第22章　Cisco 密码修复

本章主题

- Cisco密码修复概述
- 理解Cisco配置寄存器
- 在Cisco 3600上的密码修复
- 在Cisco 2500上的密码修复
- 在Catalyst 交换机上的密码修复

22.1　引言

本章将详细介绍关于在 Cisco路由器和Catalyst交换机上对丢失和未知密码进行修复的方法，同时将给出Cisco 2500，3600及Catalyst 5000上的密码修复指令。

22.1.1　密码修复概述

一个Cisco路由器要经历一个预定义的顺序的启动过程，在加电检测和装载 IOS映像之后，路由器会在NV内存寻找它的配置指令，这些指令不仅包括路由协议和地址信息，而且包括路由器的登录信息。

密码修复包括告诉路由器在启动过程中忽略 NV内存中的内容，可以通过修改位于路由器NV内存中的16位的配置寄存器来完成这项工作，这样将导致路由器装载一个不包含任何登录密码的空白配置，使用者就可以查看 NV内存配置中的密码，并决定是使用、删除还是修改它们，路由器然后就可用注册的密码重启了。

密码修复技术依路由器种类而不同，但从总体上来看，大多数是下列格式：

- 连接一个终端到路由器的控制端口。
- 如果路由器已经加电，就断电并再次加电，如果是断电的，则对它加电。
- 当引导路由器时，必须插入引导过程并置路由器于监督模式之下。
- 在监督模式下，重新启动路由器而不读取 NV内存中的配置。
- 重载路由器。
- 不读取NV内存而对路由器重载之后，就不存在任何特权和非特权密码了，进入特权方式，或者浏览或者修改或者删除 NV内存密码。
- 进入配置模式并从NV内存引导路由器。
- 重载路由器，现在的密码是已知的。

22.1.2　配置寄存器

Cisco路由器有一个称为虚拟配置登记表的 16位寄存器，它驻留在NV内存中，并被用来设置路由器的几项基本特征，例如：

- 使路由器忽略NV内存中的内容。

- 设置控制台波特速率。
- 设置IPF广播包格式。
- 配置路由器从ROM、闪存启动或是使用启动配置来决定路由器IOS映像的装载位置。

前述表中的第一个表项导致路由器忽略NV内存中的内容。

配置登记表中的16位值常用16进制格式表述，并写成OXVALUE，VALUE为登记表的设置，例如，我们将看到一个典型的配置值为ox2102。

图22-1显示了一个Cisco 3600路由器的虚拟登记表各位值的意义。

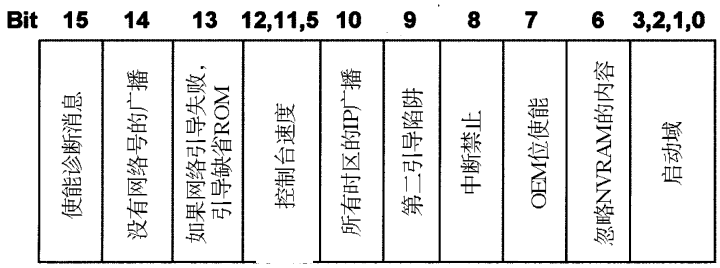


图22-1 Cisco 3600 配置寄存器

让我们看一下Cisco 3600虚拟配置登记表中的一些关键域，并审查一下它们的一些可能值。

(1) Bit 0-3 —— 引导域

这四位决定了路由器将重载入ROM监督模式，是从闪存的第一份映像引导还是从位于NV内存中的配置中获取映像装载指令。

(2) Bit 6 —— 忽略NV内存

当第6位被设为1时，路由器将忽略NV内存中的内容，当进行密码修复时将该位设为1。

(3) Bit 8 —— 不允许打断

将这位设为1则使得路由器忽略break键。

(4) Bit 5 & 11 & 12 —— 控制台速度

这三位决定了路由器控制台的速度， 3600控制台端口的默认值为9600b/s，但可以在1200~115200b/s的区间操作。

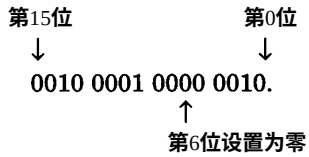
22.1.3 解释配置寄存器

让我们来一起看一下一个典型的配置寄存器值ox2102，并回忆一下如何将它变成二进制值，图22-2包含一个十六进制到二进制的转换表。

将十六进制值0x2102变为一个二进制是个简单的练习，十六进制寄存器值的每一位被转变为4个二进制位，值0x2102可一次转换一位，首位是2将变为0010，第二位1变为0001，第三位0变为0000，最后一位是2变为0010，将每位转换完毕，就可以产生一个十六位的值，该值为

