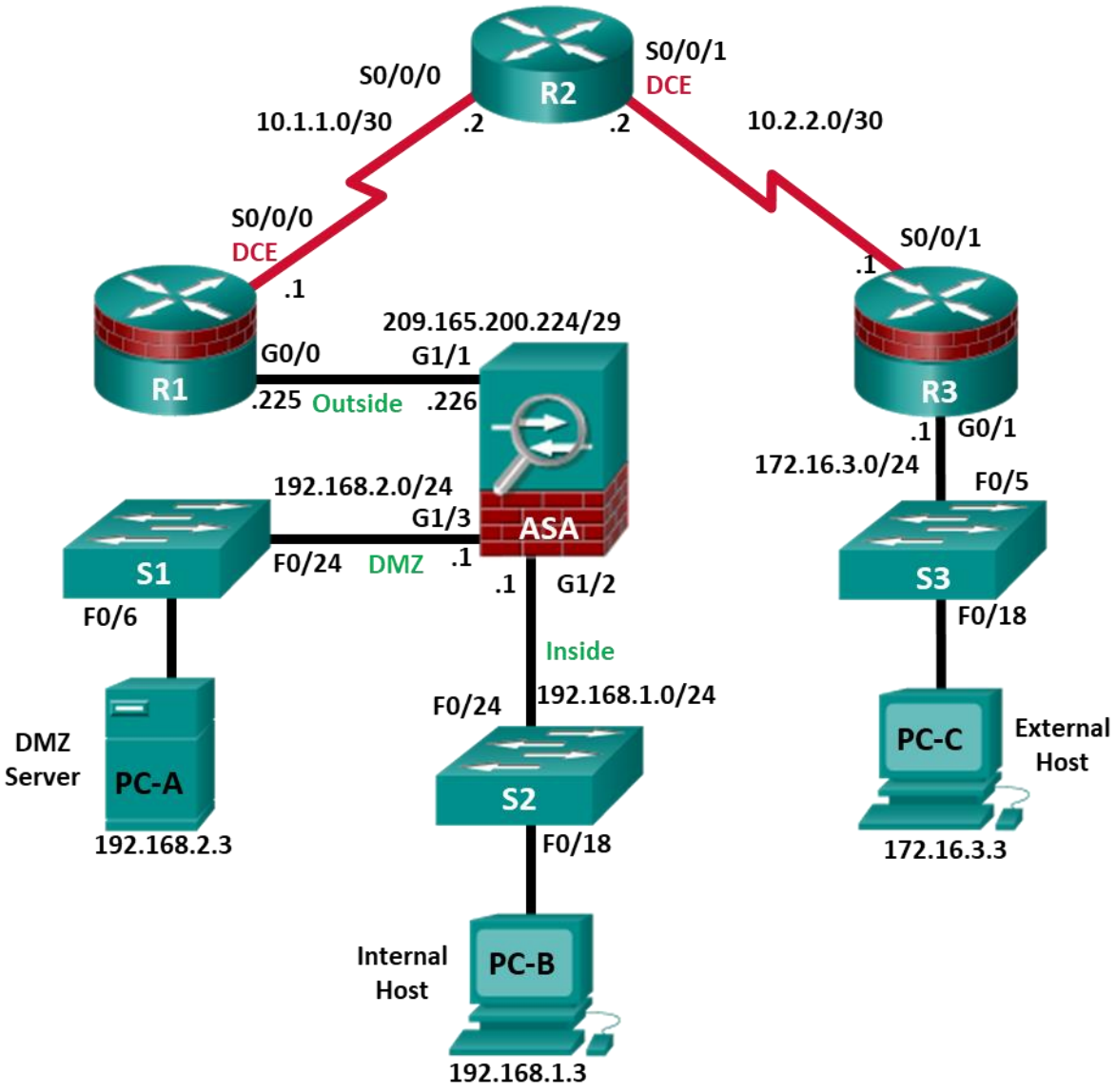
CCNA Security

Lab – Instructor Lab Using ASA 5506-X

Topology



Note: ISR G1 devices use FastEthernet interfaces instead of GigabitEthernet interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA G1/1
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
R2	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
R3	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	G1/1 (outside)	209.165.200.226	255.255.255.248	NA	R1 G0/0
ASA	G1/2 (inside)	192.168.1.1	255.255.255.0	NA	S2 F0/24
ASA	G1/3 (dmz)	192.168.2.1	255.255.255.0	NA	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Objectives

In this lab, you will initialize the router, switch, and ASA. You will download and install USB console software that allows the use of a mini-USB cable to access the console port on a Cisco device. You will also download the AnyConnect Secure Mobility Client Software and upload it to the ASA.

