Module 19: Build a Small Cisco Network

Networking Essentials (NETESS)

Module Objectives

Module Title: Build a Small Cisco Network
Module Objective: Build a simple computer network using Cisco devices.

Topic Title	Topic Objective
Basic Switch Configuration	Configure initial settings on a Cisco switch.
Configure Initial Router Settings	Configure initial settings on a router.
Secure the Devices	Configure devices for secure remote management.
Connect the Switch to the Router	Build a network that includes a switch and router.

19.1 Basic Switch Configuration

Basic Switch Configuration Steps

The Cisco switch comes preconfigured and only needs to be assigned basic security information before being connected to the network.

Elements that are usually configured on a LAN switch include:

- host name
- management IP address information
- passwords
- descriptive information.

Basic Switch Configuration Steps (Cont.)

The switch host name is the configured name of the device.

- An example might be: SW_Bldg_R-Room_216

A management IP address is only necessary if you plan to configure and manage the switch through an in-band connection on the network

- IP address information that should be configured on a switch: IP address, subnet mask, and default gateway.

In order to secure a Cisco LAN switch, it is necessary to configure passwords on each of the various methods of access to the command line.

- Minimum requirements include assigning passwords to remote access methods (Telnet/SSH).
- You should assign a password to the privileged EXEC mode.

Note: Telnet sends the username and password in plaintext and is not considered secure. SSH encrypts the username and password and is, therefore, a more secure method.

Basic Switch Configuration Steps (Cont.)

Sample Switch Configuration

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
S1(config)# banner motd #No unauthorized access allowed!#
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.1.20 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Switch Virtual Interface Configuration

To access the switch remotely, an IP address and a subnet mask must be configured on the switch virtual interface (SVI).

- To configure an SVI on a switch, use the **interface vlan 1** global configuration command.
- Next, assign an IPv4 address using the **ip address** *ip-address subnet-mask* interface configuration command.
- Finally, enable the virtual interface using the **no shutdown** interface configuration command.

After the switch is configured with these commands, the switch has all the IPv4 elements ready for communication over a local network network.

Note: Switches configured with an IPv4 address should also have a default gateway assigned. This is done using the **ip default-gateway** *ip-address* global configuration command.

Packet Tracer – Implement Basic Connectivity

In this activity, you will first perform basic switch configurations. Then you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use various show commands to verify configurations and use the ping command to verify basic connectivity between devices.

19.2 Configure Initial Router Settings

Basic Router Configuration Steps

The following tasks should be completed when configuring initial settings on a router.

Step 1. Configure the device name.

Router(config)# **hostname** hostname

Step 2. Secure privileged EXEC mode.

Router(config)# **enable secret** password

Step 3. Secure user EXEC mode.

Router(config)# **line console 0**
Router(config-line)# **password** password
Router(config-line)# **login**

Step 4. Secure remote Telnet / SSH access.

Router(config-line)# **line vty 0 4**
Router(config-line)# **password** password
Router(config-line)# **login**
Router(config-line)# **transport input** {**ssh** | **telnet** | **none** | **all**}

Step 5. Secure all passwords in the config file.

Router(config)# **service password-encryption**

Step 6. Provide legal notification.

Router(config)# **banner motd** delimiter message delimiter

Step 7. Save the configuration.

Router# **copy running-config startup-config**

Basic Router Configuration Example

The following commands secure privileged EXEC mode and user EXEC mode, enable Telnet and SSH remote access, and encrypt all plaintext (i.e., user EXEC and vty line) passwords.

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
 R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

The legal notification warns users that the device should only be accessed by permitted users:

```
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
**********************************************  WARNING:
Unauthorized access is prohibited!
********************************************** #
```

The following command saves the configuration to NVRAM:

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

R1#
```

Packet Tracer – Configure Initial Router Settings

In this activity, you will perform basic router configurations. You will secure access to the CLI and console port using encrypted and plaintext passwords. You will also configure messages for users logging into the router. These banners also warn unauthorized users that access is prohibited. Finally, you will verify and save your running configuration.

19.3 Secure the Devices

Password Recommendations

To protect network devices, it is important to use strong passwords.

Here are standard guidelines to follow:

- Use a password length of at least eight characters, preferably 10 or more characters.
- Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces.
- Avoid passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, or other easily identifiable pieces of information.
- Deliberately misspell a password. For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.
- Change passwords often.
- Do not write passwords down and leave them in obvious places.

Password Recommendations (Cont.)

Weak Password	Why it is Weak
secret	Simple dictionary password
smith	Maiden name of mother
Toyota	Make of a car
bob1967	Name and birthday of the user
Blueleaf23	Simple words and numbers
Strong Password	**Why it is Strong**
b67n42d39c	Combines alphanumeric characters
12^h u4@1p7	Combines alphanumeric characters, symbols, and includes a space

Secure Remote Access

When the device is connected to the network, it can be accessed over the network connection using SSH or Telnet.

SSH is the preferred method because it is more secure.

When the device is accessed through the network, it is considered a vty connection.

- The password must be assigned to the vty port.

- The following configuration is used to enable SSH access to the switch:

