Basics of Network Security

Version 1.0.0

Arlo Bannon-David

January 30, 2025

Contents

1 Introduction

In this document, I will outline my personal methods for basic network security on a Cisco 2950 Series Switch. This is not all-encompassing, and I plan to iterate on it in the future.

The original purpose of this document is for the Cybersecurity in Networks Workshop with ShiftKey Labs on January 16, 2025.

Although this guide is based on the build notes for a physical switch, it can be recreated using network simulation programs such as Cisco Packet Tracker. Although these programs may not have the Cisco 2950 Series Switch used in this document, others can be used, as the syntax is typically similar. You can find documentation online for most Cisco network hardware that describes its command syntax. If a command isn't working, try searching the command with your model of hardware.

2 Hardware

This guide uses the following:

1. Cisco Catalyst 2950 Series[1] (24 Ports)
2. USB to RJ45 Console Cable (Learn more about console cables here[2])
3. CAT6A Ethernet Cable
4. Windows 11 Device

3 Steps

3.1 Installation & Setup

1. Plug the RJ45 connection side of console cable into the console port on your switch, typically located on the back.
2. Plug the USB side into a USB port on your device.
3. Install PuTTY[3] or similar SSH Client
4. Open Device Manager
   (a) Expand `Ports (COM & LPT)`
   (b) Find `USB Serial Port (COMx)` and note `x`.
5. Open PuTTY
   (a) Select `Serial` connection type
   (b) Change from `COM1` to `COMx`, where `x` is the previously noted interface.

[1] https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst2955/software/release/12_1_12c_ea1/command/reference/cr2955.pdf
[2] https://www.cablesandkits.com/learning-center/what-are-console-cables-why-need-them
[3] https://www.putty.org/

(c) Set the speed based on your device (9600 is common, and is the speed the Catalyst 2950 uses)

(d) Select `Open`

6. Press enter once the console screen opens. You should see ¨,|Switch>|:· ␣␣␣␣␣␣␣␣␣␣␣␣

7. ␣Run␣the␣¨,|enable|:␣command. ␣␣␣␣␣␣␣␣␣␣␣␣You␣should␣see␣¨,|Switch|:· ␣␣␣␣␣␣␣␣␣␣␣␣

8. ␣Run␣¨,|show␣running|:␣to␣ensure␣the␣configuration␣is␣cleared. ␣␣␣␣␣␣␣␣

3.2 Switch Configuration

To enter configuration mode, enter the command `configure terminal`.
You should now see:
`Switch(config)#`

3.2.1 Hostname

Setting a hostname is especially important on multiple-device networks to tell the difference between each device.
In configuration mode, run the following command:
`hostname [new-hostname]`

3.2.2 Set a Password

This sets a password to access privileged execution mode, which will prompt you for a password when you enter the `enable` command.
`enable secret [password]`

3.2.3 Configure Telnet

Telnet[4] is a client/server application protocol used for remote access to terminals.
It is less secure than SSH, so we want to ensure that our system is secured and does not give unwanted users remote access to our console.

```
line vty 0 15
password [password]
login
exit
```

What this does is configure the first 16 virtual terminal (`vty`) lines.
We set a password and tell it we want users to have to log in to access the virtual terminal using the password we set.
Next, we configure a Telnet Access List based on IPs. This tells Telnet to only allow certain IPs to access the virtual terminal, adding another layer of security as they will also have to input a password.

```
ip access-list standard TELNET-ACCESS
permit [192.168.1.2]
exit
```

[4] https://www.geeksforgeeks.org/introduction-to-telnet/

3.2.4 Console Access

Next we set a password for accessing the console physically.

```
line console 0
password [password]
login
exit
```

3.2.5 Configure Switch IP

```
interface vlan 1
ip address 192.168.1.1 255.255.255.0
exit
```

We can also configure the default gateway, which tells the switch the router's IP address.

```
ip default-gateway 192.168.1.0
```

3.2.6 Port Error Recovery

```
errdisable recovery cause all errdisable recovery interval [seconds]
```

3.2.7 Securing Unused Ports

Any ports that you know won't be used should be shutdown to ensure that nobody can walk up and connect their device to the port.

```
interface range fa0/3 - 24
shutdown
exit
```

3.2.8 Securing Used Ports

```
interface range fa0/1 - fa0/2
switchport port-security maximum 1
```

The second command configures the maximum amount of MAC addresses that can connect to each port.