The New Improved CCNA
March 02, 2011
By Steve Means, CCSP, CCNP, CCSI# 32951

Cisco has recently released a new version of the CCNA that is reflected in the training courses and the test. Both the ICND1 and ICND2 courses have moved from version 1.0 to version 1.1. So, what does that mean for a student who has been preparing for the CCNA using “old” material? Will all that knowledge have to be scrapped and a fresh start made?

Thankfully not. The purpose of the CCNA has always been to validate the basic knowledge needed to maintain and troubleshoot a small to medium sized business network. That hasn’t changed; IP is still IP, subnetting is still subnetting and so on. Don’t think of this change as a major overhaul, but rather a minor tune-up. Some of the material has been refreshed to make it better aligned with newer technology such as developments in VoIP, Wireless and Security.

This article gives a brief summary of one topic that has been added, configuring SSH on a Cisco router. Previously the ICND1 course mentioned that telnet is a cleartext protocol and thus insecure while SSH is encrypted and secure. This hasn’t changed, however the procedure to configure SSH on a Cisco router is now covered. SSH requires a few more steps to configure than telnet, but the increased security is well worth it. The procedure is as follows:

A username and password are necessary to log in via SSH so:

```
router(config)# username cisco password cisco
```

Next generate RSA keys that will be used with SSH. Although it isn’t an absolute requirement the easiest way to configure SSH is with general use RSA keys. These require a hostname and domain name.

```
router(config)# hostname R1
R1(config)# ip domain-name ccbootcamp.com
```

With that out of the way one can generate RSA keys for use with SSH. The command shown uses a key size of 1024 bits. The default is 512, but greater than 768 is needed for the more secure SSH version 2.

```
R1(config)# crypto key generate rsa mod 1024
```

With the proper size keys created one can set the SSH version to the more secure version 2.

```
R1(config)# ip ssh version 2
```

Finally go to VTY (virtual terminal) lines and set them up to use SSH. Login local sets the lines to use the local username and password set above.

```
R1(config)# line vty 0 15
R1(config-line)# login local
R1(config-line)# transport input ssh
```

And that’s it! This is just one example of the minor tweaks that have been made to improve the already solid course material that is available for prep for the CCNA exam. CCBOOTCAMP’s classes are fully prepared with the new version 1.1 material!