

Guía para la Configuración de Usuarios y Niveles de Privilegios en Routers Cisco



Objetivo:

Configurar diferentes niveles de acceso para usuarios en un router Cisco, permitiendo la segmentación de privilegios entre Administradores, Usuarios Avanzados y Usuarios de Solo Lectura. Esto es esencial para aplicar mejores prácticas de seguridad, limitando los privilegios de los usuarios según sus necesidades.

1. Conceptos Básicos de Niveles de Privilegios en Cisco

Cisco IOS tiene 16 niveles de privilegios que van del **0** (el más bajo) al **15** (el más alto). De forma predeterminada:

- **Nivel 0:** Comandos básicos como `logout` y `exit`.
- **Nivel 1:** Comandos de visualización, como `show`.
- **Nivel 15:** Acceso completo a todos los comandos.

Niveles que configuraremos:

- **Privilegio 15:** Administrador (acceso completo).
- **Privilegio 5:** Usuario avanzado (acceso limitado a algunos comandos).
- **Privilegio 3:** Usuario de solo lectura (acceso solo a comandos de visualización).

2. Paso a Paso para Configurar Usuarios

2.1 Usuario con Privilegios de Administrador (Privilegio 15)

Este usuario tendrá acceso completo a la configuración y diagnóstico del router, además de la capacidad de agregar, modificar y eliminar otros usuarios.

Iniciar sesión en el router en modo global de configuración.

Crear el usuario con privilegios de administrador:

```
# Router(config)# username admin privilege 15 secret [contraseña]
```

- **username admin:** Nombre de usuario.
- **privilege 15:** Nivel de privilegio 15 (acceso completo).
- **secret [contraseña]:** Contraseña para el usuario.

Configurar la contraseña de **enable** para proteger el acceso privilegiado:

bash

```
# Router(config)# enable secret [contraseña_enable]
```

2.2 Usuario con Privilegios Limitados (Usuario Avanzado - Privilegio 5)

Este usuario podrá ejecutar comandos básicos como **ping** y ver la configuración del router, pero no podrá modificarla.

Definir qué comandos estarán disponibles para el nivel de privilegio 5:

```
# Router(config)# privilege exec level 5 show running-config  
# Router(config)# privilege exec level 5 ping
```

Crear el usuario con nivel de privilegio 5:

```
# Router(config)# username usuario_avanzado privilege 5 secret  
[contraseña]
```

2.3 Usuario de Solo Lectura (Privilegio 3)

Este usuario tendrá acceso únicamente para visualizar el estado y la configuración del router, sin permisos para ejecutar pruebas de diagnóstico o modificar configuraciones.

Definir los comandos permitidos para el nivel de privilegio 3:

```
# Router(config)# privilege exec level 3 show running-config
```

Crear el usuario con nivel de privilegio 3:

```
# Router(config)# username solo_lectura privilege 3 secret  
[contraseña]
```

1.

3. Configuración de Acceso Remoto mediante SSH

Para que los usuarios puedan conectarse al router mediante SSH y acceder según sus privilegios, sigue estos pasos:

Configura las líneas **vty** (líneas virtuales de terminal):

```
# Router(config)# line vty 0 4  
# Router(config-line)# login local  
# Router(config-line)# transport input ssh
```

1.

Habilita SSH si aún no está configurado:

```
# Router(config)# ip domain-name [dominio]  
# Router(config)# crypto key generate rsa  
# Router(config)# ip ssh version 2
```

4. Revisión y Verificación de Usuarios y Privilegios

4.1 Ver los Usuarios Configurados

Para ver una lista de los usuarios configurados en el router:

```
# Router# show running-config | include username
```

4.2 Verificar los Niveles de Privilegios

Para verificar los comandos permitidos a un usuario con un nivel específico:

```
# Router# show privilege
```

4.3 Probar Acceso SSH

Conéctate al router desde un dispositivo externo usando SSH para verificar que los usuarios tengan los privilegios adecuados:

```
#ssh [usuario]@[dirección_IP_del_router]
```
