Introduction to Networks v7.02

Basic Device Configuration

2.4.1

Device Names

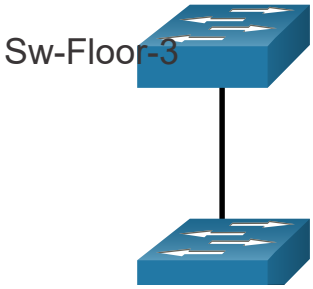
You have learned a great deal about the Cisco IOS, navigating the IOS, and the command structure. Now, you are ready to configure devices! The first configuration command on any device should be to give it a unique device name or hostname. By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."

The problem is if all switches in a network were left with their default names, it would be difficult to identify a specific device. For instance, how would you know that you are connected to the right device when accessing it remotely using SSH? The hostname provides confirmation that you are connected to the correct device.

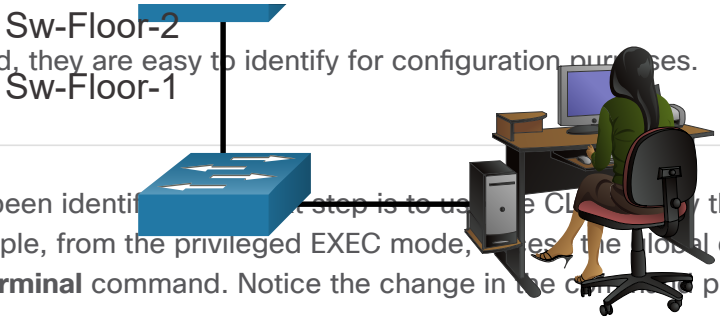
The default name should be changed to something more descriptive. By choosing names wisely, it is easier to remember, document, and identify network devices. Here are some important naming guidelines for hosts:

- Start with a letter
- Contain no spaces
- End with a letter or digit
- Use only letters, digits, and dashes
- Be less than 64 characters in length

An organization must choose a naming convention that makes it easy and intuitive to identify a specific device. The hostnames used in the device IOS preserve capitalization and lowercase characters. For example, the figure shows that three switches, spanning three different floors, are interconnected together in a network. The naming convention that was used incorporated the location and the purpose of each device. Network documentation should explain how these names were chosen so additional devices can be named accordingly.



When network devices are named, they are easy to identify for configuration purposes.



When the naming convention has been identified, the next step is to use the CLI to apply the names to the devices. As shown in the example, from the privileged EXEC mode, access the global configuration mode by entering the **configure terminal** command. Notice the change in the command prompt.

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

From global configuration mode, enter the command **hostname** followed by the name of the switch and press **Enter**. Notice the change in the command prompt name.

Note: To return the switch to the default prompt, use the **no hostname** global config command.

Always make sure the documentation is updated each time a device is added or modified. Identify devices in the documentation by their location, purpose, and address.

2.4.2

Password Guidelines

The use of weak or easily guessed passwords continues to be the biggest security concern of organizations. Network devices, including home wireless routers, should always have passwords configured to limit administrative access.

Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device.

All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.

When choosing passwords, use strong passwords that are not easily guessed. There are some key points to consider when choosing passwords:

- Use passwords that are more than eight characters in length.
- Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
- Avoid using the same password for all devices.
- Do not use common words because they are easily guessed.

Use an internet search to find a password generator. Many will allow you to set the length, character set, and other parameters.

Note: Most of the labs in this course use simple passwords such as **cisco** or **class**. These passwords are considered weak and easily guessable and should be avoided in production environments. We only use these passwords for convenience in a classroom setting, or to illustrate configuration examples.

2.4.3

Configure Passwords

When you initially connect to a device, you are in user EXEC mode. This mode is secured using the console.

To secure user EXEC mode access, enter line console configuration mode using the **line console 0** global configuration command, as shown in the example. The zero is used to represent the first (and in most cases the only) console interface. Next, specify the user EXEC mode password using the **password** *password* command. Finally, enable user EXEC access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Console access will now require a password before allowing access to the user EXEC mode.

To have administrator access to all IOS commands including configuring a device, you must gain privileged EXEC mode access. It is the most important access method because it provides complete access to the device.

To secure privileged EXEC access, use the **enable secret** *password* global config command, as shown in the example.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
```

```
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Virtual terminal (VTY) lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

To secure VTY lines, enter line VTY mode using the **line vty 0 15** global config command. Next, specify the VTY password using the **password** *password* command. Lastly, enable VTY access using the **login** command.

An example of securing the VTY lines on a switch is shown.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

2.4.4

Encrypt Passwords

The startup-config and running-config files display most passwords in plaintext. This is a security threat because anyone can discover the passwords if they have access to these files.

To encrypt all plaintext passwords, use the **service password-encryption** global config command as shown in the example.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

The command applies weak encryption to all unencrypted passwords. This encryption applies only to passwords in the configuration file, not to passwords as they are sent over the network. The purpose of this command is to keep unauthorized individuals from viewing passwords in the configuration file.

Use the **show running-config** command to verify that passwords are now encrypted.

```
Sw-Floor-1(config)# end
Sw-Floor-1# show running-config
!
(Output omitted)
!
line con 0
```

```
password 7 094F471A1A0A
login
!
line vty 0 4
 password 7 094F471A1A0A
 login
line vty 5 15
 password 7 094F471A1A0A
 login
!
!
end
```

2.4.5

Banner Messages

Although requiring passwords is one way to keep unauthorized personnel out of a network, it is vital to provide a method for declaring that only authorized personnel should attempt to access the device. To do this, add a banner to the device output. Banners can be an important part of the legal process in the event that someone is prosecuted for breaking into a device. Some legal systems do not allow prosecution, or even the monitoring of users, unless a notification is visible.

To create a banner message of the day on a network device, use the **banner motd #** *the message of the day* **#** global config command. The “#” in the command syntax is called the delimiting character. It is entered before and after the message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols such as the "#" are often used. After the command is executed, the banner will be displayed on all subsequent attempts to access the device until the banner is removed.

The following example shows the steps to configure the banner on Sw-Floor-1.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only#
```

2.4.6

Video - Secure Administrative Access to a Switch

Click Play in the figure to view a video demonstration of how to secure administrative access to a switch.

2.4.7

Syntax Checker - Basic Device Configuration

Secure management access to a switch.

- Assign a device name.
- Secure user EXEC mode access.
- Secure privileged EXEC mode access.
- Secure VTY access.
- Encrypt all plaintext passwords.
- Display a login banner.

Enter global configuration mode.

```
Switch#
```

Reset

Show Me

2.4.8

Check Your Understanding - Basic Device Configuration

Check your understanding of basic device configuration by choosing the BEST answer to the following questions.

1. What is the command to assign the name “Sw-Floor-2” to a switch?

- **hostname** Sw-Floor-2
- **host name** Sw-Floor-2
- **name** Sw-Floor-2

2. How is the privileged EXEC mode access secured on a switch?

- **enable class**
- **secret class**
- **enable secret class**
- **service password-encryption**

3. Which command enables password authentication for user EXEC mode access on a switch?

- **enable secret**
- **login**
- **secret**
- **service password-encryption**

4. Which command encrypts all plaintext passwords access on a switch?

- **enable secret**
- **login**
- **secret**
- **service password-encryption**

5. Which is the command to configure a banner to be displayed when connecting to a switch?

- banner $ Keep out $
- banner motd $ Keep out $
- display $ Keep out $
- login banner $ Keep out $

Check | Show Me

Reset

2.3 The Command Structure

2.5 Save Configurations