

Managing Cisco Devices

In this book, I will cover enabling SSH on a cisco device and just a few tweaks for added security. Also this book will cover other topics like AAA model and overall management of the device

- Enabling SSH
- Username and Passwords

Enabling SSH

It always starts with the generation of a public/private keypair that will be only used for the SSH-process. In this command we use a dedicated label "SSH-KEY" which we later assign to the SSH-config. The default-keylength is typically too small, it's time to move to a stronger crypto. For new setups I only use 4096 Bit keys, however, 2048 is still widely used. That's more than recommended on sites like <http://www.keylength.com> and makes the session-setup a little slower. But by far not that slow that it's unusable. And it typically doesn't hurt to have better crypto than the others.

Getting Started:

You will need to ensure that you have a domain name configured, for example: home.lab or example.com. Let's get started

Generate Domain name

```
switch(config)#ip domain-name home.lab
```

Generate RSA-Keypair at 4096bits

```
switch(config)# crypto key generate rsa label SSH-KEY modulus 4096
```

The RSA-Keypair is assigned to the SSH-config:

```
switch(config)#ip ssh rsa keypair-name SSH-KEY
```

Allow only SSH Version 2

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

Set Minimum Diffie-Hellman Key exchange

```
switch(config)#ip ssh dh min size 4096
```

When the SSH-session is established, the session-keys are computed with the Diffie-Hellmann key exchange protocol. By default this is done with 768 Bit, which is not state-of-the-art any more. For my setups (with MacOS and Linux clients) I configure a bitlength of 4096 Bit. You should use a powerful terminal like SecureCRT or use only a size of 2048 Bit which is still very secure. And if your IOS is too old, this command will also not be available.

SSH Logging

```
switch(config)#ip ssh logging events
```

The last step is to restrict the vty-lines to only use SSH, so that Telnet is not allowed any more:

```
switch(config)#line vty 0 4  
switch(config-line)#transport input ssh
```

If the IOS-device is running at least 15.5(2), then it's possible to [disable unwanted algorithms](#). In security-audits, all CBC-ciphers are often a problem.

Username and Passwords

There are different ways in IOS to configure users with corresponding passwords. For SSH, the Router/Switch doesn't need the cleartext password.

That means you should not configure your users with

```
switch(config)#username USER password PASS
```

Better configure your users with hashed passwords. If you are running a recent IOS, you can configure the passwords to be hashed with sha256 algorithm or a type 9 password:

```
switch(config)#username USER algorithm-type sha256 secret VERYSECUREPASSWORD
```

or

```
switch(config)#username USER algorithm-type scrypt secret VERYSECUREPASSWORD
```

If your IOS doesn't support this new username-parameter, you configure them the following way:

```
switch(config)#username USER secret VERYSECUREPASSWORD
```

Some more protection-mechanisms that should be thought about are [Control-Plane-Protection](#) and [Management-Plane-Protection](#). But that is not SSH-specific.