

Table of Contents

Password Recovery Procedure for the Cisco 2000, 2500, 3000, 4000, AccessPro, 7000 (RP), AGS, IGS, STS–10x.....1

Document ID: 12722.....1

Introduction.....1

Prerequisites.....1

Requirements.....1

Components Used.....1

Conventions.....2

Step-by-Step Procedure.....2

Sample Output.....3

Example for Enable Password Recovery.....6

Example for Password Replacement.....7

NetPro Discussion Forums – Featured Conversations.....10

Related Information.....10

Password Recovery Procedure for the Cisco 2000, 2500, 3000, 4000, AccessPro, 7000 (RP), AGS, IGS, STS-10x

Document ID: 12722

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Step-by-Step Procedure

- Sample Output

- Example for Enable Password Recovery

- Example for Password Replacement

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes the procedure to recover an **enable password** or **enable secret password**. These passwords are used to protect access to privileged EXEC and configuration modes. The **enable password** can be recovered. However, the **enable secret password** is encrypted, and can only be replaced with a new password, for which this document provides the procedure.

The **enable password** or the **enable-secret password** is stored in the startup-configuration file in the nonvolatile RAM (NVRAM). The password recovery procedure involves booting the router while ignoring the startup-configuration file in the NVRAM. To achieve this, set the 6th bit in the configuration register. The router then boots with the default configuration and all the interfaces in "shutdown" state. Since the default configuration does not have a password, anyone can now enter the *enable mode* on the router. To get back the original configuration of the router, the startup-configuration file can be copied into the router memory. If you are already in the enable mode, you can either view or change the **enable password**, but can only change the **enable secret password**, because it is always encrypted in the **show** commands. This document details this procedure.

Prerequisites

Requirements

Before you use the information in this document, see Possible Key Combinations for Break Sequence During Password Recovery. You should also be aware of concepts related to loading the Cisco IOS® Software such as, ROM monitor (ROMmon), bootflash, and the configuration register values.

Components Used

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

- Cisco IOS Software Release 12.2(10b).

- Cisco 2500 Series Router.

Note: Although a Cisco 2500 Series Router is used as an example in this document, the password recovery procedure presented here applies to all the platforms listed above.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Step-by-Step Procedure

Complete these steps to recover a lost or forgotten password:

1. Attach a terminal or PC with terminal emulation to the console port of the router. Use these terminal settings:

```
9600 baud rate
No parity
8 data bits
1 stop bit
No flow control
```

The required console cable specifications are described in the Cabling Guide for RJ-45 Console and AUX Ports (Cisco 1000 Series, 2500 Series, and AS5100).

If you still have access to the router, enter the **show version** command, and record the setting of the configuration register; it is usually 0x2102 or 0x102.

For a sample output of a **show version** command, see the Sample Output section.

If you do not have access to the router (because of a lost login or TACACS password), you can safely assume that your configuration register is set to 0x2102.

Note: Password recovery procedures cannot be done through telnet connections.

2. Turn the power switch of the router off, and then turn it back on.
3. Send a break sequence from the terminal keyboard within 60 seconds of the power-up to put the router into ROMmon. The break sequence depends on your Operating System or Terminal Emulator. See Standard Break Key Sequence Combinations During Password Recovery for different key combinations.
4. Type **o** and press ENTER at the > prompt, and record the current value of the configuration register (usually 0x2102, or 0x102):

```
>o
```

```
!--- Shows the configuration register option settings.
```

```
Configuration register = 0x2102 at last boot
Bit#      Configuration register option settings:
15        Diagnostic mode disabled
```

```
!--- Output suppressed.
```

5. Type **o/r 0x2142** and press ENTER at the > prompt to boot from Flash without loading the

configuration.

6. Type **i** at the > prompt and press ENTER.

The router reboots, but ignores its saved configuration.

7. Type **no** after each setup question or press CTRL + C to skip the initial setup procedure.
8. Type **enable** at the Router> prompt.

You will be in enable mode, and see the Router# prompt.