十六进制	二进制
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

图22-2 十六进制到二进制的转换表



数一下各位数字，最右是第0位，最左是第15位。

从这个例子中可以看到第6位被设为0，意味着在路由器引导时NV内存中的内容将被忽略。

22.1.4 打断正常的路由器启动顺序

成功地修复一个丢失的或未知的密码的关键是能够打断正常的启动顺序并获得监督模式的入口，这可以通过在引导路由器时从仿真终端上发出一个中断信号来实现，两大流行仿真终端是Windows 95 HyperTerminal和ProComm，同时按下ALT+B键就可发出Procomm的中断序列，而在Windows 95 HyperTerminal中则要同时按下Ctrl+Break键。

22.2 本章所讨论的命令

- **show version**
- **show running-config**
- **show startup-config**
- **confreg**
- **reset**
- **config-register**
- **i**
- **o/r**
- **enable**
- **config term**
- **copy startup-config running config**
- **write erase**
- **reload**
- **set pass**
- **set enablepass**

命令的定义

- show version：用于显示系统硬件、IOS版本、配置文件、引导映像和配置寄存器内容的执行命令。
- show running-config：显示正在执行的配置的内容的执行命令。
- show startup-config：显示存在于NV内存中保存起来的配置内容的执行命令。
- confreg：用于浏览和改变配置表中内容的ROM监督命令。
- reset：用于在改变配置寄存器内容之后重载路由器的ROM监督命令，这个命令可用来细化某种Cisco模式型，例如3600。

- config-register：用于改变16位的配置寄存器内容的整体配置命令。
- i：用于在改变配置寄存器内容之后重载路由器的一个 ROM监督命令，这个命令可用来细化某种Cisco路由器，如2500系列。
- o/r：用于改变配置寄存器内容的 ROM监督命令，该命令可细化到某种 Cisco路由器，如2500系列。
- enable：用于使Cisco路由器或Catalyst交换机进入使能模式的执行命令。
- config term：用于进入路由器配置模式的执行命令。
- copy startup-config running config：用于复制存于NV内存中的配置到现在正在运行的配置中去的执行命令。
- write erase：抹去存于NV内存中的配置的执行命令。
- reload：用于重载IOS的执行命令。
- set pass：用于设置非使能密码的Catalyst交换机命令。
- set enablepass：用于设置使能密码的Catalyst交换机命令。

22.3 IOS需求

这些密码修复步骤可应用于IOS 10.0 及以后的所有的版本。

22.4 实验82：Cisco 3600密码修复

22.4.1 所需设备

执行本次试验要用到以下设备：

1) Cisco 3600系列路由器；
2) 运行一个仿真终端程序的PC，推荐使用Procomm或Windows Hyper Terminal；
3) 将PC连到路由器上的一根扁平电缆。

22.4.2 配置概述

这一部分将提供在Cisco 3600系列路由器上修复未知密码的详细指令，如图 22-3所示。

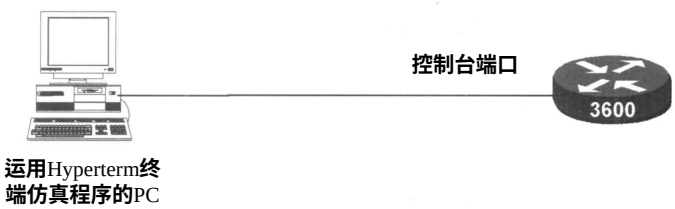


图22-3 Cisco 3600 密码修复

注意 在加电路由器之后迅即按下中断序列能导致路由器被锁住，在这种情况下，仅仅再次加电循环路由器，应等到路由器打印出描述其处理器类型和主存配置信息之后再按下中断序列。

