# **SSH Configuration Lab on Cisco 1841 Routers (Packet Tracer)**

This document explains step-by-step what I did in my Packet Tracer SSH lab, including the commands I entered, where I made mistakes, and how the configuration should work. It is based on my screenshots and command logs.

## **1. Lab Topology**

* **Devices**: Two Cisco 1841 routers (Router0 and Router1)
* **Connection**: Crossover cable between fa0/0 interfaces

[Router0: JBC1] ---- fa0/0 <-> fa0/0 ---- [Router1: JBC2]

## **2. Initial Setup**

### **Router0 (JBC1)**

Router>en

Router#conf t

Router(config)#hostname JBC1

JBC1(config)#int fa0/0

JBC1(config-if)#ip address 192.168.1.1 255.255.255.0

JBC1(config-if)#no shutdown

### **Router1 (JBC2)**

Router>en

Router#conf t

Router(config)#hostname JBC2

JBC2(config)#int fa0/0

JBC2(config-if)#ip address 192.168.1.2 255.255.255.0

JBC2(config-if)#no shutdown

✅ At this point, both routers had green link lights.

❌ I initially tried ping 192.169.1.1 instead of 192.168.1.1 — typo in the third octet caused the test to fail.

## **3. SSH Prerequisites**

SSH on Cisco devices requires:

1. **Hostname**
2. **Domain name**
3. **RSA key generation**

### **Router0 (JBC1)**

JBC1(config)#ip domain-name jbc.net

JBC1(config)#crypto key generate rsa

How many bits in the modulus [512]: 2048

### **Router1 (JBC2)**

JBC2(config)#ip domain-name jbc.net

JBC2(config)#crypto key generate rsa

How many bits in the modulus [512]: 2048

✅ Both routers generated 2048-bit RSA keys successfully.

## **4. VTY and SSH Settings (on JBC2)**

JBC2(config)#line vty 0 15

\*Mar 1 0:32:13.168: %SSH-5-ENABLED: SSH 1.99 has been enabled

JBC2(config-line)#transport input ssh

JBC2(config-line)#password jbc

JBC2(config-line)#login

JBC2(config-line)#exit

JBC2(config)#ip ssh authentication-retries 2

JBC2(config)#ip ssh time-out 120

JBC2(config)#ip ssh version 2

✅ At this point, Router1 was ready to accept SSH connections.

## **5. Attempting SSH from JBC1**

### **My Commands**

JBC1#ssh -l john 192.168.1.2

Password:

% Password: timeout expired!

I retried multiple times but kept getting **"connection closed by foreign host"**.

### **Why It Failed**

* I specified -l john, but Router2 (JBC2) did **not** have a local user john configured.
* JBC2 was only configured with a **VTY line password (jbc)**, not per-user accounts.
* IOS expected a matching local username when I used -l john, so authentication failed.

## **6. Two Fix Options**

### **Option 1: Use Line Password Only**

If I don’t care about usernames:

JBC1#ssh 192.168.1.2

Then enter the VTY password jbc.

### **Option 2: Configure a Local Username**

If I want to log in as john:

JBC2(config)#username john secret mysecurepass

JBC2(config)#line vty 0 15

JBC2(config-line)#login local

Now I can connect:

JBC1#ssh -l john 192.168.1.2

Enter password mysecurepass → login successful.

## **7. Key Takeaways**

* ✅ Hostname, domain name, and RSA keys are required before SSH works.
* ✅ VTY lines must allow SSH (transport input ssh).
* ❌ Using ssh -l <username> requires that the username exist locally.
* ✅ If only a VTY password is configured, connect without -l <username>.
* 🔒 Best practice: Use username <name> secret <password> + login local for secure logins.

## **Final Notes**

The lab worked up to the point of establishing SSH, but my mistake was trying to log in with a username (john) that didn’t exist. This is why the session timed out. Adding a local user or adjusting my SSH command fixes the issue.