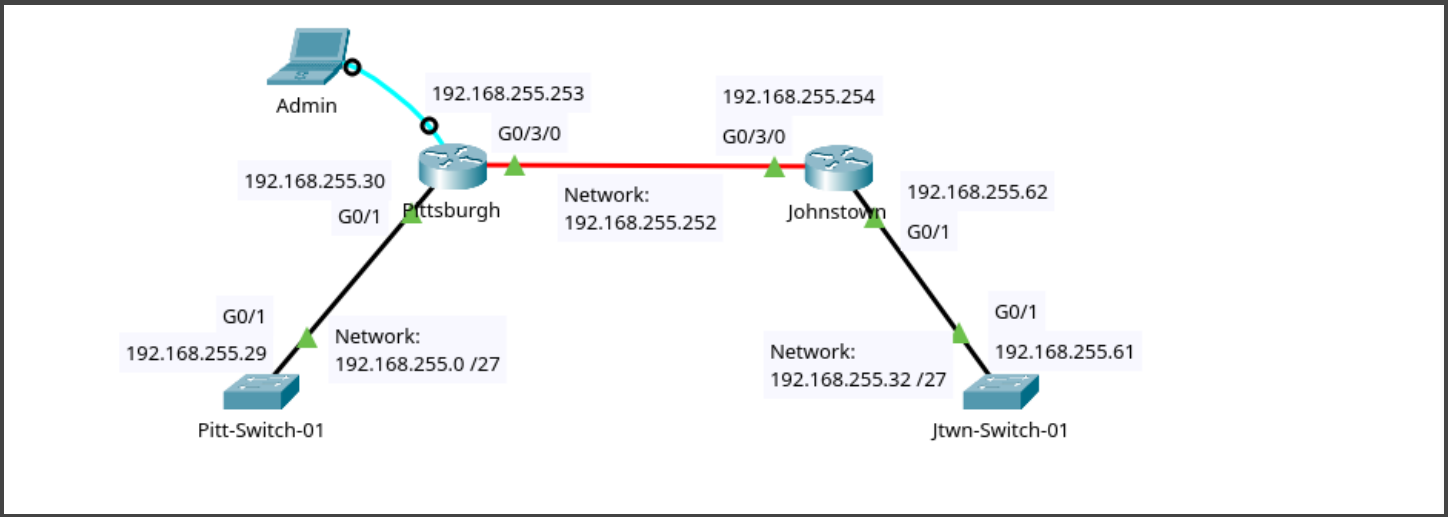
Configure Usernames and Passwords **10/19/2023**

By Nathan Fitzsimmons *nathanfitzsimmons2010.github.io*



In this lab we will configure usernames and passwords:

- Configure username and secret (password).
- Enable service password-encryption.
- Set appropriate console, auxiliary, and VTY lines settings.
- Analyze configurations.
- Save configuration.

---

1. Add usernames and passwords to our current network devices:
    a. Left Click Pittsburgh Router and enter following commands:
    b. Enable
    c. Configure terminal
    d. Username [***NAME***] secret [***PASSWORD***]

```
Pittsburgh>enable
Pittsburgh#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Pittsburgh(config)#username Nathan secret Cisco
```

2. Check the running-config to see the encrypted password.

```
Pittsburgh(config)#do show running-config | include username
username Nathan secret 5 $1$mERr$YlCkLMcTYWwkF1Ccndtll.
```

3. While our password is encrypted because of the secret command, let's make sure any future passwords created by the less secure "password" command are encrypted as well.
    a. Service password-encryption

Example:

```
Pittsburgh(config)#username James password Juniper
Pittsburgh(config)#
Pittsburgh(config)#do show run | include username James
username James password 0 Juniper
Pittsburgh(config)#
Pittsburgh(config)#service password-encryption
Pittsburgh(config)#
Pittsburgh(config)#do show run | include username James
username James password 7 080B594000090005
```

Here is an example of the service password-encryption. The input was a clear-text password of Juniper; the show run command verifies you can read the password in the configuration. Service password-encryption is configured and password is now encrypted in the running configuration.

```
Johnstown#show run | begin line
line con 0
!
line aux 0
!
line vty 0 4
 login
```

