Cisco − Password Recovery Procedure for the Cisco 6xx CP

Table of Contents

Password Recovery Procedure

for the Cisco 6xx CPE

Introduction

This document describes how to recover the ENABLE and EXEC passwords on a Cisco 6xx Customer Premises Equipment (CPE) running a version of Cisco Broadband Operating System (CBOS) earlier than version 2.3.9. The recovery procedure will not work for versions 2.3.9 and later because these versions have Message Digest 5 (MD5) password encryption enabled by default. There is no password recovery for an MD5 encrypted password.

For more information, see MD5 Encryption and CBOS Versions 2.3.9 and Later at the end of this document.

Step−by−Step Procedure

1. Set up console access.

   If you do not have a management cable, you can make one. See Making a Management Cable for the Cisco 600 Series CPE.

   a. Using the serial cable supplied with the modem, connect a COM port on your PC to the management port on the modem.

   b. Configure your Terminal Access Program (such as HyperTerminal in Windows) with the following settings:

      - COM port = port into which you plugged the cable
      - Baud rate: 38400 bps – recommended (standard 9600 bps possible)
      - Data bits: 8
      - Parity: None
      - Stop bits: 1
      - Flow control: None

   c. Press **Enter** until you see the prompt; for example, `cbos>`, `modem1>` or `usa>` .

      When you see the prompt, the PC and Cisco CPE are communicating.

2. Enter RMON mode.

Turn the Cisco CPE off, then on again by disconnecting and reconnecting the AC power plug on the back of Cisco CPE. **Immediately** after reconnecting the power plug, hold down the **Ctrl−C** keys on the keyboard until you see the following:

```
Hello!

Ron960 User Interface: Build  112 (May  9 2000 15:18:15)
NetSpeed HomeRunner(TM); i960 JX; JA step number 03
Copyright 1997 NetSpeed Corporation
Copyright 1998, 1999 Cisco Systems
=>
```

When you see the `=>` prompt, you are in RMON mode and can release the **Ctrl−C** keys.

3. To view the configuration file, execute the **db fef80030** <***# of bytes***> command.

   This command prints the configuration to the screen. The last number indicates the number of bytes to display. Use a value of 100 bytes or more. For example:

```
=>db fef80030 100
fef80030 : 5b 5b 20 49 50 20 52 6f 75 74 69 6e 67 20 3d 20 [[ IP Routing =
fef80040 : 53 65 63 74 69 6f 6e 20 53 74 61 72 74 20 5d 5d Section Start ]]
fef80050 : 0d 0a 49 50 20 50 6f 72 74 20 41 64 64 72 65 73 ..IP Port Addres
fef80060 : 73 20 3d 20 30 30 2c 20 31 37 31 2e 36 38 2e 39 s = 00, 171.68.9
fef80070 : 2e 31 0d 0a 5b 5b 20 43 42 4f 53 20 3d 20 53 65 .1..[[ CBOS = Se
fef80080 : 63 74 69 6f 6e 20 53 74 61 72 74 20 5d 5d 0d 0a ction Start ]]..
fef80090 : 4e 53 4f 53 20 50 72 6f 6d 70 74 20 3d 20 75 73 NSOS Prompt = us
fef800a0 : 61 0d 0a 4e 53 4f 53 20 45 6e 61 62 6c 65 20 50 a..NSOS Enable P
fef800b0 : 61 73 73 77 6f 72 64 20 3d 20 61 6d 6a 5f 0d 0a assword = amj_..
fef800c0 : 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
```

   Notes:
   You must assign an ENABLE password when you configure the Cisco CPE if you want the password to display as encrypted during the recovery procedure. Otherwise, the `enable password` field will be blank.

   If the EXEC password was set, then the `root password` field will hold the EXEC password.

4. Look for your encrypted ENABLE and EXEC passwords.

   The text of the password will be altered by two letters. For example, using the key: `_ = a, ' = b, a = c, b = d, c = e,` and so on, the password "cola" would be "amj_."

   For a complete listing of the ASCII characters, see the ASCII character set.

Example: ENABLE Password

```
=>db fef80030 100
fef80030 : 5b 5b 20 49 50 20 52 6f 75 74 69 6e 67 20 3d 20 [[ IP Routing =
fef80040 : 53 65 63 74 69 6f 6e 20 53 74 61 72 74 20 5d 5d Section Start ]]
fef80050 : 0d 0a 49 50 20 50 6f 72 74 20 41 64 64 72 65 73 ..IP Port Addres
fef80060 : 73 20 3d 20 30 30 2c 20 31 37 31 2e 36 38 2e 39 s = 00, 171.68.9
fef80070 : 2e 31 0d 0a 5b 5b 20 43 42 4f 53 20 3d 20 53 65 .1..[[ CBOS = Se
fef80080 : 63 74 69 6f 6e 20 53 74 61 72 74 20 5d 5d 0d 0a ction Start ]]..
fef80090 : 4e 53 4f 53 20 50 72 6f 6d 70 74 20 3d 20 75 73 NSOS Prompt = us
fef800a0 : 61 0d 0a 4e 53 4f 53 20 45 6e 61 62 6c 65 20 50 a..NSOS Enable P
```

```
fef800b0 : 61 73 73 77 6f 72 64 20 3d 20 61 6d 6a 5f 0d 0a assword = amj_..
fef800c0 : 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef800d0 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef800e0 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef800f0 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef80100 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef80110 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef80120 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
```