9. Type **configure memory** or **copy startup-config running-config** to copy the NVRAM into memory. Do *not* type **write memory** or **copy running startup-config**.
10. Type **write terminal** or **show running-config**.

The **show running-config** and **write terminal** commands show the configuration of the router. In this configuration you see under all the interfaces the **shutdown** command, which means all interfaces are currently shutdown. Also, you can see the passwords either in encrypted or unencrypted format.

11. Type **configure terminal** and make the changes.

The prompt is now:

```
hostname(config)#
```

12. Type **enable secret <password>** to change the **enable secret password**, for example..
13. Issue the **no shutdown** command on every interface that is used. If you issue a **show ip interface brief** command after you exit configuration mode, every interface that you want to use should be "up".
14. Type **config-register 0x2102**, or the value you recorded in step 4.

This causes the router to load the Cisco IOS software from the Flash with the configuration from NVRAM at the next reload.

15. Press CTRL + Z to leave the configuration mode.

The prompt is now:

```
hostname#
```

16. Type **write memory** or **copy running-config startup-config** to commit the changes.
17. Type **Reload** to restart the router with the Cisco IOS software booting from the Flash.

Sample Output

The example below presents an actual password recovery procedure. We created this example using a Cisco 2500 series router. Even if you do not use a Cisco 2500, the example shown here will be almost similar to what you experience on your product.

```
Router>enable
Password:
Password:
Password:
% Bad secrets
Router>show version
```

```
Cisco Internetwork Operating System Software
```

```
IOS (tm) 2500 Software (C2500-JS-L), Version 12.2(24a)
RELEASE SOFTWARE (fc3)
```

```
Copyright (c) 1986-2004 by cisco Systems, Inc.
```

Compiled Fri 28-May-04 19:30 by pwade

Image text-base: 0x0306C4E0, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-B00T-R), Version 11.0(10c),
RELEASE SOFTWARE (fc1)Router uptime is 5 minutes
System returned to ROM by power-on
System image file is "flash:/c2500-js-l.122-24a.bin"

cisco 2500 (68030) processor (revision D) with 14336K/2048K bytes of memory.

Processor board ID 02315272, with hardware revision 00000000

Bridging software.

X.25 software, Version 3.0.0.

SuperLAT software (copyright 1990 by Meridian Technology Corp).

TN3270 Emulation software.

1 Ethernet/IEEE 802.3 interface(s)

1 Token Ring/IEEE 802.5 interface(s)

2 Serial network interface(s)

32K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

!--- This is the current value of the configuration register.

Router>

*!--- The router was just power cycled and during bootup a
!--- break sequence was sent to the router.*

System Bootstrap, Version 11.0(10c), SOFTWARE
Copyright (c) 1986-1996 by cisco Systems
2500 processor with 16384 Kbytes of main memory

Abort at 0x10EA83C (PC)

>0

Configuration register = 0x2102 at last boot

*!--- You can also view the configuration register settings value
!--- by issuing the command "0" in the ROMmon prompt.*

Bit#	Configuration register option settings:
15	Diagnostic mode disabled
14	IP broadcasts do not have network numbers
13	Boot default ROM software if network boot fails
12-11	Console speed is 9600 baud
10	IP broadcasts with ones
08	Break disabled
07	OEM disabled
06	Ignore configuration disabled
03-00	Boot file is cisco2-2500 (or 'boot system' command)

>o/r 0x2142

*!--- Changes the value of config-register to 2142, so that the Router boots,
!--- and ignores the NVRAM contents.*

>i

*!--- Initializes or resets the router; the
!--- Router boots with the default configuration.*

System Bootstrap, Version 11.0(10c), RELEASE SOFTWARE
Copyright (c) 1986-1996 by cisco Systems
2500 processor with 8192 Kbytes of main memory
F3: 13626872+197596+780568 at 0x3000060

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco Internetwork Operating System Software

IOS (tm) 2500 Software (C2500-JS-L), Version 12.2(24a),
RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.

