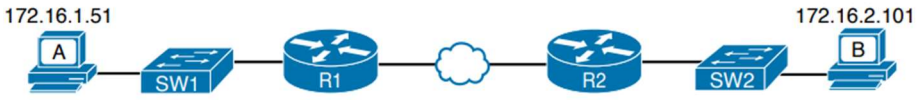
Device Hardening Config 1

In this lab, you'll learn how to harden the routers on your network using a number of different features including proper secured passwords, limited SSH access (Management server 192.168.1.100), banners, and disabling CDP. This begins with all devices already configured with IP addresses and routing.	

`R2#conf t`	Move into global configuration mode on the router you want to harden (R2 in this example, but you should do all routers)
`R2(config)#`**`enable secret cs`**	Configure an enable password in the most secure method supported with a password of **cs**
`R2(config)#`**`username cisco secret cs`**	Configure a user named **cisco** with a secret password of **cs**
`R2(config)#`**`ip domain-name testing.com`**	Configure a domain-name of **testing.com**
`R2(config)#`**`crypto key generate rsa`**	Generate an RSA key pair using a 2048 bit key.
`R2(config)#`**`ip ssh version 2`**	Enable SSH version 2
`R2(config)#`**`access-list 1 permit 192.168.1.100`**	Configure a standard ACL 1 permitting the management server IP address 192.168.1.100
`R2(config)#`**`line console 0`** `R2(config-line)#`**`login local`**	Move into console line configuration mode and configure it to require login using the local user database.
`R2(config-line)#`**`line vty 0 4`** `R2(config-line)#`**`login local`**	Move into terminal line configuration mode and also configure it to require a login using the local user database
`R2(config-line)#`**`transport input ssh`**	Configure the lines to only support SSH logins
`R2(config-line)#`**`access-class 1 in`**	Configure the lines to only allow access from the address specified in ACL 1.

`R2(config)#`**`banner motd #`**
`Enter TEXT message. End with the character '#'.`
 	
`UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED`
 	
`All activities performed on this device are logged and monitored`**`#`**
	Exit into global configuration mode and configure the following Message of the Day (MOTD) banner:
	
	UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
	
	All activities performed on this device are logged and monitored.

`R2(config)#`**`banner login #`** `Enter TEXT message.  End with the character '#'.` `LOGIN IS REQUIRED - UNAUTHORIZED ATTEMPTS TO ACCESS THIS DEVICE WILL BE LOGGED AND REPORTED`**`#`**	Configure the following login banner LOGIN IS REQUIRED - UNAUTHORIZED ATTEMPTS TO ACCESS THIS DEVICE WILL BE LOGGED AND REPORTED

`R2(config)#`**`banner exec #`**
`Enter TEXT message.  End with the character '#'.`
 	
`BY LOGGING INTO THIS SYSTEM, YOU ACKNOWLEDGE THAT YOU ARE AUTHORIZED`
 	
`If any changes are made to the configuration, ensure documentation has been provided on appropriate systems`**`#`**
	Configure the following EXEC banner
	
	BY LOGGING INTO THIS SYSTEM, YOU ACKNOWLEDGE THAT YOU ARE AUTHORIZED
	
	If any changes are made to the configuration, ensure documentation has been provided on appropriate systems

`R2(config)#`**`no cdp run`**	Disable CDP globally.