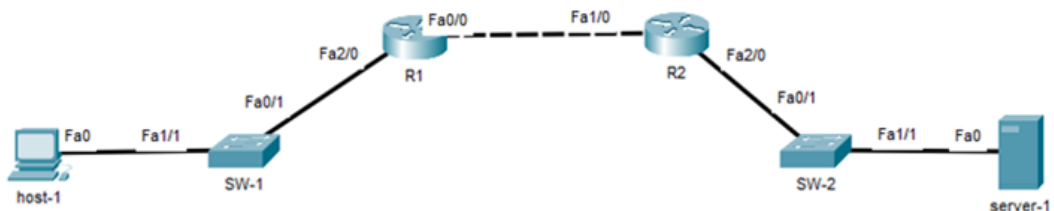


# Secure Shell (SSHv2)

## Lab Summary

Configure and verify SSHv2 remote management access on R2 router.

**Figure 1** Lab Topology



## Lab Configuration

Start Packet Tracer File: **sshv2.pkt**

Step 1: Click *R2* icon and select *CLI* folder.

Step 2: Enter global configuration mode.

```
R2 > enable
```

```
R2# configure terminal
```

Step 3: Configure username account *cisco* with privilege level 15 and secret password *ccnalabs* for SSH session authentication.

```
R2(config)# username cisco privilege 15 secret ccnalabs
```

Step 4: Enable SSH (encrypted) remote management access to R2.

```
R2(config)# ip domain-name lab.cisconet.com
```

```
R2(config)# crypto key generate rsa
```

```
[type yes to create key]
```

```
bits? [768] 1024
```

```
R2(config)# ip ssh version 2
```

```
R2(config)# ip ssh time-out 60
```

Step 5: Enable VTY lines for local authentication and permit SSH protocol only to R2 for security purposes.

```
R2#(config)# line vty 0 4
```

```
R2#(config-line)# login local
```

```
R2#(config-line)# transport input ssh
```

```
R2(config-line)# end
```

```
R2# copy running-config startup-config
```

### Step 6: Verify Lab

Start an SSHv2 session from host-1 to R2 and confirm there is remote access.  
Attempt to access R2 with Telnet and verify that it is denied to that router.

SSH from host-1 to R2 router with the following commands.

```
c:\> ssh -l cisco 192.168.2.2  
Open  
Password: ccnalabs  
R2# exit
```

Telnet from host-1 to R2 router and verify that access is denied.

```
c:\> telnet 192.168.2.2  
Trying 192.168.2.2 ...Open  
[Connection to 192.168.2.2 closed by foreign host]
```