Compiled Fri 28-May-04 19:30 by pwade

Image text-base: 0x0306C4E0, data-base: 0x00001000

cisco 2500 (68030) processor (revision D) with 14336K/2048K bytes of memory.

Processor board ID 02315272, with hardware revision 00000000

Bridging software.

X.25 software, Version 3.0.0.

SuperLAT software (copyright 1990 by Meridian Technology Corp).

TN3270 Emulation software.

1 Ethernet/IEEE 802.3 interface(s)

1 Token Ring/IEEE 802.5 interface(s)

2 Serial network interface(s)

32K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read ONLY)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

!--- Ctrl+C pressed.

!

Press RETURN to get started!

00:00:08: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up

00:00:08: %LINK-3-UPDOWN: Interface Serial0, changed state to up

00:00:08: %LINK-3-UPDOWN: Interface Serial1, changed state to up

00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to up

00:00:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1,
changed state to up

00:01:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0,
changed state to up

00:01:29: %LINK-3-UPDOWN: Interface Ethernet0Translating "Router"...
domain server (255.255.255.255), changed state to up

00:01:30: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1,
changed state to up

00:01:31: %SYS-5-RESTART: System restarted --

```
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.2(24a),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Fri 28-May-04 19:30 by pwade
00:01:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to down
00:01:33: %LINK-5-CHANGED: Interface Ethernet0, changed state to
```

administratively down

```
00:01:33: %LINK-5-CHANGED: Interface Serial0, changed state to
```

administratively down

```
00:01:33: %LINK-5-CHANGED: Interface Serial1, changed state to
```

administratively down

```
00:01:33: %LINK-5-CHANGED: Interface TokenRing0, changed state to
```

administratively down

```
00:01:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0,
changed state to down
```

```
00:01:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1,
changed state to down
```

```
00:01:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface TokenRing0,
changed state to down
```

```
Router>enable
```

```
Router#copy startup-config running-config
```

```
Destination filename [running-config]?
```

!--- Press ENTER.

```
1278 bytes copied in 10.448 secs (127 bytes/sec)
```

Note: After you copy the configuration file from NVRAM to RAM, based on how the password is last configured, you can:

- Either perform a password recovery, if the **enable password** is configured (which is in plain text format).
- Or, perform a password replacement, if the **enable secret password** is configured (which is in encrypted format).

Note: To check the format in which the password is configured on the router, use the **show running-config** command, and look for **enable password** or **enable secret password** in the configuration.

Example for Enable Password Recovery

The following **show running-config** output shows that **enable password** is configured. Password recovery can be done as shown below:

```
Router#show running-config
```

!--- This command can be used to view the unencrypted password.

```
Building configuration...
```

```
Current configuration : 431 bytes
```

```
!
```

```
version 12.2
```

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable password XxXxXx

```

*!--- Here the Password is **plain clear text**. We can either maintain
!--- the same password or replace with a new password for security reasons.*

!--- Output Suppressed.

Example for Password Replacement

The following output from a **show running-config** shows that the **enable secret password** is configured. As a result, password replacement can be performed as shown below:

```

Router#show running-config
Building configuration...
Current configuration : 835 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable secret 5 $1$0ea234/6Ppi0PZYzAj/vX0

```

!--- Password replacement has to be done as the password is in encrypted format.

!--- Output suppressed.

```

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret xxxxxxxx
Router(config)#
00:03:39: %SYS-5-CONFIG_I: Configured from console by console

```

When the password recovery or replacement is done, the remaining steps are the same, as shown below:

```

Router#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	10.3.4.4	YES	TFTP	administratively down	down
Serial0	172.16.1.4	YES	TFTP	administratively down	down
Serial1	192.168.1.4	YES	TFTP	administratively down	down
TokenRing0	unassigned	YES	TFTP	administratively down	down

```

Router(config)#interface ethernet 0
Router(config-if)#no shutdown
*Mar 1 00:04:12.863: %LINK-3-UPDOWN: Interface Ethernet0,
changed state to up