Part 1: Initialize and Reload Network Devices

- Initialize the router and reload.
- Enable the security technology package license.
- Initialize the switch and reload.
- Initialize the ASA.

Part 2: Access a Cisco Router Using a Mini-USB Console Cable

- Setup the physical connection with a mini-USB cable.
- Verify that the USB console is ready.
- Enable the COM port.

Part 3: Download and Install the AnyConnect Secure Mobility Client Software Package

- Download the AnyConnect Secure Mobility Client software from cisco.com.
- Upload AnyConnect Secure Mobility Client to ASA 5506-X.

Background/Scenario

Part 1 of this instructor lab provides the steps for initializing devices back to their default settings. Part 2 of this lab provides the steps necessary to set Java settings on the PC hosts. Part 3 of this lab provides optional information on how to download, install, and use the Cisco USB driver on a Windows PC.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology Package license)
- 3 Switches (Cisco 2960 with cryptography IOS image for SSH support – Release 15.0(2)SE7 or comparable)
- 1 ASA 5506-X (OS version 9.10(1) and ASDM version 7.10(1) and Base license or comparable)
- 3 PCs (Windows, SSH Client and Java version compatible with installed ASDM version)
- Serial and Ethernet cables, as shown in the topology
- Console cables to configure Cisco networking devices

Part 1: Initialize and Reload Network Devices

Task 1: Initialize the Router and Reload.

Step 1: Connect to the router.

Console into the router and enter privileged EXEC mode using the **enable** command.

```
Router> enable
Router#
```

Step 2: Erase the startup configuration file from NVRAM.

Type the **erase startup-config** command to remove the startup configuration from NVRAM.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Step 3: Enable the security technology package license.

a. Use the **show version** command to determine the technology packages that are available and enabled on the router.

```
R1# show version
<some output omitted>
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          disable
data          None          None          None

Configuration register is 0x2102
```

b. Enter the **license boot module c1900 technology-package securityk9** to enable the securityk9 technology package.

```
R1(config)# license boot module c1900 technology-package securityk9
R1(config)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Step 4: Reload the router.

Issue the **reload** command to remove old configurations from memory. When prompted to proceed with reload, press **Enter** to confirm the reload. Pressing any other key will abort the reload.

```
Router# reload
Proceed with reload? [confirm]


*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing **no** and press **Enter**.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 5: Bypass the initial configuration dialog.

After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press **Enter**.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Step 6: Terminate the autoinstall program.

You will be prompted to terminate the autoinstall program. Respond **yes** and then press **Enter**.

```
Would you like to terminate autoinstall? [yes]: yes
Router>
```

Task 2: Initialize the Switch and Reload.

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any VLANs created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash

Directory of flash:/

    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00  config.text
```

```
4   -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
5   -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
6   -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

Step 3: Delete the VLAN file.

a. If the **vlan.dat** file was found in flash, delete the file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

b. You will be prompted to verify the file name. At this point, you can change the file name or press **Enter** if you have entered the name correctly.

c. When you are prompted to delete this file, press **Enter** to confirm the deletion. Pressing any other key will abort the deletion.

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When prompted to remove the configuration file, press **Enter** to confirm the removal. Pressing any other key will abort the operation.

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove old configuration information from memory. When prompted to reload the switch, press **Enter** to proceed with the reload. Pressing any other key will abort the reload.

```
Switch# reload
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press **Enter**.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press **Enter**.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Task 3: Initialize the ASA and Reload

Step 1: Connect to the ASA.

a. Console into the ASA and enter privileged EXEC mode.

Note: If you press enter at the prompt **Pre-configure Firewall now through interactive prompts [yes]?**, press Ctrl-Z to exit the interactive prompts.

```
ciscoasa> enable
Password: <Enter>
```

Step 2: Erase the startup configuration file.

Use the **write erase** command to erase the startup configuration file from NVRAM. When prompted to remove the configuration file, press Enter to confirm the removal. Pressing any other key will abort the operation.

```
ciscoasa# write erase
Erase configuration in flash memory? [confirm]
[OK]
```

Step 3: Step 5: Reload the ASA.

Reload the switch to remove old configuration information from memory. When prompted to reload the switch, press Enter to proceed with the reload. Pressing any other key will abort the reload.

```
ciscoasa# reload
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 4: Step 6: Bypass the initial configuration dialog.

