

# How to use recover passwords (Cisco)

CIS Network & System Technology Lab  
September 2006

---

## Step-by-Step Password Recovery Instructions

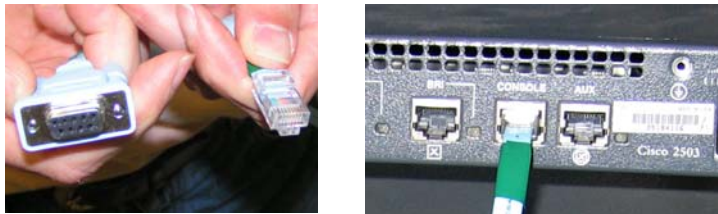
The passwords for a router are stored in the startup-config file in NVRAM. Recovering the password involves “breaking-in” during the router bootup process and configuring the configuration register so that the startup-config file is bypassed. This allows the router to start in an un-configured state with no password. From that point the network administrator has control again of the router and can both recover configuration information as well as reset the password

The instructions below apply to the Cisco router model 2503. For specific instructions relating to other routers models see:

<http://www.cisco.com/warp/public/474/>

Step 1 – Attach a PC console to the router

- Connect a flat rollover cable from the router’s console port to the Serial COM port on a PC that will act as the console.



- Insure TeraTerm terminal emulation software is installed on the console PC.  
<http://hp.vector.co.jp/authors/VA002416/teraterm.html>
- Configure TeraTerm to connect using the serial COM 1 port with 9600 baud, no parity, 8 databits, 1 stop bit, no flow control. Other COM ports can be used as well if COM 1 is not available.

Step 2 – Record current configuration register setting

- If you still have access to the router, enter a `show version` command and record the setting of the configuration register at the end of the version information:

```
Configuration register is 0x2102
```

We will use this later to restore the routers configuration register after changing it.

### Step 3 – Reboot and “break in” into the router.

- Note, if this is a production router you will need to schedule this operation accordingly and notify users the network will be down.
- Reboot - power off the router, then power it back on using the router’s power switch.
- Break in - send a break sequence within 60 seconds of powering on the router. With TeraTerm this is done by typing **Alt-b** (pressing alt and b keys at the same time)
- If you hit the **alt-b** enough times during the 60 second window you will enter ROMmon mode which looks as follows:

```
System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE  
Copyright (c) 1986-1995 by cisco Systems  
2500 processor with 8192 Kbytes of main memory  
  
Abort at 0x10EA82E (PC)  
>
```

If you don’t get into ROMmon mode the first time, keep rebooting and entering multiple Alt-b’s till you hit the right time window.

### Step 4 – In ROMmon mode, reconfigure router boot to bypass startup-config and reboot again

- Use the following commands to reset the configuration register and reboot:

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

- When the router comes up type `no` to the setup prompt or `ctrl-c`

```
--- System Configuration Dialog ---  
  
Would you like to enter the initial configuration dialog?  
[yes/no]: no
```

### Step 5 – Perform password recovery

- Enter privileged mode

```
Router>enable  
Router#
```

- Restore previous startup configuration:

```
Router#copy startup-config running-config
Destination filename [running-config]?
683 bytes copied in 4.784 secs (170 bytes/sec)
simms#
```

- Set new password:

```
simms#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
simms(config)#enable secret class
```

- Restore the configuration register to the value recorded in Step 2:

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

- Save new configuration (with reset password):

```
simms#copy running-config startup-config
```

- Verify configuration register change by issuing show version command and looking at the end of the output for the restored setting of the configuration register:

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

- Reboot the router now and check that your new password is correct.