

Lab - Install the CSR1000v VM

Objectives

Part 1: Install the CSR1000v VM on VirtualBox

Part 2: Verify Communications to CSR1000v VM

Background / Scenario

In this lab, you will install the CSR1000v Cloud Services Router. This is a Cisco software virtual router deployed on a virtual machine (VM) instance on x86 server hardware. When the Cisco CSR 1000v is deployed on a VM, the Cisco IOS XE software functions as if it were deployed on a traditional Cisco hardware platform. You can configure different features depending on the Cisco IOS XE software image.

Note: The CSR1000v name will be shortened to CSR1kv in future labs. However, for this lab we use CSR1000v.

Required Resources

- Host computer with at least 4 GB of RAM and 2 GB of free disk space
- Virtual Box or VMware
- DEVASC Virtual Machine

Instructions

Part 1: Install the CSR1000v VM

Install the CSR1000v VM directly on your x86 computer. It requires at least 4GB of RAM.

Step 1: Instructor only: Download the CSR1000v ISO file.

Note: Only the instructor or anyone with proper credentials is allowed to download ISO files from Cisco. This step must be done by the instructor.

- To download the CSR1000v ISO go to:
<https://software.cisco.com/download/home/284364978/type/282046477/release/Fuji-16.9.5>

Note: To download software from cisco.com, you must be an active NetAcad instructor and have a CCO account with the activated [NetAcad Maintenance contract](#).

- Select the download icon to the right of the following file:

Cisco CSR1000V IOS XE Universal - CRYPTO ISO

csr1000v-universalk9.16.09.05.iso

- The instructor may now distribute this ISO to students to use in the DevNet Associate course only.

Step 2: Download the CSR1000v VM OVA file.

- Navigate to the [DevNet Associate Virtual Machines \(VMs\)](#) page on netacad.com.
- Download the **DEVASC_CSR1000v.zip** and note the location of file.
- This file contains both the VirtualBox and VMware template files. Unzip the file to access the VMs.

Step 3: Install the CSR1000v VM.

- Open Oracle VirtualBox Manager or VMware Workstation.
- Select **File > Import** in VirtualBox or **File > Open** in VMware. In VMware Workstation Player, select **Player > File > Open**.
- In VirtualBox, select the file **CSR1000v_for_VirtualBox.ova** and click **Open** and **Import**.
In VMware, select the file **CSR1000v_for_VMware.ova** and click **Open**.
- Click **Import**.
- You will now see the **CSR1000v** VM added to VirtualBox or VMware.

Step 4: Update the installation ISO location.

- Select the Virtual Machine **Settings** or click **Edit virtual machine settings**.
- In the VM Settings, go to the very first CD Drive setting.
 - In VirtualBox: **VM Settings > Storage > CD device** (the first CD Drive in the list)
 - In VMware: VM Settings > the first "CD/DVD (IDE)" Drive in the list
- In the first CD Drive settings, replace the currently used ISO file
 - In VirtualBox: Attributes > CD icon > Choose a disk file ...
 - In VMware: Next to "Use ISO image file", click **Browse**.
- Select the ISO file you received from your instructor in Step 1.
At the time this lab was written, the file name was **csr1000v-universalk9.16.09.05.iso**. However, the version (16.09.05) may have changed, altering the file name.
- Do **NOT** change the Second CD Drive settings. That is used for the initial configuration of the router.
- Click **OK** to save the Virtual Machine settings.

Step 5: For VirtualBox on Mac and Linux, verify the CSR1000v is using a Host-Only Adapter.

- In VirtualBox, click **File > Host Network Manager...**
- Verify that there is a host adapter with a name such as **vxboxnet0** with an IPv4 Address/Mask 192.168.56.1/24. It is important that your host-only adapter is on the 192.168.56.0/24 network.
- If host adapter does not exist, click **Create**.
- If the IPv4 address is not on 192.168.56.1/24, select the adapter and click **Properties**. Modify the IPv4 address and click **Close**.

Step 6: Start CSR1000v VM.

- Select the **CSR1000v** VM and click **Start** or **Power On**.
- If you receive the following message, continue with this step, otherwise, go to the next step:
Could not start the machine DEVASC-CSR1000v because the following physical network interfaces were not found:
VirtualBox Host-Only Ethernet Adapter (adapter 1)
You can either change the machine's network settings or stop the machine.
- Verify the following:
Adapter 1 - Attached to: **Host-only Adapter**

- d. Click **OK**.

Step 7: VM Loading Process.

During the loading process you will see several messages including a message to **Press any key to continue**. You can ignore all of these messages.

A selection screen will appear where you can choose different configuration options. Do not choose any configuration options. Installation will continue on its own.

Wait for the initial installation process to complete. This will take several minutes the first time you boot the CSR1000v.

You will begin to see IOS messages from different processes including %SSH, %PKI and %CRYPTO_ENGINE. After a few minutes the messages will stop.

- a. Within the VM window, press **Enter**.

