CHAPTER 4

Password Recovery in ROM Monitor Mode

This chapter describes how to recover a password on the router. It also includes instructions to bypass ksh authentication on a node.

This chapter contains the following sections:

If the root password is forgotten, it can be recovered only at the RP card. To recover the password at the Designated Shelf Controller (DSC), set the configuration register to 0x142 on the active RP and reboot the router. When the router boots, a password recovery dialog appears. This dialog prompts you to reset the root-system username and password. After you save the new password, the configuration register automatically resets to the prior value (such as 0x102).

Note The AAA authentication configuration can still prevent access, even after the root password is recovered. In this case, you must bypass the ksh authentication via the auxiliary port.

Recovering the Root Password on Single-RP Routers

Use the following procedure to recover the router password from a router with a single RP:

Step 1 Place the router in ROM Monitor mode (ROMMON), as described in the "Entering ROM Monitor Mode" section on page 1-3.

Step 2 Set the RP configuration register to 0x42 at the ROM Monitor prompt:

```
rommon B1> confreg 0x42
```

Note The configuration register is not an environment variable like TURBOBOOT. Do not enter an equal sign when entering the **confreg** command.

Step 3 Reset or power cycle the router so that the new setting takes effect:

```
rommon B2> reset
```

Step 4 Press **Return** at the prompt to enter the password recovery dialog, and then enter the new root-system username and password, and save the configuration.

```
router con0/0RP0/CPU0 is now available

Press RETURN to get started.


--- Administrative User Dialog ---


  Enter root-system username: user
  Enter secret:
  Enter secret again:
RP/0/0/CPU0:Jan 10 12:50:53.105 : exec[65652]: %MGBL-CONFIG-6-DB_COMMIT :
'Administration configuration committed by system'. Use 'show configuration commit changes
2000000009' to view the changes.
Use the 'admin' mode 'configure' command to modify this configuration.



User Access Verification

Username: user
Password:
RP/0/RP0/CPU0:router#
```

Recovering the Root Password on Redundant-RP Routers

Use the following procedure to recover the router password from a router with redundant RPs.

Step 1 Place both RPs in ROM Monitor mode, as described in the "Entering ROM Monitor Mode" section on page 1-3.

Step 2 Set the configuration register of the standby RP to 0x0 so that the standby RP does not take control during the password recovery.

```
rommon B1> confreg 0x0
```

Note The configuration register is not an environment variable like TURBOBOOT. Do not enter an equal sign "(=)" when entering the **confreg** command. See the "ROM Monitor Overview" section on page 1-1 for more information on ROM Monitor mode commands and environmental variables.

Step 3 Set the active RP configuration register to 0x42:

```
rommon B1> confreg 0x42
```

Step 4 Reset or power cycle the router so that the new setting takes effect.

```
rommon B2> reset
```

Step 5 Press **Return** at the prompt to enter the password recovery dialog. Then enter the new root-system username and password and save the configuration, as shown in the following example:

```
router con0/0RP0/CPU0 is now available

Press RETURN to get started.
```

```
--- Administrative User Dialog ---


  Enter root-system username: user
  Enter secret:
  Enter secret again:
RP/0/RP0/CPU0:Jan 10 12:50:53.105 : exec[65652]: %MGBL-CONFIG-6-DB_COMMIT :
'Administration configuration committed by system'. Use 'show configuration commit changes
2000000009' to view the changes.
Use the 'admin' mode 'configure' command to modify this configuration.



User Access Verification

Username: user
Password:
RP/0/0/CPU0:router#
```

Step 6 Set the configuration register of the standby RP to 0x102:

```
rommon B3> confreg 0x102
```

Step 7 Reset the standby RP so that the new setting takes effect and the standby RP becomes operational.

```
rommon B4> reset
```

Bypassing ksh Authentication

You can bypass the ksh authentication for the auxiliary port of the route processor (RP), standby RP, and distributed RP cards and for console and auxiliary ports of line cards (LCs) and service processors (SPs). The situations in which ksh authentication may need to be bypassed include the following:

- DSC (active RP) disk0 corruption
- Loss of Qnet connectivity
- Inability to determine the node ID of the DSC (Active RP)

For information and instructions to bypass ksh authentication, see the “Configuring AAA Services on Cisco IOS XR Software” chapter of *Cisco IOS XR System Security Configuration Guide for the Cisco CRS Router.*

Additional References

The following sections provide references related to the ROM Monitor.

Related Documents

Related Topic	Document Title
How to bypass ksh authentication	*Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide for the Cisco CRS Router*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support