Password Recovery Procedure for the Cisco 600 Series Customer Premises Equipment

Document ID: 12820

Introduction

This document describes how to recover the ENABLE and EXEC passwords on Cisco 600 Series Customer Premises Equipment (CPE) Routers with the Cisco Broadband Operating System (CBOS) earlier than version 2.3.9.

Note: This password recovery procedure does not work for CBOS 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.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these hardware and software versions:

- Cisco 600 Series Customer Premises Equipment (CPE) Routers
- Cisco Broadband Operating System earlier than version 2.3.9

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

Refer to Password Recovery Procedures for information on how to recover passwords for related products.

Conventions

Refer to Cisco Technical Tips Conventions for information on document conventions.

Password Recovery

Follow these steps in order to recover your password:

1. Set up console access.

   Note: If you do not have a management cable, refer to Making a Management Cable for the Cisco 600 Series CPE for information on how to make one.

   a. Use the serial cable supplied with the modem in order to connect a COM port on your PC to the management port on the modem.
   b. Configure a terminal access program, such as Windows HyperTerminal, with these settings:

      ◊ COM port: The 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, you might see one of these prompts: `cbos>, modem1>,` or `usa>`

   Once the prompt appears, communication is established between the PC and Cisco CPE.
2. Disconnect and then reconnect the AC power plug on the back of the Cisco CPI in order to powercycle the unit.

   Note: ***Immediately*** after you reconnect the power plug, press and hold the **Ctrl−C** keys on the keyboard until you see this message:

   ```
   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 you can release the **Ctrl−C** keys.
3. Execute the **db fef80030** <***# of bytes***> command in order to view the configuration file.

   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 ................
```

Note: You must assign an ENABLE password when you configure the Cisco CPE if you want the password to display as encrypted while you complete the recovery procedure. Otherwise, the enable password field is blank.

Note: If the EXEC password is set, then the root password field contains the EXEC password.

4. Locate your encrypted password in the output of the configuration file. The text of the password is altered by two letters.

   For example, the password in this example output is *amj_*. If you locate each character in the ASCII character set and then count two characters ahead, the *amj_* password is interpreted as *cola*. For a complete list of the ASCII characters, refer to 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: 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 recovered.

5. Turn off and then turn on the Cisco CPE in order to reboot. You can also type **rb** at the **=>** prompt, and then 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.

Erase the Configuration

You might need to reconfigure the Cisco CPE if it does not function properly. However, you must first erase the current configuration.

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

- In order to erase the configuration while in RMON mode, use this example:

```
=>es 6

Erasing sector 00000006...
```

```
Sector erased

=>rb

Hello!
CBOS v2.0.1.01
```

Important: This procedure reboots a Cisco 600 CPE with no configuration. You must reconfigure the CPE, and then use the **write** command in order to save the changes to nonvolatile RAM (NVRAM).

- In order to erase the configuration while in normal operating mode, complete these steps:

1. Log in.
2. Use this command in order to enter enable mode.

```
set nvram erase
write
reboot
```

3. Type **rb** in order 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 upgrade from a previous release of CBOS and did not use passwords, you will not need to use passwords. If you upgrade and did use passwords, CBOS versions 2.3.9 and later encrypt those passwords and save them to NVRAM. No change is visible to the end user.

Disable Encryption

In order to disable encryption, type the **set password encryption disable** command. CBOS displays this statement:

```
MD5 password encryption Disabled
```

Since the old passwords cannot be recovered, the ENABLE and EXEC passwords have been cleared. In order to assign new passwords, use the command line interface commands. You must type **write** in order to persist encryption mode into memory and then issue the **write** command in order to make the change permanent. You can then add passwords, but they will not be encrypted.

Enable Encryption

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

Caution: If you forget an encrypted password, you must follow the instructions described in Erase the Configuration. Remember that all settings stored in memory are lost. The current configuration is erased, and you must reconfigure the Cisco CPE for it to be operational again.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Router and IOS Architecture
Network Infrastructure: LAN Routing and Switching
Network Infrastructure: WAN Routing and Switching

Related Information

- **ASCII Character Set**
- **Password Recovery Procedures**
- **Making a Management Cable for the Cisco 600 Series CPE**
- **Technical Support − Cisco Systems**

Updated: Jan 04, 2007 Document ID: 12820