Telnet vs SSH

- All Telnet communications cross the network in plain text
- If somebody sniffs the traffic using a tool such as Wireshark they can see all the commands you enter including your username and password
- All SSH Secure Shell traffic is encrypted
- If somebody sniffs the traffic they cannot read it
- Best practice is to disable Telnet and only allow SSH for administrator CLI access

Enable SSH

- A digital certificate with a key length of at least 768 bits must be generated to enable SSH encryption

```
R1(config)#ip domain-name flackbox.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.flackbox.com
Choose the size of the key modulus in the range of 360 to 2048
for your General Purpose Keys. Choosing a key modulus greater
than 512 may take a few minutes.

How many bits in the modulus [512]: 768
% Generating 768 bit RSA keys, keys will be non-
exportable...[OK]
```

Disable Telnet

- VTY lines are used for both Telnet and SSH connections
- Access is allowed for both by default
- A username is required for SSH access (line level passwords are not supported)

```
R1(config)#username Flackbox secret Flackbox1
R1(config)#line vty 0 15
R1(config-line)#transport input ssh (telnet not added)
R1(config-line)#login local (use local usernames)
R1(config-line)#exit
R1(config)#ip ssh version 2 (limit SSH to v2)
```

SSH Access

```
C:\> ssh –l Flackbox 10.0.0.1
Open
Password: Flackbox1
R1>
```