Example: EXEC (Root) Password

Note that the ENABLE password is not set.

```
=> db fef80030 100
fef80030 : 5b 5b 20 49 50 20 52 6f 75 74 69 6e 67 20 3d 20 [[ IP Routing =
fef80040 : 53 65 63 74 69 6f 6e 20 53 74 61 72 74 20 5d 5d Section Start ]]
fef80050 : 0d 0a 49 50 20 50 6f 72 74 20 41 64 64 72 65 73 ..IP Port Addres
fef80060 : 73 20 3d 20 30 30 2c 20 31 37 31 2e 36 38 2e 39 s = 00, 171.68.9
fef80070 : 2e 31 0d 0a 5b 5b 20 43 42 4f 53 20 3d 20 53 65 .1..[[ CBOS = Se
fef80080 : 63 74 69 6f 6e 20 53 74 61 72 74 20 5d 5d 0d 0a ction Start ]]..
fef80090 : 4e 53 4f 53 20 50 72 6f 6d 70 74 20 3d 20 75 73 NSOS Prompt = us
fef800a0 : 61 0d 0a 4e 53 4f 53 20 45 6e 61 62 6c 65 20 50 a..NSOS Enable P
fef800b0 : 61 73 73 77 6f 72 64 20 3d 20 0d 0a 4e 53 4f 53 assword = ..NSOS
fef800c0 : 20 52 6f 6f 74 20 50 61 73 73 77 6f 72 64 20 3d  Root Password =
fef800d0 : 20 61 6d 6a 5f 0d 0a 00 ff ff ff ff ff ff ff ff  amj_........
fef800e0 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef800f0 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef80100 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef80110 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef80120 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
=>
```

Example: ENABLE and EXEC Passwords

```
=> db fef80030 100
fef80030 : 5b 5b 20 49 50 20 52 6f 75 74 69 6e 67 20 3d 20 [[ IP Routing =
fef80040 : 53 65 63 74 69 6f 6e 20 53 74 61 72 74 20 5d 5d Section Start ]]
fef80050 : 0d 0a 49 50 20 50 6f 72 74 20 41 64 64 72 65 73 ..IP Port Addres
fef80060 : 73 20 3d 20 30 30 2c 20 31 37 31 2e 36 38 2e 39 s = 00, 171.68.9
fef80070 : 2e 31 0d 0a 5b 5b 20 43 42 4f 53 20 3d 20 53 65 .1..[[ CBOS = Se
fef80080 : 63 74 69 6f 6e 20 53 74 61 72 74 20 5d 5d 0d 0a ction Start ]]..
fef80090 : 4e 53 4f 53 20 50 72 6f 6d 70 74 20 3d 20 75 73 NSOS Prompt = us
fef800a0 : 61 0d 0a 4e 53 4f 53 20 52 6f 6f 74 20 50 61 73 a..NSOS Root Pas
fef800b0 : 73 77 6f 72 64 20 3d 20 61 6d 6a 5f 0d 0a 4e 53 sword = amj_..NS
fef800c0 : 4f 53 20 45 6e 61 62 6c 65 20 50 61 73 73 77 6f OS Enable Passwo
fef800d0 : 72 64 20 3d 20 61 6d 6a 5f 0d 0a 00 ff ff ff ff rd = amj_.......
fef800e0 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef800f0 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef80100 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef80110 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
fef80120 : ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ................
```

The passwords are now recovered.

5. Reboot the Cisco CPE by turning it off then on again, or by typing **rb** at the `=>rb` prompt, and type the password you recovered.

```
=>rb
```

```
Hello!
Expanding CBOS image...
CBOS v2.3.5.012 − Release Software

User Access Verification
Password:

usa>
```

Password recovery is now complete.

Erasing the Configuration

If the Cisco CPE is not functioning properly, you may need to reconfigure it, but you must first erase the existing configuration.

 **Caution:** All settings are lost when you erase the configuration.

- To erase the configuration while in RMON mode, see the example shown below.

  Important: This procedure reboots a Cisco 6xx CPE with no configuration. You will need to reconfigure the CPE and then use the **write** command to save the changes to nonvolatile RAM (NVRAM).

  ```
  =>es 6

  Erasing sector 00000006...
  Sector erased

  =>rb

  Hello!
  CBOS v2.0.1.01
  ```

- To erase the configuration while in normal operating mode:

  1. Log in.
  2. Enter `enable` mode using the following commands:
     ```
     set nvram erase
     write
     reboot
     ```
  3. Type **`rb`** to reboot the Cisco CPE in normal mode.

MD5 Encryption and CBOS Versions 2.3.9 and Later

CBOS versions 2.3.9 and later have MD5 password encryption enabled by default. This section contains important information regarding MD5 password encryption.

If you are upgrading from a previous release of CBOS and were not using passwords, you will not need to use passwords. If you are upgrading and were using passwords, CBOS versions 2.3.9 and later will encrypt those passwords and save them to NVRAM. No change is visible to the end user.

Disabling Encryption

To disable encryption, type the command **set password encryption disable**. CBOS will return the statement "MD5 password encryption Disabled." Since the old passwords cannot be recovered, the ENABLE and EXEC passwords have been cleared. To assign new passwords, use the command line interface commands. You must type "write" to persist encryption mode into memory and then issue the **write** command to make the change permanent. You can then add passwords, but they will not be encrypted.

Enabling Encryption

To enable encryption, type the command **set password encryption enable**. CBOS will return the statement "MD5 password encryption Enabled." You must type "write" to persist encryption mode into memory and then issue the **write** command to make the change permanent.

 **Caution:** If you forget an encrypted password, you must follow the instructions above in the "Erasing the Configuration" section. Remember that all settings stored in memory are lost. The current configuration will be erased and you will need to reconfigure the Cisco CPE for it to be operational again.

Related Information

- **Password Recovery Procedures Index**