同样，记住终端仿真程序使用不同的按键组合来产生中断序列，最流行的两大终端仿真器是Windows 95 Hyper Terminal 和Procomm，对于 Windows 95

HyperTerminal应同时按下Ctrl+Break来产生中断序列，而 Procomm则要同时按下ALT+B键。

密码修复只有在将终端连到路由器控制台端口的情况下才可被执行，这些步骤在路由器的辅助端口是行不通的。

22.4.3 密码修复步骤

在开始前，路由器应有一个使能密码和一个登录密码集，下面显示了使能和登录密码均设为Cisco的一个例子：

1. 路由器

```
Current configuration:
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Cisco3620
!
enable password cisco←Enable password.
!
no ip classless
!
line con 0
 password cisco←Login Password
 login
line aux 0
line vty 0 4
 login
!
end
```

下面用show version命令显示路由器的配置寄存器的值，可以看到其值为 0x2102。如前所述，这个值将导致路由器在启动过程中使用 NV内存中的配置文件。寄存器的值将在密码修复过程中被修改，从而导致路由器在启动过程中忽略 NV内存中的配置寄存器的内容。

```
Cisco3620#sh ver
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-I-M), Version 11.2(8)P, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Mon 11-Aug-97 19:50 by ccai
Image text-base: 0x600088E0, data-base: 0x6044A000

ROM: System Bootstrap, Version 11.1(7)AX [kuong (7)AX], EARLY DEPLOYMENT
RELEASE SOFTWARE (fc2)

Cisco3620 uptime is 1 minute
System restarted by reload
System image file is "flash:c3620-i-mz.112-8.P", booted via flash

cisco 3620 (R4700) processor (revision 0x81) with 12288K/4096K bytes of memory.
Processor board ID 05706480
R4700 processor, Implementation 33, Revision 1.0
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
DRAM configuration is 32 bits wide with parity disabled.
29K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
8192K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

```
Configuration register is 0x2102
```

密码修复过程中的第一步是加电循环路由器，关闭之后再加电，如果已处于关闭状态，则将它打开，在引导过程中的前几秒，可以看到如下内容将被显示：

```
System Bootstrap, Version 11.1(7)AX [kuong (7)AX], EARLY DEPLOYMENT RELEASE
SOFTWARE (fc2)
Copyright (c) 1994-1996 by cisco Systems, Inc.
C3600 processor with 16384 Kbytes of main memory
Main memory is configured to 32 bit mode with parity disabled←Press the break
                                                              sequence here.
```

这些信息显示之后，按下正确的中断序列，记住每个终端仿真程序有其自己的按键组合来强行中断，Procomm是ALT+B，Windows 95 HyperTerminal是Ctrl+Break，当正确的中断序列被按下之后，路由器将进入ROM监督方式：

```
monitor: command "boot" aborted due to user interrupt
```

在rommon提示下键入命令：confreg

```
rommon 1 >
rommon 1 > confreg
```

一个当前的配置统计就显示出来了，将有几个问题要你回答，对每一问应以正确的 yes或no回答，对“ Do you wish to change the configuration? ”,“ Ignore system config info？”及“ Change the boot characteristics ”回答yes，而对其它则答no。最后，敲一个2来使系统在启动时引导全部IOS映像。

```
     Configuration Summary
enabled are:
load rom after netboot fails
console baud: 9600
boot: image specified by the boot system commands
      or default to: cisco2-C3600
do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]:  n
enable  "use net in IP bcast address"? y/n  [n]:  n
disable "load rom after netboot fails"? y/n  [n]:  n
enable  "use all zero broadcast"? y/n  [n]:  n
enable  "break/abort has effect"? y/n  [n]:  n
enable  "ignore system config info"? y/n  [n]:  y
change console baud rate? y/n  [n]:  n
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [2]:  2
```

一个配置统计将被打印出，表明路由器现在将在启动时忽略系统配置信息（ NV内存）：

```
     Configuration Summary
enabled are:
load rom after netboot fails
ignore system config info
console baud: 9600
boot: image specified by the boot system commands
      or default to: cisco2-C3600
```

你会被再次问到是否要更改设置，这一次，回答 no。

```
do you wish to change the configuration? y/n  [n]:  n
```

路由器将显示出一条提示信息：必须重启才可以使更改生效，在监督提示下键入reset命令。

```
You must reset or power cycle for new config to take effect
rommon 2 >
rommon 2 > reset
```

路由器将重载，这次，它将忽略NV内存中的配置信息，当路由器引导结束后，就不存在控制密码或使能密码了，按下enter进入用户模式并键入enable来进入特权模式：

```
Press RETURN to get started!


