Role-Based CLI Access

The Role-Based CLI Access feature allows the network administrator to define “views,” which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

Feature History for Role-Based CLI Access

Release	Modification
12.3(7)T	This feature was introduced.
12.3(11)T	The CLI view capability was extended to restrict user access on a per-interface level, and additional CLI views were introduced to support the extended view capability. Also, support to group configured CLI views into a superview was introduced.
12.2(33)SRB	This feature was integrated into Cisco IOS Release 12.2(33)SRB.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Role-Based CLI Access

Your image must support CLI views.

Restrictions for Role-Based CLI Access

Lawful Intercept Images Limitation

Because CLI views are a part of the Cisco IOS parser, CLI views are a part of all platforms and Cisco IOS images. However, the lawful intercept view is available only in images that contain the lawful intercept subsystem.

Maximum Number of Allowed Views

The maximum number of CLI views and superviews, including one lawful intercept view, that can be configured is 15. (This does not include the root view.)

Information About Role-Based CLI Access

To create and use views, you should understand the following concepts:

Benefits of Using CLI Views

Views: Detailed Access Control

Although users can control CLI access via both privilege levels and enable mode passwords, these functions do not provide network administrators with the necessary level of detail needed when working with Cisco IOS routers and switches. CLI views provide a more detailed access control capability for network administrators, thereby, improving the overall security and accountability of Cisco IOS software.

As of Cisco IOS Release 12.3(11)T, network administrators can also specify an interface or a group of interfaces to a view; thereby, allowing access on the basis of specified interfaces.

Root View

When a system is in “root view,” it has all of the access privileges as a user who has level 15 privileges. If the administrator wishes to configure any view to the system (such as a CLI view, a superview, or a lawful intercept view), the system must be in root view.

The difference between a user who has level 15 privileges and a root view user is that a root view user can configure a new view and add or remove commands from the view. Also, when you are in a CLI view, you have access only to the commands that have been added to that view by the root view user.

View Authentication via a New AAA Attribute

View authentication is performed by an external authentication, authorization, and accounting (AAA) server via the new attribute "cli-view-name."

AAA authentication associates only one view name to a particular user; that is, only one view name can be configured for a user in an authentication server.

How to Use Role-Based CLI Access

This section contains the following procedures:

- Configuring a CLI View, page 3 (required)
- Configuring a Lawful Intercept View, page 5 (optional)
- Configuring a Superview, page 7 (optional)
- Monitoring Views and View Users, page 9 (optional)

Configuring a CLI View

Use this task to create a CLI view and add commands or interfaces to the view, as appropriate.

Prerequisites

Before you create a view, you must perform the following tasks:

- Enable AAA via the **aaa new-model** command. (For more information on enabling AAA, see the chapter "Configuring Authentication" in the *Cisco IOS Security Configuration Guide*, Release 12.3.
- Ensure that your system is in root view—not privilege level 15.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **parser view** *view-name*
4. **secret 5** *encrypted-password*
5. **commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*]
6. **exit**
7. **exit**
8. **enable** [*privilege-level*] [**view** *view-name*]
9. **show parser view** [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable view** **Example:** `Router> enable view`	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**parser view** *view-name* **Example:** `Router(config)# parser view first`	Creates a view and enters view configuration mode.
Step 4	**secret 5** *encrypted-password* **Example:** `Router(config-view)# secret 5 secret`	Associates a command-line interface (CLI) view or superview with a password. **Note** You must issue this command before you can configure additional attributes for the view.
Step 5	**commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*] **Example:** `Router(config-view)# commands exec include show version`	Adds commands or interfaces to a view. • *parser-mode*—The mode in which the specified command exists. • **include**—Adds a command or an interface to the view and allows the same command or interface to be added to an additional view. • **include-exclusive**—Adds a command or an interface to the view and excludes the same command or interface from being added to all other views. • **exclude**—Excludes a command or an interface from the view; that is, customers cannot access a command or an interface. • **all**—A "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view. • **interface** *interface-name*— Interface that is added to the view. • *command*—Command that is added to the view.
Step 6	**exit** **Example:** `Router(config-view)# exit`	Exits view configuration mode.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 8	**enable** [*privilege-level*] [**view** *view-name*] **Example:** `Router# enable view first`	Prompts the user for a password, which allows the user to access a configured CLI view, and is used to switch from one view to another view. After the correct password is given, the user can access the view.
Step 9	**show parser view** [**all**] **Example:** `Router# show parser view`	(Optional) Displays information about the view that the user is currently in. • **all**—Displays information for all views that are configured on the router. **Note** Although this command is available for both root and lawful intercept users, the **all** keyword is available only to root users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.