You should now see the prompt: **CSR1kv>**.

- b. Enter **enable** for the privileged EXEC prompt. There is no enable password.

```
CSR1kv> enable
CSR1kv#
```

Part 2: Verify Communications to CSR1000v VM.

In this Part, you will verify communications between devices:

Step 1: Verify the CSR1000v IPv4 address.

From the CSR1000v VM, use the **show ip interface brief** command to verify the IPv4 address of the GigabitEthernet1 interface. The CSR1000v is most likely using the IPv4 address from the **192.168.x.y** address space.

```
CSR1kv# show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet1        192.168.56.101  YES DHCP    up              up
CSR1kv#
```

```
csr1000ce#sh ip int brief
Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet1        192.168.56.101  YES DHCP    up              up
csr1000ce#
```

Make note of this address and use it in the rest of this lab as well as other labs in this course in place of the default of **192.168.56.101**.

Step 2: Launch the DEVASC VM.

If you have not completed the **Lab 1.1.2 Lab - Install the Virtual Machine Environment**, do so now. If you have already completed that lab, launch the DEVASC VM now.

Step 3: Ping the CSR1000v VM from the DEVASC VM VM.

- a. Select the **DEVASC VM** VM.
- b. Open a **Terminal** window.
- c. Ping the CSR1000v VM at its IPv4 address.

```
devasc@labvm:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=63 time=8.04 ms
```

Lab - Install the CSR1000v VM

```
64 bytes from 192.168.56.101: icmp_seq=2 ttl=63 time=3.08 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=63 time=1.04 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=63 time=1.08 ms
```

```
^C
--- 192.168.56.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 1.038/3.310/8.043/2.854 ms
devasc@labvm:~$
```

```

caxj000c$#
2ncceaa t9c6 ta j00 b6ic6ur (2\2)' konuq-citb wtu\ead\wex = j\j\j wa
iiii
2euqtud 2' j00-p4c6 icw6 ecv6a co j2s'j68'2e'j0j' ctw6onr ta 3 2ecouqa:
j4b6 6ac6b6 2edn6uc6 co 6p6ic6'
caxj000c$#b7ud j2s'j68'2e'j0j
p22am6icq:
caxj000c$>6v

```

Step 4: Establish a secure shell (SSH) session with the CSR1000v.

Some of the tasks you will complete in later labs will require an SSH session with the CSR1000v.

- a. Connect to the CSR1000v with SSH from the DEVASC VM. Use the password **cisco123!** to authenticate. Notice that you are automatically in privileged EXEC mode. Enter **exit** to end the SSH session.

```
devasc@labvm:~$ ssh cisco@192.168.56.101
Password:
```

```

*
**
***
*** Cisco Networking Academy
***
*** This software is provided for
*** Educational Purposes
*** Only in Networking Academies
***
**
*

```

```
CSR1kv# exit
Connection to 192.168.56.101 closed by remote host.
Connection to 192.168.56.101 closed.
devasc@labvm:~$
```

192.168.56.101 - PuTTY

```
login as: chakir
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

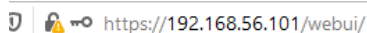
*
*
***
*** Cisco Networking Academy
***
*** This software is provided for
*** Educational Purposes
*** Only in Networking Academies
***
**
*

csr1000ce>en
Password:
csr1000ce#ping 192.168.56.101
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.56.101, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
csr1000ce#sh ip int brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet1 192.168.56.101 YES DHCP up up
csr1000ce#
```

Step 5: From the DEVASC VM, access the CSR1000v WebUI (Web User Interface).

- a. Open a web browser on the DEVASC VM.
- b. For the URL enter: **https://192.168.56.101**
Note: Be sure to use "https"
- c. If your browser displays a warning similar to, "Your connection is not private":
 - 1) Click **Advanced**.
 - 2) Click **Proceed to 192.168.56.101 (unsafe)**.
- d. You will now see a LOGIN screen. Enter the following:
 - 1) Username: **cisco**
 - 2) Password: **cisco123!**
 - 3) Click **LOGIN NOW**.

You will now see the Dashboard for the CSR1000v. You are now accessing the CSR1000v's WebUI from the DEVASC virtual machine.

 https://192.168.56.101/webui/



LOGIN

Language: English | 日本語

LOGIN NOW

Step 6: From your local computer, access the CSR1000v WebUI (Web User Interface).

- a. Open a web browser on your local computer, not inside the **DEVASC VM**.
- b. For the URL, enter: **https://192.168.56.101**.
Note: Be sure to use "https".
- c. If your browser displays a warning similar to, "Your connection is not private":
 - 1) Click **Advanced**.
 - 2) Click **Proceed to 192.168.56.101 (unsafe)**.
- d. You will now see a LOGIN screen. Enter the following:
 - 1) Username: **cisco**
 - 2) Password: **cisco123!**
 - 3) Click **LOGIN NOW**.

You will now see the Dashboard for the CSR1000v. You are now accessing the CSR1000v's WebUI from your local computer.