Router>
Router>ena
Router#
```

使用show running-configuration命令来浏览一下路由器的现行配置，你将会发现配置中没有任何密码了，当路由器忽略了NV内存中的内容时，这种配置就产生了：

```
Current configuration:
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router
!
no ip classless
!
line con 0←No passwords
line aux 0
line vty 0 4
 login
!
end
```

密码修复的关键是能够查看、更改或删除包含在路由器正常启动配置中存储于NV内存中的密码。

查看：如果你想得到现在的密码并继续使用它，可以键入show startup-configuration命令，从下面的配置可以观察到控制台密码和使能密码都被设置为“cisco”，只有在密码未被加密时查看选项才可以用，否则，你就只能更改它或删除它。

```
Router#sh start
Using 355 out of 30712 bytes
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Cisco3620
!
enable password cisco←Enable password
!
no ip classless
!
line con 0
 password cisco←Login password
 login
line aux 0
line vty 0 4
 login
!
end
```

更改：要更改现行密码，需要复制NV内存配置到运行中的配置，可通过命令copy

startup-configuration running-configuration来完成这项任务，使用config term命令进入配置模式，键入新密码，完成之后可按下ctrl+Z退出配置模式，键入write mem将新密码保存到NV内存中。

删除：使用write erase命令可删除密码。

在重载之前的最后一步是将路由器配置寄存器中的值改为一个可以引起路由器从NV内存载入原始配置的值，现在的配置登记值可通过命令show version查看，在命令输入尾部可看到该值，在这种情况下，值ox2142将导致路由器忽略NV内存中的内容。

```
Router#sh ver
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-I-M), Version 11.2(8)P, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Mon 11-Aug-97 19:50 by ccai
Image text-base: 0x600088E0, data-base: 0x6044A000

ROM: System Bootstrap, Version 11.1(7)AX [kuong (7)AX], EARLY DEPLOYMENT
     RELEASE SOFTWARE (fc2)

Router uptime is 0 minutes
System restarted by power-on
System image file is "flash:c3620-i-mz.112-8.P", booted via flash

cisco 3620 (R4700) processor (revision 0x81) with 12288K/4096K bytes of memory.
Processor board ID 05706480
R4700 processor, Implementation 33, Revision 1.0
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
DRAM configuration is 32 bits wide with parity disabled.
29K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
8192K bytes of processor board PCMCIA Slot0 flash (Read/Write)
Configuration register is 0x2142
```

通过在命令提示下键入configure term就可更改路由器的配置寄存器中的值，使用config-register命令来进入新的配置值，在此例中，新的配置值是ox2102。

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

show version命令现在将显示新的设置，注意新设置只有在重载路由器之后才会生效。

```
Router#sh ver
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-I-M), Version 11.2(8)P, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Mon 11-Aug-97 19:50 by ccai
Image text-base: 0x600088E0, data-base: 0x6044A000

ROM: System Bootstrap, Version 11.1(7)AX [kuong (7)AX], EARLY DEPLOYMENT
     RELEASE SOFTWARE (fc2)

Router uptime is 1 minute
System restarted by power-on
System image file is "flash:c3620-i-mz.112-8.P", booted via flash

cisco 3620 (R4700) processor (revision 0x81) with 12288K/4096K bytes of memory.
Processor board ID 05706480
R4700 processor, Implementation 33, Revision 1.0
Bridging software.
```

```
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
DRAM configuration is 32 bits wide with parity disabled.
29K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
8192K bytes of processor board PCMCIA Slot0 flash (Read/Write)
Configuration register is 0x2142 (will be 0x2102 at next reload)
```

在router提示下键入reload命令来重载路由器并使新的注册值生效，不必保存新配置寄存器的更改。