After the ASA reloads, you should see a prompt to enter the initial configuration dialog. Type no at the prompt and press Enter.

```
Pre-configure Firewall now through interactive prompts [yes]? no
ciscoasa>
```

Part 2: Access a Cisco Router Using a Mini-USB Console Cable

If you are using a Cisco 1941 router or other Cisco IOS devices with a mini-USB console port, you can access the device console port using a mini-USB cable connected to the USB port on your computer.

Note: The mini-USB console cable is the same type of mini-USB cable used with other electronics devices, such as USB hard drives, USB printers, or USB hubs. These mini-USB cables can be purchased through Cisco Systems, Inc. or other third-party vendors. Please verify that you are using a mini-USB cable, not a micro-USB cable, to connect to the mini-USB console port on a Cisco IOS device.

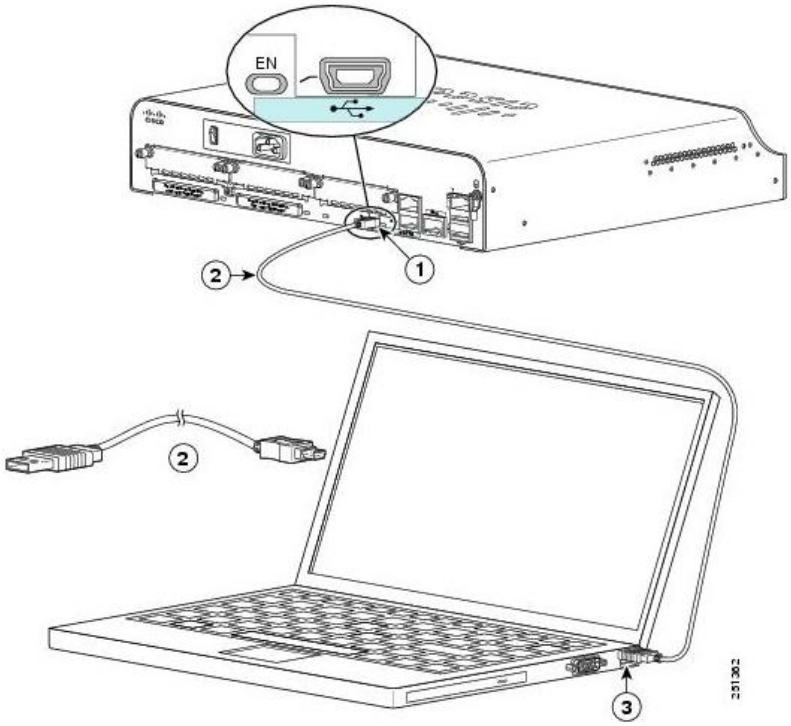
Note: You must use either the USB port or the RJ-45 port. Do not use them simultaneously. When the USB port is used, it takes priority over the RJ-45 console port.

Step 1: Set up the physical connection with a mini-USB cable.

a. Connect the mini-USB cable to the mini-USB console port of the router.

b. Connect the other cable end to a USB port on the computer.

c. Turn on the Cisco router and computer.



1) USB 5-pin mini Type-B console port
2) USB 5-pin mini Type-B to USB Type-A Console Cable
3) USB Type-A connector

Step 2: Verify that the USB console is ready.

If you are using a Microsoft Windows-based PC and the USB console port LED indicator (labeled EN) does not turn green, please install the Cisco USB console driver.

A USB driver must be installed prior to being used on a Microsoft Windows-based PC that is connecting to a Cisco IOS device with a USB cable. The USB driver can be found on www.cisco.com with the related Cisco IOS device. The USB driver can be downloaded from the following location:

https://software.cisco.com/download/home/282774238/type/282855122/release/3.1

Note: You must have a valid Cisco Connection Online (CCO) account to download this file.

Note: The URL provided above is specifically related to the Cisco 1941 router. However, the USB console driver is not Cisco IOS device-model specific, but it only works with Cisco routers and switches. The computer requires a reboot after finishing the installation of the USB driver.

Note: After the files are extracted, the folder contains instructions for installation, removal, and the required drivers for different operating systems and architectures. Please choose the appropriate version for your system.

When the LED indicator for the USB console port has turned green, the USB console port is ready for access.

a. Open the **Device Manager** to determine the associated COM port.

b. Click the **Ports (COM & LPT)** tree link to expand it. Right-click the **USB Serial Port** icon to determine the COM port associated with USB Serial Port. Take note of the assigned port number. In this sample, COM 5 is used for communication with the router.

c. Open **Tera Term**. Click the **Serial** radio button and choose **COM5: Cisco Serial (COM 5)**. If it is successful, skip the next step. Otherwise, perform the next step to enable to COM port.

