to the current session, displays information about the transaction:

```
[local]Redback>show transaction


 TID   State              User     Wait      Comment
------------------------------------------------------------------
 3491  Waiting to Commit admin1   60 min    Cfg BGP in local ctx
```

For more information on the `show transaction` command, see the *Command List*.

### 1.9.2 Delete Transactions

The following example deletes the current transaction:

```
[local]Redback(config)#abort
```

### 1.9.3 Provide Comments for Transactions

The following example provides a comment for the current transaction:

```
[local]Redback(config-ctx)#comment Config context local
```

## 1.10 Configure System-Wide Management Features

To configure system-wide management features, such as crash dumps, core dumps, and system monitoring, perform the tasks described in Table 7; enter all commands in global configuration mode.

*Table 7 Configure System-Wide Management Features*

| Task | Root Command | Notes |
|---|---|---|
| Enable the logging of system events to a remote syslog server that is reachable within the current context. You can configure up to four syslog servers per context. | *logging syslog ip-addr* | Enter the command in context configuration.<br>Log files must be sent to Customer Support when submitting a support request. |
| Enable dynamic random-access memory (DRAM) crash dump data collection. | *service crash-dump -dram* | This is the default condition.<br>To disable it enter the **no** form of the command. |
| Set the duration of the system monitoring process. | *monitor duration* | |
| Enable the sending of core dump files to a URL using the File Transfer Protocol (FTP). | *service upload-core dump* | Core dump files must be sent to Customer support when submitting a support request. |

**Note:** For more information about system data required when submitting a support request, see *Data Collection Guideline for the SmartEdge Router.*

## 1.11 Process Monitoring

The following example sets process management parameters for the Border Gateway Protocol (BGP) process, sets the monitor duration, and then enables monitoring of the BGP process:

```
[local]Redback#configure
[local]Redback(config)#monitor duration 3600
[local]Redback(config)#exit
[local]Redback#monitor process bgp

% enter ctrl-C to exit monitor mode, monitor duration(sec): 3600 (00:00:08)

NAME           PID    SPAWN      MEMORY  TIME           %CPU   STATE
rip            12652      1      576K    00:00:00.02    0.00%  run
```

## 1.12 About Basic System Parameters

Basic system parameters identify and locate the system being used, establish basic services, enable software for paid licensed features, set the system clock parameters, set Transmission Control Protocol (TCP) keepalive parameters, and modify command-line interface (CLI) commands for the system.

Certain key features on the SmartEdge router are separately licensed. These features can be selectively enabled and disabled, using the paid license password for a feature. These features include:

- Layer 2 Tunneling Protocol (L2TP) features and functions—There is a single license for all L2TP features and functions.
- Multiprotocol Label Switching (MPLS) features and functions—There is a single license for all MPLS features and functions.
- IP version 6 (IPv6) features—There is a single license for all IPv6 features and functions.
- Protocol Independent Multicast (PIM) features—There is a single license for all PIM features and functions.
- Internet Group Management Protocol (IGMP) features—There is a single license for all IGMP features and functions.
- Subscriber features and functions—There are separate licenses for specifying the number of active subscribers, IPv6 subscribers, enabling dynamic services for subscribers, and specifying the average subscriber bandwidth, and specifying that subscriber sessions remain active during a controller card switchover for any reason. Dynamic subscriber services include nonstatic Asynchronous Transfer Mode (ATM) profiles, the dynamic assignment of profiles to ATM permanent virtual circuits (PVCs),

clientless IP service selection (CLIPS) circuits, HTTP redirect, and Remote Authentication Dial-In User Service (RADIUS) refresh.

## 1.13 How to Identify Basic System Identification and Services

The following example defines system contact information, hostname, location, and services:

```
[local]Redback#configure
[local]Redback(config)#system contact IS Hotline 1-800-555-1567
[local]Redback(config)#system hostname freebird
[local]freebird(config)#system location Building 3, 2nd Floor, Lab 3
[local]freebird(config)#service multiple-contexts
[local]freebird(config)#service card-auto-reload
[local]freebird(config)#service auto-system-recovery
```

## 1.14 Access Global Configuration Mode

To perform any configuration task, you must first access global configuration mode. To access global configuration mode, perform the task in Table 8.

*Table 8 Access Global Configuration Mode*

| Task | Root Command | Notes |
|---|---|---|
| Access global configuration mode. | *configure* | Enter this command in exec mode. |

## 1.15 Configure the System Identity

To configure the system contact, location, Link Aggregation Control Protocol (LACP) address and priority levels, and system hostname, perform the tasks described in Table 9; enter all commands in global configuration mode.