```
Router#reload

System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]
```

现在路由器就被重载了，它将会从NV内存的内容中获取原始配置，现在路由器的密码是已知的了，并可用来进入特权模式。

22.5 实验83：Cisco 2500上的密码修复

22.5.1 设备需求

要运行本次试验练习将用到以下配置

1) Cisco 2500系列路由器；
2) 运行终端仿真程序的PC，推荐使用Procomm或Windows HyperTerminal；
3) 用于连接路由器和PC的Cisco扁平电缆。

22.5.2 配置概述

该部分将提供在一个Cisco 2500系列机路由器上修复一个未知密码的详细指导，如图22-4所示。

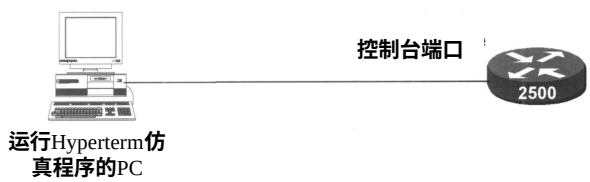


图22-4 Cisco 2500密码恢复

注意 在加电之后迅即接下中断序列将锁住路由器，在这种情况下，只要再次加电循环路由器即可。应等到路由器打印出描述其处理器类型和主存配置的信息之后再按下中断序列。

记住不同的终端仿真程序使用不同的按键组合来产生中断序列，两大不同的仿真终端是Windows 95 HyperTerminal和Procomm，要产生中断序列，在Procomm中应同时按下ALT+B键，在Windows 95 HyperTerminal中则要按下Ctrl+Break键。

注意 密码修复只能在连接到路由器控制台端口的终端上执行。在路由器的辅助端口，此过程不工作。

22.5.3 密码修复步骤

开始前，路由器应该有一个使能密码和登录密码集，下例显示了一个将它们均设为Cisco的配置实例：

1. 路由器

```
Current configuration:
!
version 11.0
service udp-small-servers
service tcp-small-servers
!
hostname Cisco2500
!
enable password cisco←Enable password
!
line con 0
 password cisco←Login password
 login
line aux 0
 transport input all
line vty 0 4
 login
!
end
```

下面的show version命令表明路由器的配置寄存器值被设为 ox2102，如前部分所述，该值将导致路由器在引导过程中使用 NV内存配置文件，该注册值也可在修复密码的过程中更改，并导致在引导过程中路由器将忽略NV内存配置文件中的内容。

```
Cisco2500#sh ver
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-D-L), Version 11.0(10), RELEASE SOFTWARE (fc3)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 05-Aug-96 18:19 by loreilly
Image text-base: 0x03025A14, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
ROM: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE
(fc1)
Cisco2500 uptime is 2 minutes
System restarted by reload
System image file is "flash:igs-d-1.110-10", booted via flash

cisco 2500 (68030) processor (revision A) with 4096K/2048K bytes of memory.
Processor board ID 01412484, with hardware revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102
```

密码修复过程的第一步是加电循环路由器，关上再打开，如果路由器已处于关闭状态，那么就打开它。在引导过程中的前几秒钟，你可以看到下面的信息被显示出：

```
System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
2500 processor with 4096 Kbytes of main memory←Press the break sequence here
```

这些信息显示完毕，按下正确的中断序列，记住每种终端仿真程序有各自的按键组合来强行一次中断，对于 Procomm是同时按下ALT+B键，而Windows 95 HyperTerminal则要同时按下Ctrl+Break键，当按下正确的中断序列之后，路由器将会进入监督模式：

```
Abort at 0x10EA838 (PC)
>
```

在>的提示下键入命令：o/r 0x42

```
>o/r 0x42
>
```

键入i来重新引导路由器

```
>
>i
```

路由器将重新加载。此时，它将忽略NV内存中包含的配置信息，当路由器结束引导之后，就不存在控制台密码或使能密码了，按下enter键进入用户模式，输入enable进入特权模式：

```
Press RETURN to get started!


Router>
Router>ena
Router#
```

使用show running-configuration命令来查看路由器的现行配置，就会发现配置中不存在任何密码，当路由器忽略了NV内存中的内容时就会产生此种配置：

```
Router#sh run


Building configuration...

