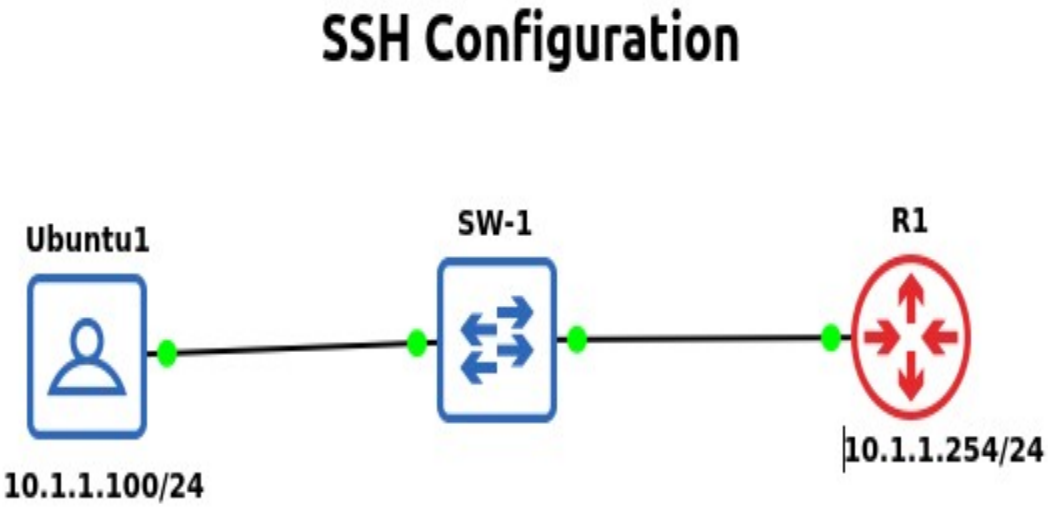
# SSH Configuration on a Router R1




**Objetivos de la Práctica**

Configurar el dispositivo **Router R1** para que pueda ser alcanzado a través de **SSH**.

**Actividades**

1.- Configurar el **hostname** y las **IPv4 address** en las correspondiente interfaz como se inica en la siguiente tabla.

| **HOSTNAME** | **IPv4 Address** |
|---|---|
| R1 | Gi0/0 --- 10.1.1.254 |

***Router#configure terminal***
***Router(config)#hostname R1***
***R1(config)#interface gi0/0***
***R1(config-if)#ip address 10.1.1.254 255.255.255.0***
***R1(config-if)#no shutdown***

2.- Configuración para el acceso privilegiado "**enable mode**" otorgando la contraseña "**ciscoonline**".
***R1(config)#enable secret ciscoonline***

Pasos para la configuración de **SSH** en dispositivos de Capa 2 y/o Capa 3.

1. Crear el usuario "**admin**" con la contraseña "**admin12345**" con un nivel de **privilegios 15**.

***R1(config)#username admin privilege 15 secret admin12345***

2.- Definir el nombre del dominio en "**ccnacourse.com**".

***R1(config)#ip domain-name ccnacourse.com***

3.- Cree las llaves **publicas** y **privadas** de **SSH**.

***R1(config)#crypto key generate rsa modulus 2048***

4.- habilite **SSHv2** en los dispositivos y que solo se permitan 2 intentos de autenticación.
***R1(config)#ip ssh version 2***
***R1(config)#ip ssh authentication-retries 2***

5.- Dentro de la línea de **consola 0**

1. Habilitar la línea de consola para que permita el logeo del usuario "**admin**".
2. Habilitar "**logging synchronous**"
3. Habilitar el tiempo que durará la seccion activa si es que se no existe alguna actividad en 5 minutos.

***R1(config)#line console 0***
***R1(config-line)#login local***
***R1(config-line)#loggin synchronous***
***R1(config-line)#exec-timeout 5 0***

6.- Dentro de las líneas **vty 0 4:**

1. Habilitar las línea de consola para que permita el logeo del usuario "**admin**".
2. Habilitar "**logging synchronous**".
3. Habilitar el tiempo que durará la seccion activa si es que se no existe alguna actividad en 5 minutos.

***R1(config)#line vty 0 4***
***R1(config-line)#login local***
***R1(config-line)#loggin synchronous***
***R1(config-line)#exec-timeout 5 0***

7.- Habilitar la conexiónes entrantes y/o salientes a través de **SSH**.

***R1(config-line)#transport input ssh***
***R1(config-line)#transport output ssh***

9.- Encripte las contraseñas que el IOS guarda en texto plano

***R1(config)#service password-encryption***

10.- Pruebe la conectividad con un **cliente SSH** hacia el **Router R1**.

```
root@Ubuntu1:~# ssh -l admin 10.1.1.254
The authenticity of host '10.1.1.254 (10.1.1.254)' can't be established.
RSA key fingerprint is SHA256:wh56a/KbxKVAlJcn+Qfj5sqxKAQijfk0y/mfolDLQpQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.1.254' (RSA) to the list of known hosts.

**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************Password:
```

# Comandos utililes para esta práctica.

**show running-config**
**copy running-config startup-config**