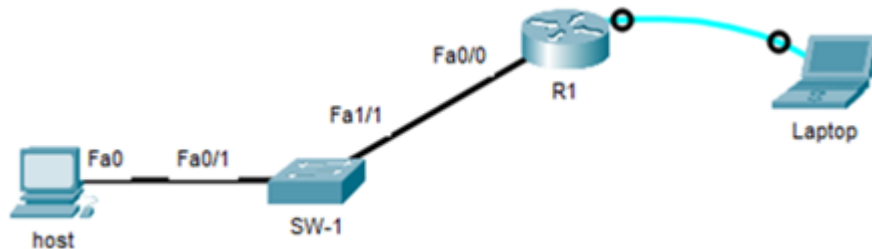


# Local Authentication

## Lab Summary

Configure a username account locally on R1 to enable local account authentication.

**Figure 1** Lab Topology



## Lab Configuration

Start Packet Tracer File: **local authentication.pkt**

Step 1: Click *R1* icon and select *CLI* folder.

Step 2: Enter global configuration mode

```
R1 > enable  
R1# configure terminal
```

Step 3: Enable default VTY 0 4 lines with local authentication.

```
R1(config)# line vty 0 4  
R1(config-line)# login local  
R1(config-line)# exit
```

Step 4: Configure local username *admin* with highest security privilege level 15 and secret password *ccnaexam*.

```
R1(config)# username admin privilege 15 secret ccnaexam
```

Step 5: Enable console port with local authentication.

```
R1(config)# line console 0  
R1(config-line)# login local  
R1(config-line)# end  
R1# copy running-config startup-config  
R1# exit
```

## Step 6: Verify Lab

Telnet from host-1 to R1 and verify remote access with local authentication.

Click *Host* icon and select the *Desktop* folder. Select *Command Prompt* icon.

```
c:/> telnet 192.168.1.2
```

```
Username: admin
```

```
Password: ccnaexam
```

```
R1# exit
```

```
[Connection to 192.168.1.2 closed by foreign host]
```

Start a console session from laptop to R1 and verify there is local authentication enabled. Click *Laptop* icon and select the *Desktop* folder. Select *Terminal* icon and verify the terminal settings are correct on the Laptop USB interface. Click OK and hit enter for user mode prompt.

### **Cisco Default Terminal Settings**

- 9600 bps
- 8 data bits
- no parity
- 1 stop bit
- no flow control

Login to the local console port with username *admin* and password *ccnaexam*.

```
Username: admin
```

```
Password: ccnaexam
```

```
R1# exit
```

```
[Connection to 192.168.1.2 closed by foreign host]
```

## Lab Notes

Enable password is optional with local authentication for Telnet session to VTY lines. It is common to copy the same encrypted password to multiple devices. List the running configuration to copy the hidden password and paste it to the new device with **username admin privilege 15 secret 5 [encrypted password]**.