Current configuration:
!
version 11.0
service udp-small-servers
service tcp-small-servers
!
hostname Router
!
line con 0←No passwords
line aux 0
 transport input all
line vty 0 4
 login
!
end
```

密码修复的关键是能查看、更改或删除存储于NV内存中路由器正常启动配置中的密码。

查看：如果想知道现在的密码并继续使用它，键入 show startup-configuration命令，从下列配置中，可注意到控制台密码和使能密码均被设为“ cisco ”，只有在密码未被加密时查看操作才可用，否则，就只能更改或删除它。

```
Router#sh start
Using 348 out of 32762 bytes
!
version 11.0
service udp-small-servers
service tcp-small-servers
!
hostname Cisco2500
!
enable password cisco←Enable password
!
line con 0
 password cisco←Login password
 login
line aux 0
 transport input all
line vty 0 4
```

```
 login
!
end
```

修改：欲更改当前密码，只需将 NV**内存中的配置复制到运行的配置中去，通过命令** copy startup-configuration running-configuration**即可完成，使用命令** config term**进入配置模式，键入新密码，完成之后，投下** ctrl+Z**键可退出该模式，键入** write mem**将新密码保存到** NV**内存中去。**

清除：使用命令 write erase**可删除密码。**

在重载之前的最后一步是将路由器配置寄存器中的值改为一个可以导致路由器从 NV**内存中装载其原始配置的值。使用命令** show version**可以查看配置寄存器的当前值，在命令输出的尾部会显示出该值，在本例中，值** 0x2142**导致路由器忽略了** NV**内存中的内容。**

```
Router#sh ver
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-D-L), Version 11.0(10), RELEASE SOFTWARE (fc3)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 05-Aug-96 18:19 by loreilly
Image text-base: 0x03025A14, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
ROM: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE
(fc1)

Router uptime is 1 minute
System restarted by power-on
System image file is "flash:igs-d-l.110-10", booted via flash

cisco 2500 (68030) processor (revision A) with 4096K/2048K bytes of memory.
Processor board ID 01412484, with hardware revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x42
```

在命令提示下键入 configure term**命令可以更改路由器的配置寄存器的值，使用命令** config-register**来键入新值，在本例中，新值为** 0x2102**。**

```
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#conf
Router(config)#config-register 0x2102
Router(config)#exit
```

命令show version**将显示新设置，注意该新设置只有在路由器重载之后才会生效。**

```
Router#sh ver
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-D-L), Version 11.0(10), RELEASE SOFTWARE (fc3)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 05-Aug-96 18:19 by loreilly
Image text-base: 0x03025A14, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
ROM: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE
(fc1)

Router uptime is 1 minute
```

```
System restarted by power-on
System image file is "flash:igs-d-l.110-10", booted via flash

cisco 2500 (68030) processor (revision A) with 4096K/2048K bytes of memory.
Processor board ID 01412484, with hardware revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x42 (will be 0x2102 at next reload)
```

在router提示符下键入命令reload来重载路由器，并从而导致新的配置寄存器值生效，不必保存新的配置寄存器值。

```
Router#reload

System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]
```

路由器现在将重载并从NV内存的内容中获取原始配置，现在密码我们已经知道，也就可用它来进入路由器的特权模式了。

22.6 实验84：Cisco Catalyst 5000密码修复

22.6.1 所需设备

要进行本次练习将用到以下配置：

1) 一台Cisco Catalyst 5000系列交换机；
2) 运行终端仿真程序的PC，推荐使用ProComm或Windows 95 HyperTerminal；
3) 连接交换机与PC的一条直缆。

22.6.2 配置概述

如图22-5所示，这一部分将提供有关修复Cisco Catalyst 5000系列交换机未知密码的详细指导。

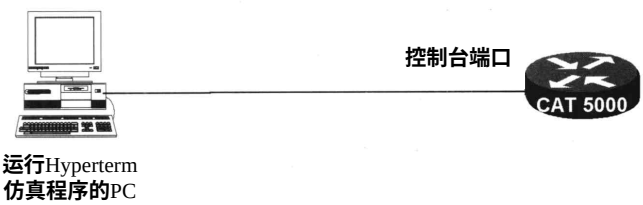


图22-5 Catalyst 5000 密码修复

注意 只有在附属于交换机控制台端口的终端上才可进行密码的修复，在Catalyst 5500上的Supervisor III既有控制端口又有辅助端口，只有在交换机的控制端口才可进行密码修复。

22.6.3 密码修复步骤

Catalyst交换机遵循一个与路由器不同的密码修复步骤，在交换机加电后并送出原始的系统登录提示后的前 30秒钟Catalyst交换机中的密码是不合法的，这种特征使得你只要在Password提示下按下Enter键就可获准进入交换机的，这种特征的缺陷是只有 30秒钟的时间来

获得入口权并更改密码，在30秒钟内更改两个系统密码是比较困难的。

针对这种情况，一种方法是将密码更改序列键入一个文本编辑器并将数据复制到剪贴板中去，当Catalyst交换机启动时，可以把这个序列粘贴到屏幕上并同时送出密码更改命令。

在密码修复过程中的第一步是加电循环交换机，关闭再打开，和路由器一样，必须连接到控制端口，如果交换机已处于关闭状态，那么就打开它，在启动过程中的前几秒，将会看到如下信息显示：