*Table 9 Configure the System Identity*

| Task | Root Command | Notes |
|---|---|---|
| Identify the department or person to contact, and how, for information regarding the system. | *system contact* | |
| Query the user before creating a new context. | *system confirmations context* | |
| Specify the system hostname. | *system hostname* | The default hostname is Redback. |

*Table 9 Configure the System Identity*

| Task | Root Command | Notes |
|---|---|---|
| Configure the MAC address that will be used in the LACP packet negotiation with peers. | *system lacp mac-address* | |
| Configure the LACP priority order that will be used in the LACP packet negotiation with peers. | *system lacp priority* | The default value is 2. |
| Configure the system location information. | *system location* | |

## 1.16 Configure Service Options

When configuring service options, you cannot create a context until you have enabled the multiple context feature; the only context available without this feature is the local context.

**Caution!**

Risk of data loss. If the console port is directly attached to the serial port of a computer running Windows NT or UNIX, the computer might send a break sequence when it reboots. This has the effect of halting the system and entering kernel debug mode. To reduce the risk, do not enable the console-break feature if the workstation attached to the console port is running Windows NT or UNIX.

To configure service options, perform one or more of the tasks described in Table 10; enter all commands in global configuration mode.

*Table 10 Configure Service Options*

| Task | Root Command | Notes |
|---|---|---|
| Enable the creation of multiple contexts. | *service multiple-contexts* | |
| Enable the automatic reload of the PPA code on a traffic card if either of its PPAs becomes inoperable. | *service card-auto-reload* | This command enables automatic reload for all traffic cards. |
| Enable automatic system recovery when a process halts. | *service auto-system-recovery* | |

*Table 10 Configure Service Options*

| Task | Root Command | Notes |
|---|---|---|
| Enable the console break feature. | *service console-break* | |
| Enable an application-layer protocol (FTP, RCP, SCP, SFTP, SSH, Telnet, TFTP). These services are enabled by default on the local context. | *service* | |

## 1.17 Configure the System Clock

The system clock is the logical clock running the hardware and software functions of the SmartEdge router, regardless of the source of its timing. The real-time clock is a battery backed-up clock derived from an on-board oscillator that updates the system clock during system reload and other circumstances. For further information on clocks, see the hardware guide for your SmartEdge router.

To configure the system clock, perform the tasks described in Table 11. Enter all commands in global configuration mode, except the `clock set` command, which is entered in exec mode.

*Table 11 Configure the System Clock*

| # | Task | Root Command | Notes |
|---|---|---|---|
| 1. | Specify the type of timing interface. | *system clock-source timing-type* | This command is for XCRP4 Controller card only. |
| 2. | Optional. Specify the clock source with one of the following tasks: | | |
| | Specify an internal source. | *system clock-source* | The default value is the active controller card. |
| | Specify an external source. | *system clock-source external* | |
| 3. | Define one or more time zones, including the one in which the system is located. | *system clock timezone* | Use the `local` keyword to identify the zone in which the system is located. |
| 4. | Optional. Enable the system to automatically switch to daylight saving or standard time. | *system clock summer-time* | |
| 5. | Set the current time and date. | *clock set* | Sets both system and real-time clock. Enter this command in exec mode. |

### 1.17.1 How to Enable the System Clock

The following example shows how to specify system clock settings; the SmartEdge router has XCRP4 Controller card installed and the external source is a synchronization supply unit (SSU) with an E1 interface:

```
[local]Redback(config)#system clock-source timing-type sdh
[local]Redback(config)#system clock-source external primary framing crc4
```

If using line timing mode, do the following:

```
[local]Redback(config)#system clock-source timing-type sdh
[local]Redback(config)#system clock-source line primary 3/1
```

**Note:** The `system clock-source timing-type sdh` and `system clock-source line primary 3/1` commands are dependent on the framing type that is configured on the POS port.

## 1.18 Configure the TCP Keepalive Parameters

To modify the TCP keepalive parameters, perform the task described in Table 12; enter the command in global configuration mode.

*Table 12 Configure TCP Keepalive Parameters*

| Task | Root Command |
|---|---|
| Optional. Modify the following TCP keepalive parameters as needed by your configuration:<br>• Maximum number of times the SmartEdge router tries to reestablish a dropped connection.<br>• Amount of time that the SmartEdge router allows a TCP connection to remain open.<br>• Amount of time that the SmartEdge router keeps an idle connection open before disconnecting it. | *tcp keepalive* |

## 1.19 Accessing the CLI

You can access the operating system software and its command line-interface (CLI) using either of the following methods:

- The console port—Located on the controller card and labeled *Craft 2*; you can connect a terminal to this port, either directly or through a terminal server.

- The Ethernet management port—Located on the controller card and labeled *ENET*; you can configure the system to enable remote access using Telnet and Secure Shell (SSH) with this port; you can then access the system remotely using a LAN.

