Video - Securing Access Methods (9 min)

One of the first things you'll want to do when installing a device on your network, like a Cisco series switch, is secure access to the device so only an administrator will be able to configure it or change its settings. To do this, we'll need to set some initial configuration settings to secure access. I'll click on the desktop PC and click on the terminal emulation program, and you can see that I now have a console connection to the switch.

For this video, I'll use the command line interface directly on the switch. As you can see, I'm logged into the switch in user exec mode without any authentication. This is a security risk. An even greater security risk is that I can type the enable command and get to privileged exec mode also without any type of authentication or password. From privileged exec mode, I can begin configuring the switch, so the first thing you'll want to do is secure access to privileged exec mode.

To do this, I'll go to global configuration mode and put in the command "enable secret" and then the password. You'll want to use complex strong passwords whenever possible. Since this is a test case scenario, I'll use the password "class." The "secret" parameter assures me that the password "class" will be encrypted in the configuration file. An alternative form of this command is "enable password class." This form of the command does not provide encryption for the password within the configuration file. So I'll backspace out of the command. Let's see if our enable secret password class has worked. I'll do a Ctrl+C to get to privileged exec mode and then exit the switch. Now I'll press Enter. I'm in privileged exec mode. I'll type "enable," and you can see I'm asked for the password. When I type the password in, you won't be able to see any characters as I type. I'll type in "class" and press Enter, and you can see that I'm now in privileged exec mode.

Let's take a look at our running configuration up to this point. We can do this by typing in the command "show running-config" to look at our running configuration. I'll press Enter, and you can see up here at the top, there's our "enable secret" command here. The 5 means that it's an MD5 hash, and this is a one-way hash of our password "class." So you can see how the "enable secret" command obfuscates the password within the configuration file. To see the rest of your configuration file, you press the space bar on your keyboard. Now we've encrypted the "enable password" or access to privileged exec mode, but what about access to simply consoling into the switch? We can secure that as well. To do that, I'll type "enable," the password "class," I'll get to global config mode with a "conf t" command, and I'll need to go into line configuration mode for line console 0. I'll type in "line console 0," and now I'm in line configuration mode. I can now put in a password for my console connection. I'll type in "password," and normally I would use a complex password, but for this demonstration, I'll simply use the password "cisco" and press Enter. I'll type in the "login" command, which enables global admin login at line console 0. Now that I've secured the console port, I'll also want to secure virtual terminal access for remote logins. I'll type in "line vty" for virtual terminal or virtual teletype, and then how many lines I want to allow remote access to. The Cisco switch is capable of 16 simultaneous remote logins through virtual terminals. To configure all 16, I simply type in 0 for the first terminal, a space, and then the last terminal that I want to configure. In this case, I'll put 15. This will allow me to configure virtual terminals 0 through 15. I'll put in "password cisco," and then the login command.

Let's take a look at these passwords in our running configuration. To do that, I'll do a Ctrl+C to get to privileged exec mode, and then put in the command "show run" which is short for "show running-config." I'll press the Tab key, and you can see the full command. So here's the running configuration file. I'll press the space bar and go down towards the bottom, and you can see there's the configurations for line con 0, line vty 0 to 4, and line vty 5 to 15. The IOS breaks up the virtual terminal lines into two groupings: 0 to 4, and 5 to 15. Notice the password "cisco" is seen in plain text. This is different than the "enable secret password," which has been encrypted through a one-way hash. We can add greater security to the switch if we can encrypt these passwords so that they're no longer visible in clear, plain text.

To do this, I'll go back to global figuration mode and put in the command "service password-encryption." This command will put a light level of encryption on all passwords on the switch. We can see this now if we go back to privileged exec mode, look at the running configuration file... I'll space-bar down to the bottom, and you can see that now the password "cisco" has been encrypted with a type 7 encryption. This is not a very strong form of encryption, but it does add a layer of security. Another important initial configuration command for securing access to the switch is setting a banner message. To do this, I'll go to global configuration mode and I'll type in the command "banner motd" for "message of the day." Now I could put in a message that will

be presented to users when they log in. This message will serve as a legal warning for unauthorized users informing them that they are trespassing, and legal action will be taken. I can now put in my security message. The message that I type will need to be between two delimiters. It's a good idea to use a delimiter that won't be a character within the message. For instance, I'll use quotation marks as delimiters for my message. In between the question marks, I'll put in the message "No unauthorized access allowed "violators will be prosecuted to the full extent of the law!" This lets any would-be hackers know that they're trespassing on a secure device or secure network and that this is a protected environment enforceable by law. I'll press Enter, and the banner is set. And now let's observe some of these security configurations. I'll do a Ctrl+C; type "exit" to leave the switch. I'll press Enter. Notice that I'm presented with the banner warning as well as a request for a password just to get access to the console. I'll put in the password "cisco," and now I'm in user exec mode. I'll type in "enable." I'm now asked for another password to reach privileged exec mode. I'll type in the password "class," and now I have full access to the switch.