```
System Bootstrap, Version 3.1(2)
Copyright (c) 1994-1997 by cisco Systems, Inc.
Processor with 32768 Kbytes of main memory

Autoboot executing command: "boot bootflash:"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Uncompressing file:
##########################################################
###################################################################################
###################################################################################
###################################################################################
###################################################################################
###################################################################################
###################################################################################
#############################################################################
System Power On Diagnostics
NVRAM Size .. .................512KB
ID Prom Test .................Passed
DPRAM Size ...................16KB
DPRAM Data 0x55 Test ..........Passed
DPRAM Data 0xaa Test ..........Passed
DPRAM Address Test ............Passed
Clearing DPRAM ................Done
System DRAM Memory Size .......32MB
DRAM Data 0x55 Test ...........Passed
DRAM Data 0xaa Test ...........Passed
DRAM Address Test  ............Passed
Clearing DRAM .................Done
EARL++ ........................Present
EARL RAM Test .................Passed
EARL Serial Prom Test .........Passed
Level2 Cache ..................Present
Level2 Cache test..............Passed

Boot image: bootflash:cat5000-sup3.3-1-1.bin

Running System Diagnostics from this Supervisor (Module 2)
This may take up to 2 minutes....please wait
```

当下列控制信息出现时，按下Enter键登录到交换机，记住在接下来的30秒钟内，交换机密码未被设置，在密码提示下按下Enter键将可获得防问权限。

```
Cisco System Console←press the enter key when you see this message.
```

首次按下Enter键将使你进入交换机的非特权模式：

```
Console>
```

下面的序列要么在30秒的没有密码的阶段键入，要么粘贴到一个终端仿真屏，如果你想粘贴到屏幕上，就必须首先在将正确的密码更改脚本输入文本编辑器中，字符串可能如下所示：

```
Ena←ena is the Catalyst command for entering privileged mode. Follow this word
    by pressing enter twice.

set pass←set pass will cause the Catalyst to change the non-privileged mode
```

```
        password. Follow this command by pressing the Enter key four times.


set enablepass←set enablepass will cause the Catalyst to change the privileged
               mode password. Follow this command by pressing the Enter key
               four times.
```

在文本编辑器中产生这些字符串之后，做一个全选并复制信息到剪贴板中，当 Catalyst提示出现时，复制该文本序列到终端：

```
Console> ena
Enter password:
Console> (enable) set pass
Enter old password:
Enter new password:
Retype new password:
Password changed.
Console> (enable) set enablepass
Enter old password:
Enter new password:
Retype new password:
Password changed.
Console> (enable)
```

现在Catalyst的特权模式及非特权模式的密码均被设为 Enter键，Catalyst密码现在就可任意设了。

22.7 结论

本章提供了关于修复 Cisco路由器及Catalyst交换机上丢失或未知密码的详细信息，也看到在Cisco路由器上修复密码，包括获得路由器控制台入口及更改配置寄存器，以保证路由器在加电时忽略NV内存中的内容。

在Catalyst 5000系列的交换机上进行密码修复包括获得准进入 Catalyst控制台并能在交换机加电时的30秒内首次获得控制台入口通道。