```
Switch(config)# line vty 0 15
Switch(config)# password password
Switch(config)# transport input ssh
Switch(config)# login
```

Configure SSH

Before configuring SSH, the switch must be minimally configured with a unique hostname and the correct network connectivity settings.

Step 1. Verify SSH support.
Use the **show ip ssh** command to verify that the switch supports SSH.

Step 2. Configure the IP domain.
Configure the IP domain name of the network using the **ip domain-name** *domain-name* global configuration mode command.

Step 3. Generate RSA key pairs.
Use the **crypto key generate rsa** global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. A longer modulus length is more secure, but it takes more time to generate and to use.
Note: To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Configure SSH (Cont.)

Step 4. Configure user authentication.
The SSH server can authenticate users locally or use an authentication server.
To use the local authentication method, create a username and password pair with the **username** *username* **secret** *password* global configuration mode command.

Step 5. Configure the vty lines.
Enable the SSH protocol on the vty lines using the **transport input ssh** line configuration mode command.
Use the **line vty** global configuration mode command and then the **login local** line configuration mode command to require local authentication for SSH connections from the local username database.

Step 6. Enable SSH version 2.
By default, SSH supports both versions 1 and 2. Version 1 has vulnerabilities.
Use the **show ip ssh** command to see the version.
Enable SSH version using the **ip ssh version 2** global configuration command.

Verify SSH

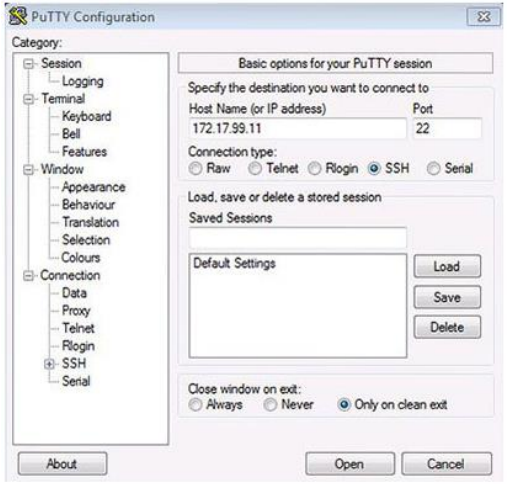
On a PC, an SSH client such as PuTTY, is used to connect to an SSH server.

For the graphics, the following has been configured:

- SSH enabled on switch S1
- Interface VLAN 99 (SVI) with IPv4 address 172.17.99.11 on switch S1
- PC1 with IPv4 address 172.17.99.21

Use the **show ip ssh** command to display the version and configuration data for SSH on the SSH server.

To check the SSH connections to the device, use the **show ssh** command.