```

```

*Mar 1 00:04:13.947: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0,
changed state to up
Router(config-if)#interface serial 0
Router(config-if)#no shutdown
*Mar 1 00:04:18.107: %LINK-3-UPDOWN: Interface Serial0,
changed state to up
*Mar 1 00:04:19.167: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to up
Router(config-if)#interface serial 1
Router(config-if)#no shutdown
Router(config-if)#
*Mar 1 00:04:27.055: %LINK-3-UPDOWN: Interface Serial1,
changed state to up
*Mar 1 00:04:28.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1,
changed state to up #
Router(config-if)#^Z
Router#
00:02:35: %SYS-5-CONFIG_I: Configured from console by console
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

After you have recovered or replaced the password we have to reset the Configuration register value to 0x2102, which was earlier changed to 0x2142 to ignore the Start-up configuration, and to boot the Router. You can verify the configuration register value. To do so, issue the **show version** command.

```

Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.2(24a)RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 28-May-04 19:30 by pwade
Image text-base: 0x0306C4E0, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-B00T-R), Version 11.0(10c),
RELEASE SOFTWARE (fc1)

Router uptime is 5 minutes
System returned to ROM by power-on
System image file is "flash:/c2500-js-l.122-24a.bin"

cisco 2500 (68030) processor (revision D) with 14336K/2048K bytes of memory.
Processor board ID 02315272, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Ethernet/IEEE 802.3 interface(s)
1 Token Ring/IEEE 802.5 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2142

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#config-register 0x2102

```

```

!--- The config-register is changed back to load the router
!--- with NVRAM configuration.

```

```
Router(config)#^Z
00:03:20: %SYS-5-CONFIG_I: Configured from console by console
```

When you issue the **config-reg 0x2102** command, the new configuration register value does not take effect immediately. The new value will be effective only after the router is reloaded. The **show version** command shows the current value (0x2142), and the value that will be effective after the next reload (0x2102).

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.2(24a)RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 28-May-04 19:30 by pwade
Image text-base: 0x0306C4E0, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-B00T-R), Version 11.0(10c),
RELEASE SOFTWARE (fc1)

Router uptime is 5 minutes
System returned to ROM by power-on
System image file is "flash:/c2500-js-l.122-24a.bin"

cisco 2500 (68030) processor (revision D) with 14336K/2048K bytes of memory.
Processor board ID 02315272, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Ethernet/IEEE 802.3 interface(s)
1 Token Ring/IEEE 802.5 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2142 (will be 0x2102 at next reload)

Router#
```

After you save the configuration, reload the router, and verify the configuration register value is 0x2102, as shown here:

```
Router#write memory
*Mar  1 00:05:09.035: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...
[OK]
Router#
Router#reload
Proceed with reload? [confirm]

!--- Press Enter to continue.

!--- Starts to load the Cisco IOS from Flash,
and takes the configuration from the NVRAM.

00:17:36: %SYS-5-RELOAD: Reload requested by console.

System Bootstrap, Version 11.0(10c), SOFTWARE
Copyright (c) 1986-1996 by cisco Systems
2500 processor with 14336 Kbytes of main memory
```

F3: 15011856+968960+947120 at 0x3000060

!--- Output suppressed.

Router#**show version**

Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.2(24a)RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 28-May-04 19:30 by pwade
Image text-base: 0x0306C4E0, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-B00T-R), Version 11.0(10c),
RELEASE SOFTWARE (fc1)

Router uptime is 5 minutes
System returned to ROM by reload
System image file is "flash:/c2500-js-l.122-24a.bin"

cisco 2500 (68030) processor (revision D) with 14336K/2048K bytes of memory.
Processor board ID 02315272, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Ethernet/IEEE 802.3 interface(s)
1 Token Ring/IEEE 802.5 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)
Configuration register is **0x2102**

Router#

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

- **Standard Break Key Sequence Combinations During Password Recovery**
- **Technical Support – Cisco Systems**

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Oct 01, 2004

Document ID: 12722