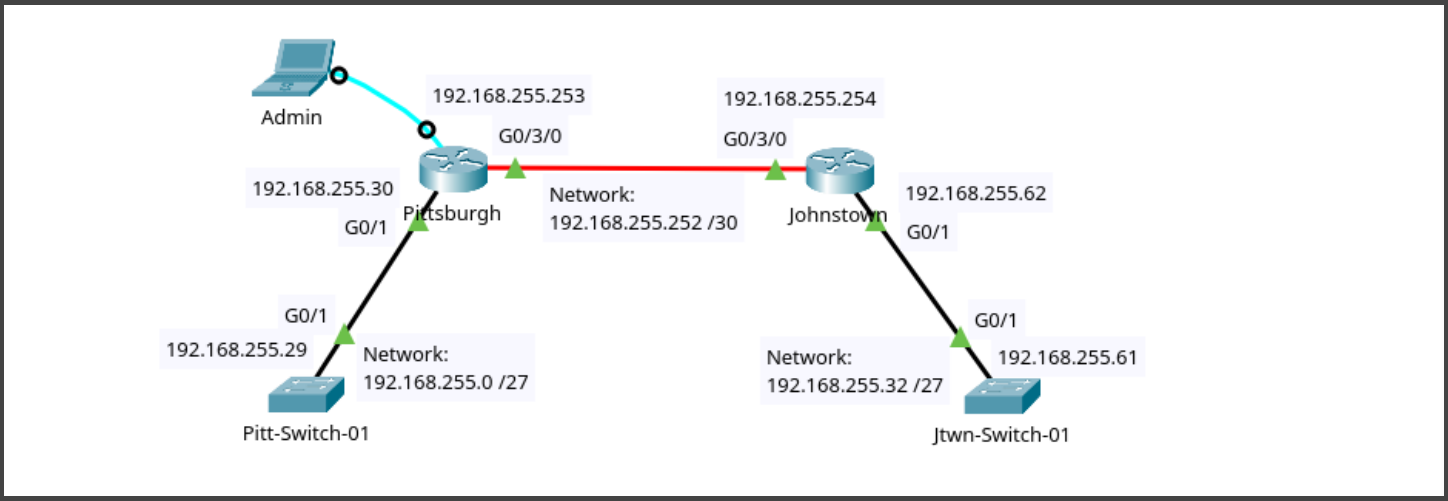
4. We need to configure the console, auxiliary, and virtual terminal lines to login with our local username and secret that we just configured.
    a. Enable
    b. Configure terminal
    c. Line console 0
        i. Login local
        ii. Exit
    d. Line aux 0
        i. Login local
        ii. Exit
    e. Line vty 0 15
        i. Login local
        ii. Exit

```
Pittsburgh>enable
Pittsburgh#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Pittsburgh(config)#
Pittsburgh(config)#line console 0
Pittsburgh(config-line)#login local
Pittsburgh(config-line)#exit
Pittsburgh(config)#
Pittsburgh(config)#line aux 0
Pittsburgh(config-line)#login local
Pittsburgh(config-line)#exit
Pittsburgh(config)#
Pittsburgh(config)#line vty 0 15
Pittsburgh(config-line)#login local
Pittsburgh(config-line)#exit
Pittsburgh(config)#
```

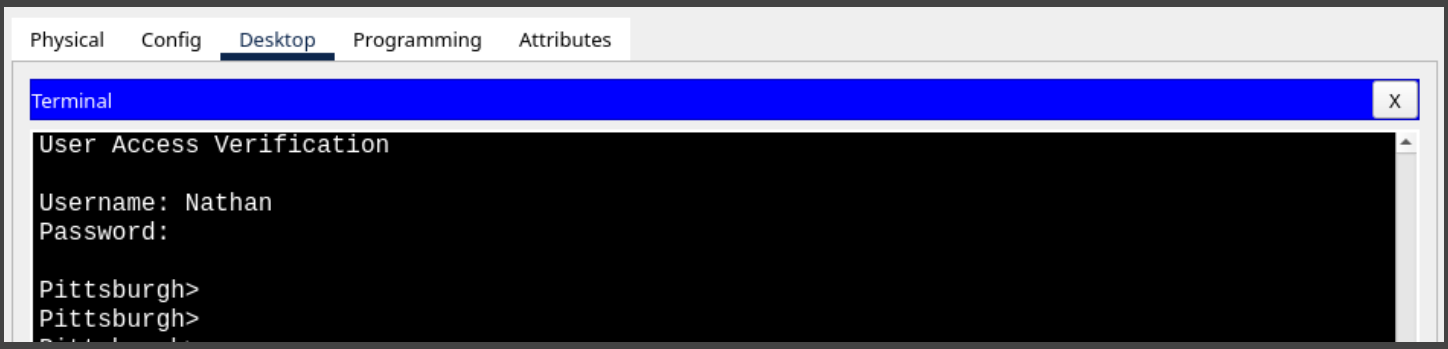
5. Check the running-configuration again.

```
Pittsburgh#show run | section line
line con 0
 login local
line aux 0
 login local
line vty 0 4
 login local
line vty 5 15
 login local
```

6. Now to test the logins:
    a. Enter the exit command until you leave user exec mode.
    b. Bottom left of the packet tracer window, choose end devices and drag and drop a laptop onto the topology. I renamed mine to admin on the topology.
    c. Now in the connections window, choose a console cable and connect the laptop to the Pittsburgh router. Laptop's RS 232 port to Pittsburgh's Console port.



    d. Left Click the laptop and go to the Desktop tab.
    e. Click the Terminal button and click OK.
    f. Log in.



7. Write running-config to the startup-config.

```
User Access Verification

Username: Nathan
Password:

Pittsburgh>
Pittsburgh>enable
Pittsburgh#wr
Building configuration...
[OK]
Pittsburgh#
```

8. Repeat on all four network devices.
    a. Enable service password encryption
    b. Configure Username and Secret
    c. Set appropriate console, auxiliary, and VTY lines to login local.
    d. Test
    e. Save configuration