

# Los niveles de privilegio de IOS no pueden ver la configuración completa en ejecución

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Ver la configuración del router](#)

[Nivel de privilegio](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento explica cómo los niveles de privilegio afectan a la capacidad de un usuario de ejecutar ciertos comandos en un router.

## [Prerequisites](#)

## [Requirements](#)

No hay requisitos específicos para este documento.

## [Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

## [Convenciones](#)

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

## [Ver la configuración del router](#)

Cuando el acceso al router se configura mediante niveles de privilegio, un problema común es que los comandos **show running** o **write terminal** se configuran con un nivel de privilegio de usuario o inferior a este. Cuando el usuario ejecuta el comando, la configuración aparece en blanco. En realidad, esto sucede a propósito por los siguientes motivos:

- El comando **write terminal/show running-confi** muestra una configuración en blanco. Este comando muestra todos los comandos que el usuario actual puede modificar (en otras palabras, todos los comandos con el nivel de privilegio actual del usuario o inferior a este). El comando no debe mostrar comandos con un nivel de privilegio superior al actual del usuario por cuestiones de seguridad. Si fuera así, los comandos como **snmp-server community** podrían utilizarse para modificar la configuración actual del router y obtener acceso completo al router.
- El comando **show config / show start-up config** muestra una configuración completa, pero no se muestra auténticamente la configuración real. El comando, en cambio, simplemente imprime el contenido de NVRAM, que es la configuración del router en el momento en que el usuario ejecuta un comando **write memory**.

## Nivel de privilegio

Para habilitar a un usuario con privilegios para que vea toda la configuración en la memoria, el usuario debe modificar los privilegios para todos los comandos que se configuran en el router. Por ejemplo:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local

username john privilege 9 password 0 doe
username six privilege 6 password 0 six
username poweruser privilege 15 password poweruser
username inout password inout
username inout privilege 15 autocommand show running

privilege configure level 8 snmp-server community
privilege exec level 6 show running
privilege exec level 8 configure terminal
```

Para entender este ejemplo, es necesario comprender los niveles de privilegio. De forma predeterminada, hay tres niveles de comando en el router:

- Nivel de privilegio 0: incluye los comandos **disable**, **enable**, **exit**, **help** y **logout**.
- Nivel de privilegio 1: es el nivel normal en Telnet e incluye todos los comandos de nivel de usuario en la petición de entrada `router>`.
- Nivel de privilegio 15: incluye todos los comandos de nivel de habilitación en la petición de entrada `router#`.

Para encontrar los comandos disponibles en un nivel específico de un router en particular, escriba `?` en la petición de entrada `router`. Se puede utilizar el comando **privilege para cambiar los niveles de privilegio para los comandos, como se muestra en el ejemplo**. Si bien en este ejemplo se muestran la autenticación y la autorización locales, los comandos funcionan de forma similar para la autenticación y ejecución de autorización TACACS+ o RADIUS (se puede lograr un control más granular del router con la implementación de la autorización de comando TACACS+ con un servidor).

En el ejemplo se presentan detalles adicionales sobre los usuarios y los niveles de privilegio:

- El usuario *six* es capaz de usar Telnet y ejecutar el comando **show run**, pero la configuración

que se obtiene como resultado se muestra prácticamente en blanco porque este usuario no puede realizar ninguna configuración (el comando `configure terminal` está en el nivel 8, no en nivel 6). El usuario no está autorizado para ver los nombres de usuario y las contraseñas de los demás usuarios, ni para ver información del Protocolo simple de administración de redes (SNMP).

- El usuario john puede usar Telnet y ejecutar el comando **show run**, pero solo verá los comandos que puede configurar (es decir, la parte `snmp-server community` de la configuración del router, ya que este usuario es el administrador de nuestra red). Puede configurar `snmp-server community` porque `configure terminal` está en el nivel 8 (en o debajo del nivel 9) y `snmp-server community` es un comando de nivel 8. El usuario no está autorizado para ver los nombres de usuario y contraseñas de los demás usuarios, pero se le confía la configuración de SNMP.
- El usuario inout puede usar Telnet y, por estar configurado para **autocommand show running**, verá la configuración que se muestra, pero se desconectará posteriormente.
- El usuario poweruser puede usar Telnet y ejecutar el comando **show run**. Este usuario está en el nivel 15 y puede ver todos los comandos. Todos los comandos están en o por debajo del nivel 15. Los usuarios con este nivel también pueden ver y controlar los nombres de usuario y las contraseñas.

## [Información Relacionada](#)

- [Comando lookup tool \(sólo para clientes registrados\)](#)
- [Documentación de IOS para TACACS + y RADIUS](#)
- [Página de soporte de TACACS/TACACS+](#)
- [Página de soporte de RADIUS](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico - Cisco Systems](#)