

IOS Privilege Levels Cannot See Complete Running Configuration

Document ID: 23383

Introduction

Prerequisites

Requirements

Components Used

Conventions

View the Router Configuration

Privilege Levels

Related Information

Introduction

This document explains how privilege levels affect a user's ability to perform certain commands on a router.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

View the Router Configuration

When access to the router is configured by privilege levels, a common issue is that the **show running** or **write terminal** commands are configured at or below the user's privilege level. When the user executes the command, the configuration appears to be blank. This is actually by design for these reasons:

- The **write terminal** / **show running-config** command shows a blank configuration. This command displays all of the commands that the current user is able to modify (in other words, all the commands at or below the user's current privilege level). The command should not display commands above the user's current privilege level because of security considerations. If so, commands such as **snmp-server community** could be used to modify the current configuration of the router and gain complete access to the router.
- The **show config** / **show start-up config** command displays a full configuration, but does not truly show the actual configuration. Instead, the command simply prints out the contents of NVRAM, which happens to be the configuration of the router at the time the user does a **write memory**.

Privilege Levels

To enable a privileged user to view the entire configuration in memory, the user needs to modify privileges for all commands that are configured on the router. For example:

```
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
```

To understand this example, it is necessary to understand privilege levels. By default, there are three command levels on the router:

- privilege level 0 Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands.
- privilege level 1 Normal level on Telnet; includes all user-level commands at the `router>` prompt.
- privilege level 15 Includes all enable-level commands at the `router#` prompt.

Commands available at a particular level in a particular router can be found by typing a `?` at the router prompt. Commands may be moved between privilege levels by using the **privilege** command, as illustrated in the example. While this example shows local authentication and authorization, the commands work similarly for TACACS+ or RADIUS authentication and exec authorization (more granularity in control of the router may be achieved with implementation of TACACS+ command authorization with a server.)

Additional details on the users and privilege levels presented in the example:

- User *six* is able to Telnet in and execute the **show run** command, but the resulting configuration is virtually blank because this user cannot configure anything (**configure terminal** is at level 8, not at level 6). The user is not permitted to see usernames and passwords of the other users, or to see Simple Network Management Protocol (SNMP) information.
 - User *john* is able to Telnet in and execute the **show run** command, but only sees commands that he can configure (the **snmp-server community** part of the router configuration, since this user is our network management administrator). He can configure **snmp-server community** because **configure terminal** is at level 8 (at or below level 9), and **snmp-server community** is a level 8 command. The user is not permitted to see usernames and passwords of the other users, but he is trusted with the SNMP configuration.
 - User *inout* is able to Telnet in, and, by virtue of being configured for **autocommand show running**, sees the configuration displayed but is disconnected thereafter.
 - User *poweruser* is able to Telnet in and execute the **show run** command. This user is at level 15, and is able to see all commands. All commands are at or below level 15; users at this level can also view and control usernames and passwords.
-

Related Information

- **Command Lookup Tool** (registered customers only)
 - **IOS Documentation for TACACS+ and RADIUS**
 - **TACACS/TACACS+ Support Page**
 - **RADIUS Support Page**
 - **Requests for Comments (RFCs)**
 - **Technical Support – Cisco Systems**
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 24, 2007

Document ID: 23383