Step 3: Enable the COM port for the Windows PC.

If you are using a Microsoft Windows PC, you may need to perform the following steps to enable the COM port:

a. Click the **Windows Start** icon to access the **Control Panel**.

b. Open the **Device Manager**.

c. Click the **Ports (COM & LPT)** tree link to expand it. Right-click the **USB Serial Port** icon to determine the COM port associated with USB Serial Port and choose **Update Driver Software**.

d. Choose **Browse my computer for driver software**.

e. Choose **Let me pick from a list of device drivers on my computer** and click **Next**.

f. Choose the **Cisco Serial** driver and click **Next**.

g. The device driver is installed successfully. Take note of the assigned port number listed at the top of the window. In this sample, COM 5 is used for communication with the router. Click **Close**.

h. Open **Tera Term**. Click the **Serial** radio button and choose **Port COM5: Cisco Serial (COM 5)**. This port should now be available for communication with the router. Click **OK**.

Part 3: Download and Install the AnyConnect Client Software Packages

Updated versions of Cisco's AnyConnect Client software packages can be downloaded from Cisco.com.

Note: AnyConnect client version 4.5 is available for download in CCNA Security Instructor Resources.

Step 1: Download the AnyConnect Secure Mobility Client software packages from cisco.com.

a. Using a browser, connect to the www.cisco.com and log in.

b. Click **Support & Downloads** > Search for **AnyConnect Secure Mobility Client v4.x**. or use this directly link for the available versions:

https://software.cisco.com/download/home/286281283/type/282364313/release/

c. Download the AnyConnect Headend Deployment Package (.pkg) version compatible with your operating system.

d. From the Download Software – Select a Product screen, click **AnyConnect Secure Mobility Client**.

Step 2: Upload the AnyConnect Secure Mobility Client to the ASA 5506-X.

a. After the AnyConnect client has been downloaded, connect the PC to the ASA 5506-X G1/2 interface and assign a static IP address of **192.168.1.3** with a subnet mask of **255.255.255.0**.

Note: This PC will also need TFTP server software installed. Free or trial versions of TFTP server can be downloaded from the Internet. Use a web browser to search for "free windows tftp server" and refer to the software documentation for more information.

The IP addresses used in this example are for reference only. The file **anyconnect-win-4.5.05030-webdeploy-k9.pkg** will be used in this example.

b. Configure the ASA's interface G1/2 with an IP address of **192.168.1.1**, a subnet mask of **255.255.255.0**, and the nameif to **inside**.

```
ciscoasa(config)# interface G1/2
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shut
```

c. Start the TFTP server software and verify that the AnyConnect Secuity Mobility Client is located in the default directory.

d. From the CLI on the ASA, issue the **copy tftp://192.168.1.1/ anyconnect-win-4.5.05030-webdeploy-k9.pkg flash:** command.

```
ciscoasa# copy tftp://192.168.1.3/anyconnect-win-4.5.05030-webdeploy-k9.pkg
flash:

Address or name of remote host [192.168.1.3]?

Source filename [anyconnect-win-4.5.05030-webdeploy-k9.pkg]?

Destination filename [anyconnect-win-4.5.05030-webdeploy-k9.pkg]?

Accessing tftp://192.168.1.3/anyconnect-win-4.5.05030-webdeploy-
k9.pkg...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/anyconnect-win-4.5.05030-webdeploy-k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
INFO: No digital signature found
35431181 bytes copied in 37.410 secs (957599 bytes/sec)
```

e. Issue the **show flash** command on the ASA to verify that the file has been uploaded to flash.

```
ciscoasa# show flash
--#--  --length--  -----date/time------  path
  121  35431181    Mar 04 2018 10:57:43  anyconnect-win-4.5.05030-webdeploy-k9.pkg
   21  4096        Aug 29 2017 13:16:38  coredumpinfo
   22  59          Aug 29 2017 13:16:38  coredumpinfo/coredump.cfg
   20  4096        Sep 17 2017 12:07:32  crypto_archive
  119  115316320   Feb 21 2018 18:01:22  asa9101-lfbff-k8.SPA
```

```
        120  34143680    Feb 21 2018 18:04:06  asdm-7101.bin

      7365472256 bytes total (3913506816 bytes free)
```

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces, identify the type of router used, and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.