Remote access through the Ethernet management port is disabled by default.

Remote access enables remote file operations, such as downloading and uploading files from and to a remote server, with utilities such as File Transfer Protocol (FTP), Secure Shell FTP (SFTP), Trivial FTP (TFTP), and others.

**Note:** In the following descriptions, the term controller card applies to the Cross-Connect Route Processor (XCRP4) Controller card, including the controller carrier card unless otherwise noted.

The term controller carrier card refers to the controller functions on the carrier card within the SmartEdge 100 chassis. The term I/O carrier card refers to the traffic card functions on the carrier card; these functions are compatible with the similar functions that are implemented on the traffic card that are supported on all other SmartEdge routers.

## 1.20 Log On to the Console Port for the First Time

You can connect a terminal to this port, either directly or through a terminal server; see the appropriate hardware guide for your system for information about connecting and configuring a terminal for use with the console port.

Before you configure the system, the console is not secure; to initiate a session, simply press **`Enter`**.

## 1.21 Configure a Local Administrator Account

To secure the local console and enable remote access, you must configure at least one administrator account on the system. For a newly installed system with only the local context available, you configure an administrator account in the local context. For information about administrator accounts configured in any context, see *Configuring Contexts*.

To configure an administrator account, perform the tasks described in Table 13.

*Table 13 Configure an Administrator Account*

| # | Task | Root Command | Notes |
|---|---|---|---|
| 1. | Access context configuration mode. | *context* | Enter this command in global configuration mode.<br>Specify **`local`** as the context. |

*Table 13 Configure an Administrator Account*

| # | Task | Root Command | Notes |
|---|---|---|---|
| 2. | Create an administrator logon account, secure the console port, enable remote access to the system, and access administrator configuration mode. | *administrator* | Enter this command in content configuration mode. |
| 3. | Specify general attributes for the account; enter these commands in administrator configuration mode (all attributes are optional): | | |
| | Assign a full name or textual description for the administrator. | *full-name* | |
| | Specify the initial privilege level for exec sessions initiated by an administrator. | *privilege start* | The default value is 6; specify a setting of 10 to allow the local administrator to enter configuration commands without needing to enter the **`enable`** command (in exec mode). |
| | Specify the maximum privilege level for an administrator. | *privilege max* | The default value is 15, which is suitable for the local administrator. |
| | Specify public key authentication for an administrator accessing the operating system CLI through SSH. | *public-key* | |

### 1.21.1 How to Configure an Administrator Account

The following example displays the creation of an administrator account with the administrator name **super** and the password **icandoanything**. Because this account is created in the **local** context, this administrator is able to view and modify the entire system configuration, and view all running information on the system. When the administrator logs on to the system, the initial privilege level is **10**. The administrator can modify the privilege level up to the maximum of **15:**

```
[local]Redback#configure
[local]Redback(config)#context local
[local]Redback(config-ctx)#administrator super password icandoanything
[local]Redback(config-administrator)#full-name "Fred P. Lynch x.1234"
[local]Redback(config-administrator)#privilege start 10
[local]Redback(config-administrator)#privilege max 15
[local]Redback(config-administrator)#enable password
pwd_for_priv_level_15
[local]Redback(config-ctx)#
```

Because this account is created in the **local** context, this administrator is able to view and modify the entire system configuration and view all running information on the system.

The next time the administrator **super** logs on to the system with the **icandoanything** password, the administrator is at privilege level 10. To enter privilege level 15, the administrator needs to issue the following commands with the password chosen to enter privilege 15 (in this example, the chosen administrator password is **`pwd_for_priv_level_15`**). This password will not be displayed at the CLI:

```
[local]Redback>enable
Password <enter the password, pwd_for_priv_level_15>
[local]Redback#
```

## 1.22 Secure the Standby Console Port

On systems equipped with two controller cards, the standby console port on the standby controller card is labeled *Craft 2*. You can connect a terminal to this port, either directly or through a terminal server.

Before you configure the system, the standby console port is not secure. To initiate a session, you simply press **`Enter`**.

To secure the standby console port, use the same commands that you use to configure an administrator account on the active console port; see Configure a Local Administrator Account.

## 1.23 Configure the Management Port

The management port is the 10/100 Ethernet port located on the controller card and is designated for system management. The management port is usually configured in the local context.

**Note:** Only the management port on the active controller card is enabled. By default, when the system is powered on or reloaded, the active controller card is in slot 6 in the SmartEdge 400 chassis and slot 7 in the SmartEdge 600, SmartEdge 800, SmartEdge 1200, and SmartEdge 1200H chassis.

To configure the management port, perform the tasks described in Table 14.

