

ery Procedure for the Cisco 2000, 2500, 3000, 4000, AccessPro,

Table of Contents

<u>Password Recovery Procedure for the Cisco 2000, 2500, 3000, 4000, AccessPro, 7000 (RP), AGS, IGS, STS-10x</u>	1
<u>Introduction</u>	1
<u>Before You Begin</u>	1
<u>Conventions</u>	1
<u>Overview</u>	1
<u>Prerequisites</u>	2
<u>Hardware and Software Versions</u>	2
<u>Step-by-Step Procedure</u>	2
<u>Sample Output</u>	3
<u>Related Information</u>	7

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

Introduction

Before You Begin

Conventions

Overview

Prerequisites

Hardware and Software Versions

Step-by-Step Procedure

Sample Output

Related Information

Introduction

This document describes the password recovery procedure for the following Cisco products:

- Cisco 2000
- Cisco 2500
- Cisco 3000
- Cisco 4000
- Cisco AccessPro
- Cisco 7000 (RP)
- Cisco AGS
- Cisco IGS
- Cisco STS-10x

Before You Begin

Conventions

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

Overview

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. This can be achieved by setting 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 and 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

Before using 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.

Hardware and Software Versions

The information in this document is based on the following versions:

- Cisco IOS Software Release 12.2(10b)
- 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.

Step-by-Step Procedure

Follow this procedure to recover a lost or forgotten password:

1. Attach a terminal or PC with terminal emulation to the console port of the router. Use the following 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).

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

2. Using the power switch, turn 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/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
.....
```

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'll 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>**.
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 sample output shown here is the result of the password recovery procedure on a Cisco 2500 Series Router.

```
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(10b)
RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Fri 12-Jul-02 02:13 by pwade

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

ROM: System Bootstrap, Version 11.0(10c), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a),
RELEASE SOFTWARE (fc1)Router uptime is 5 minutes
```

System returned to ROM by power-on
System image file is "flash:/c2500-js-1.122-10b"

cisco 2500 (68030) processor (revision D) with 8192K/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 config-register.

Router>

*!--- The router was just powercycled 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)

>o/r 0x2142

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

>i

*!--- Initializes or resets the router; the
!--- Router is booting 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(10b),
RELEASE SOFTWARE (fcl)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Fri 12-Jul-02 02:13 by pwade
Image text-base: 0x0306C4E0, data-base: 0x00001000
cisco 2500 (68030) processor (revision D) with 8192K/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(10b),
RELEASE SOFTWARE (fcl)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Fri 12-Jul-02 02:13 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)
```

```
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 secret 5 $1$zRZR$NhWuILiIqlVzow/z/.Fe30
```

```
!--- This is the 'enable-secret' password which is being replaced.
```

```
ip subnet-zero
!
interface Ethernet0
no ip address
shutdown
!
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown .....
```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#enable secret Cisco
```

```
!--- Cisco is the 'enable-secret' password
```

```
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)#exit
Router(config)#config-register 0x2102

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

Router(config)#^Z
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 loading the Cisco IOS from Flash,
taking the configuration from the NVRAM.

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

System Bootstrap, Version 11.0(10c), SOFTWARE.....
```

Related Information

- [Password Recovery Procedures Index](#)
 - [Technical Support – Cisco Systems](#)
-

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.