Title:
Configuring Basic Cisco Router Security

Word Count:
407

Summary:
Basic Cisco router security is easy to configure, but is often overlooked. Chris Bryant, CCIE #12933, explains some basic steps you can take to protect your Cisco devices from unwanted access.

Keywords:
ccna, ccnp, free, pass, exam, cisco, certification, computer, mcse, ccie, chris, bryant

Article Body:
Network security is a hot topic today, and will only increase in importance in the months and years ahead.

While most of the attention is paid to exterior threats, there are some steps you can take to prevent unwanted Cisco router access from within your organization.

Whether you want to limit what certain users can do and run on your routers, or prevent unauthorized users in your company from getting to config mode in the first place, here are four important yet simple steps you can take to do so.

Encrypt the passwords in your running configuration.

This is a basic Cisco router security command that is often overlooked. It doesn’t do you any good to set passwords for your ISDN connection or Telnet

connections if anyone who can see your router's running configuration can see the passwords. By default, these passwords are displayed in your running config in clear text.

One simple command takes care of that. In global configuration mode, run service password-encryption. This command will encrypt all clear text passwords in your running configuration.

Set a console password.

If I walked into your network room right now, could I sit down and start configuring your Cisco routers?

If so, you need to set a console password. This password is a basic yet important step in limiting router access in your network. Go into line configuration mode with the command "line con 0", and set a password with the password command.

Limit user capabilities with privilege level commands.

Not everyone who has access to your routers should be able to do anything they want. With careful use of privilege levels, you can limit the commands given users can run on your routers.

Privilege levels can be a little clumsy at first, but with practice you'll be

tying your routers down as tight as you like. Visit www.cisco.com/univercd for documentation on configuring privilege levels.

Configure an “enable secret” password.

It’s not uncommon for me to see a router that has an enable mode password set, but it’s in clear text.

By using “enable secret”, the enable mode password will automatically be encrypted. Remember, if you have an enable password and enable secret password set on the same router, the enable secret password takes precedence.

These four basic steps will help prevent unwanted router access from inside your network. If only preventing problems from outside your network was as simple!