*Table 14 Configure the Management Port*

| # | Task | Root Command | Notes |
|---|---|---|---|
| 1. | Access context configuration mode. | *context* | Enter this command in global configuration mode.<br>Specify local as the context. |

*Table 14 Configure the Management Port*

| # | Task | Root Command | Notes |
|---|---|---|---|
| 2. | Create an interface for the management port and access interface configuration mode. | *interface* | Enter this command in context configuration mode. |
| 3. | Assign an IP address to the interface. | *ip address* | Enter this command in interface configuration mode. |
| 4. | Select the management port and access port configuration mode. | *port ethernet* | Enter this command in global configuration mode.<br>The Ethernet management port is port 1 on a controller card. The slot number is 6 in a SmartEdge 400 chassis and slot 7 in a SmartEdge 800 chassis.<br>For a description of this command, see *Configuring ATM, Ethernet, and POS Ports*. |
| 5. | Bind the management port to the interface created in step 2. | *bind interface* | For a description of this command, see *Configuring Bindings*. |
| 6. | Disable the port. | *shutdown* | Use the `no` form to enable the port. |

**Note:** If the system has dual controller cards installed, it is sufficient to configure the Ethernet management port on the controller card in slot 6 or 7, depending on the chassis. Access to the system is switched to the standby controller card if it should become the active controller card during normal operations.

### 1.23.1 How to Configure a Management Port

The following example configures the management port on the controller card in slot **7:**

```
[local]Redback#configure
!Create the interface in the local context and assign an IP address
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface mgmt
[local]Redback(config-if)#ip address 192.168.110.1 255.255.255.0
[local]Redback(config-if)#exit

!Configure the management port
[local]Redback(config)#port ethernet 7/1
[local]Redback(config-port)#bind interface mgmt local
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#end
```

## 1.24 Configure SSH Remote Access Attributes

The operating system software supports SSH and Telnet access to the CLI.

Remote access to the CLI using SSH is similar to remote access using Telnet, in that administrators use the same administrator name and password stored in the operating system configuration file, in Remote Authentication Dial-In User Service (RADIUS), or in Terminal Access Controller Access Control System Plus (TACACS+). The difference is that with SSH, the interactive session is encrypted with the single DES encryption algorithm.

You must complete the tasks described in Table 14 before you configure the SSH attributes. SSH is enabled by default on the local context.

To configure the global SSH attributes, perform one or more of the tasks described in Table 15; enter all commands in global configuration mode.

*Table 15 Configure SSH Attributes*

| Task | Root Command | Notes |
|---|---|---|
| Specify the maximum number of concurrent SSH sessions on the system. | *ssh server full-drop* | The operating system supports up to 32 concurrent administrative sessions (Telnet and SSH) plus one connection to the console port. |
| Specify the number of concurrent sessions after which the system starts dropping SSH connection requests. | *ssh server start-drop* | |
| Specify the rate at which the system drops SSH connection requests after the start-drop value has been reached. | *ssh server rate-drop* | |

**Note:** The preceding task table configures the global attributes of remote administrative sessions. The number of authenticated administrative sessions in any context is also configurable. For more information about specifying the maximum number of authenticated administrative sessions in a context, see the *Command List*.

### 1.24.1 How to Access the System Using Telnet

You can use many different tools to provide Telnet access to the system. The following example initiates a Telnet session to the system with hostname **Host** from a UNIX system. The administrator **super** types in the **icandoanything** password to log on; the password is not echoed by the operating system:

```
unix>telnet Host
Connected to Redback.

Escape character is '^]'.

Username:super@local
Password:
[local]Redback#
.
.
[local]Redback#exit
```

## 1.25 Configure Banners

To configure banners to display different types of messages seen by administrators and subscribers, perform one or more of the tasks described in Table 16; enter all commands in global configuration mode.

*Table 16 Configure Banners*

| Task | Root Command | Notes |
|---|---|---|
| Create a message that displays after a user logs on to the system. | *banner exec* | |
| Create a message of the day (MOTD) that displays on all connected systems before the login prompt. | *banner motd* | The message displays only for Telnet and SSH sessions. |
| Create a message that displays on all connected systems after the login prompt. | *banner login* | The message displays only for Telnet and SSH sessions. |

### 1.25.1 How to Configure System Banners

The following example configures the system banners:

```
[local]Redback#configure
[local]Redback(config)#banner motd /Warning - System going down at 0400./
[local]Redback(config)#banner exec /Welcome to the system/
```

## 1.26 Configure Session Inactivity Timers

To configure session inactivity timers, perform one or more of the tasks described in Table 17; enter all commands in global configuration mode.

*Table 17 Configure Session Inactivity Timers*

| Task | Root Command |
|---|---|
| Set the amount of time the system waits before timing out during a logon attempt. | *timeout login* |
| Set the amount of time before a CLI session times out. | *timeout session* |