

Los niveles de privilegio IOS no pueden considerar la configuración corriente completa

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Vea la configuración del router](#)

[Niveles 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.

[prerrequisitos](#)

[Requisitos](#)

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](#)

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

[Vea la configuración del router](#)

Cuando el acceso al router es configurado por los niveles de privilegio, un problema frecuente es que configuran a los **comandos show running or write terminal** en o por debajo del nivel de privilegio del usuario. Cuando el usuario ejecuta el comando, la configuración aparece ser en blanco. Esto está realmente por el diseño por estas razones:

- **La terminal/el comando show running-config de la escritura** muestra una configuración vacía. Este comando visualiza todos los comandos que el Usuario usuario actual puede modificarse (es decir todos los comandos en o por debajo del nivel de privilegio actual del usuario). El comando no debe los comandos display sobre el nivel de privilegio actual del usuario debido a las observaciones de seguridad. Si es así los comandos tales como **comunidad del SNMP-servidor** se podían utilizar para modificar la configuración actual del router y para tener el acceso completo al router.
- **El comando show config/show start-up config** visualiza una configuración total, pero no muestra verdad la configuración real. En lugar, el comando imprime simplemente el contenido del NVRAM, que sucede ser la configuración del router que el usuario hace en ese entonces una **memoria de la escritura**.

Niveles de privilegio

Para permitir a un usuario con privilegios para ver la configuración completa en la memoria, el usuario necesita modificar los privilegios para los comandos all 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 entender los niveles de privilegio. Por abandono, hay tres niveles del comando en el router:

- nivel de privilegio 0 — Incluye la **neutralización, permiso, los comandos exit, help, y logout**.
- nivel de privilegio 1 — Nivel normal en Telnet; incluye todos los comandos del nivel de usuario en el prompt del `router>`.
- nivel de privilegio 15 — Incluye todos los comandos del permiso-nivel en el prompt del `router-`

¿Los comandos disponibles en un nivel determinado en un router determinado pueden ser encontrados tecleando `a?` en el prompt de router. Los comandos se pueden mover entre los niveles de privilegio usando el **comando privilege**, como se ilustra en el ejemplo. Mientras que este ejemplo muestra la autenticación local y autorización, los comandos trabajan semejantemente para el TACACS+ o la autenticación de RADIUS y la autorización de EXEC (más granularity en control del router se puede alcanzar con la implementación de la autorización del comando tacacs+ con un servidor.)

Detalles adicionales en los usuarios y los niveles de privilegio presentados en el ejemplo:

- El usuario *seis* puede a Telnet adentro y ejecuta el **comando show run**, pero la configuración resultante es virtualmente en blanco porque este usuario no puede configurar cualquier cosa

(**configurado terminal** está en el nivel 8, no en el nivel 6). No permiten al usuario para ver los nombres de usuario y contraseña de los otros usuarios, o para ver la información del Simple Network Management Protocol (SNMP).

- Usuario john puede a Telnet adentro y ejecuta el **comando show run**, pero ve solamente los comandos que él puede configurar (la parte de la **comunidad del SNMP-servidor** la configuración del router, puesto que este usuario es nuestro administrador de la Administración de redes). Él puede configurar a la **comunidad del SNMP-servidor** porque **está configurado terminal** está en el nivel 8 (en o por debajo del nivel 9), y de la **comunidad del SNMP-servidor** es un comando del nivel 8. No permiten al usuario para ver los nombres de usuario y contraseña de los otros usuarios, sino que lo confían en con la configuración SNMP.
- El usuario inout puede a Telnet adentro, y, en virtud de ser configurado para el **funcionamiento de la demostración del autocommand**, ve la configuración visualizada pero se desconecta después de eso.
- El poweruser usuario puede a Telnet adentro y ejecuta el **comando show run**. Este usuario puede en el nivel 15, y es ver los comandos all. Los comandos all están en o por debajo del nivel 15; los usuarios a este nivel pueden también ver y controlar los nombres de usuario y contraseña.

[Información Relacionada](#)

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