```
Login as: admin
Using keyboard-interactive authentication.
Password: <ccna>

S1> enable
Password: <class>
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8 /8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAaP3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac       State        Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started admin
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started admin
%No SSHv1 server connections running.
S1#
```

Packet Tracer – Configure SSH

SSH should replace Telnet for management connections. Telnet uses insecure plaintext communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

19.4 Connecting the Switch to the Router

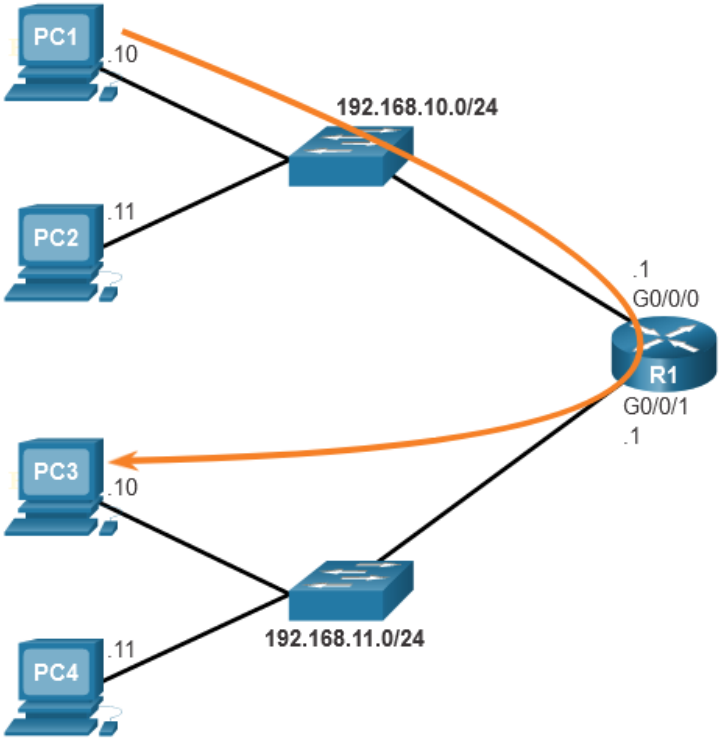
Default Gateway for a Host

If your local network has only one router, it will be the gateway router, and all hosts and switches on your network must be configured with this information.

The default gateway is only used when the host wants to send a packet to a device on another network.

The default gateway address is generally the router interface address attached to the local network of the host.

The IP address of the host device and the router interface address must be in the same network.



Default Gateway on a Switch

A switch that interconnects client computers is typically a Layer 2 device and does not require an IP address to function.

However, an IP configuration can be configured on a switch to provide remote access to the switch.

To connect to and manage a switch over a local IP network, it must have a switch virtual interface (SVI) configured.

- The SVI is configured with an IPv4 address and subnet mask on the local LAN.
- The switch must have a default gateway address configured to remotely manage the switch.
  - Use the **ip default-gateway** *ip-address* global configuration command.

Packet Tracer – Build a Switch and Router Network

In this activity, you will cable and then configure the devices to match the address table. After the configurations have been saved, you will verify your configurations by testing for network connectivity and retrieve information from the network devices.

19.5 Build a Small Cisco Network Summary

What Did I Learn in this Module?

The Cisco switch comes preconfigured and only needs to be assigned basic security information before being connected to the network.

- Configure the device name.
- Configure a management IP address information.
- Secure the local and remote access methods using passwords.
- Provide descriptive information.
- To access the switch remotely, an IP address and a subnet mask must be configured on the switch virtual interface (SVI).

The Cisco router needs to be configured with initial settings before being connected to the network.

- Configure the device name.
- Secure the privileged EXEC mode.
- Secure the local and remote access methods using passwords
- Secure all plaintext passwords.
- Provide legal notification.

What Did I Learn in this Module? (Cont.)

To protect network devices, it is important to use strong passwords.

- Use a password length of at least eight characters, preferably 10 or more characters.
- Make passwords complex.
- Avoid passwords based on repetition, common dictionary words or other easily identifiable pieces of information.
- Deliberately misspell a password.
- Change passwords often.
- Do not write passwords down and leave them in obvious places.

Configure SSH on a switch or router.

- Step 1. Verify SSH support.
- Step 2. Configure the IP domain.
- Step 3. Generate RSA key pairs.
- Step 4. Configure user authentication.
- Step 5. Configure the vty lines.
- Step 6. Enable SSH version 2.

What Did I Learn in this Module? (Cont.)

The default gateway is only used when the host wants to send a packet to a device on another network.

- The default gateway address is generally the router interface address attached to the local network of the host.
- The IP address of the host device and the router interface address must be in the same network.

A Layer 2 switch does not require an IP address to function properly, however, it must have a switch virtual interface (SVI) configured in order to be remotely accessed and configured.

- The SVI is configured with an IPv4 address and subnet mask on the local LAN.
- The switch must also have a default gateway address configured to remotely manage the switch from another network.

Module 19 – New Terms and Commands

- **enable secret** password
- **hostname** name
- **line console** 0
- **password** password
- **login**
- **line vty** 0 15
- **transport input** ssh telnet
- **service password-encryption**
- **banner motd** delimiter message delimiter
- **copy running-config startup-config**
- switch virtual interface (svi)
- **interface vlan** 1
- **ip default-gateway** ip-address
- **show ip ssh**
- **ip domain-name** name
- **crypto key generate rsa**
- **crypto key zeroize rsa**
- **ip ssh version** number
- **username** username **secret** password


CISCO