Troubleshooting Tips

After you have successfully created a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_CREATED: view 'first' successfully created.
```

After you have successfully deleted a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_DELETED: view 'first' successfully deleted.
```

You must associate a password with a view. If you do not associate a password, and you attempt to add commands to the view via the **commands** command, a system message such as the following will be displayed:

```
%Password not set for view <viewname>.
```

Configuring a Lawful Intercept View

Use this task to initialize and configure a view for lawful-intercept-specific commands and configuration information. (Only an administrator or a user who has level 15 privileges can initialize a lawful intercept view.)

About Lawful Intercept Views

Like a CLI view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that store information about calls and users.

Commands available in lawful intercept view belong to one of the following categories:

- Lawful intercept commands that should not be made available to any other view or privilege level
- CLI views that are useful for lawful intercept users but do not have to be excluded from other views or privilege levels

Prerequisites

Before you initialize a lawful intercept view, ensure that the privilege level is set to 15 via the **privilege** command.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **li-view** *li-password* **user** *username* **password** *password*
4. **username** [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*
5. **parser view** *view-name*
6. **secret 5** *encrypted-password*
7. **name** *new-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable view** **Example:** `Router> enable view`	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**li-view** *li-password* **user** *username* **password** *password* **Example:** `Router(config)# li-view lipass user li_admin password li_adminpass`	Initializes a lawful intercept view. After the li-view is initialized, you must specify at least one user via **user** *username* **password** *password* options.
Step 4	**username** [**lawful-intercept** [*name*] [**privilege** *privilege-level* | **view** *view-name*] **password** *password* **Example:** `Router(config)# username lawful-intercept li-user1 password li-user1pass`	Configures lawful intercept users on a Cisco device.

	Command or Action	Purpose
Step 5	**parser view** *view-name* **Example:** `Router(config)# parser view li view name`	(Optional) Enters view configuration mode, which allows you to change the lawful intercept view password or the lawful intercept view name.
Step 6	**secret 5** *encrypted-password* **Example:** `Router(config-view)# secret 5 secret`	(Optional) Changes an existing password for a lawful intercept view.
Step 7	**name** *new-name* **Example:** `Router(config-view)# name second`	(Optional) Changes the name of a lawful intercept view. If this command is not issued, the default name of the lawful intercept view is "li-view."

Troubleshooting Tips

To display information for all users who have access to a lawful intercept view, issue the **show users lawful-intercept** command. (This command is available only to authorized lawful intercept view users.)

Configuring a Superview

Use this task to create a superview and add at least one CLI view to the superview.

About Superviews

A superview consists of one or more CLI views, which allow users to define what commands are accepted and what configuration information is visible. Superviews allow a network administrator to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.

Superviews contain the following characteristics:

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview; that is, you must add commands to the CLI view and add that CLI view to the superview.
- Users who are logged into a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.
- If a superview is deleted, all CLI views associated with that superview will not be deleted too.

Adding CLI Views to a Superview

You can add a view to a superview only after a password has been configured for the superview (via the **secret 5** command). Thereafter, issue the **view** command in view configuration mode to add at least one CLI view to the superview.

Note Before adding a CLI view to a superview, ensure that the CLI views that are added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **parser view** *superview-name* **superview**
4. **secret 5** *encrypted-password*
5. **view** *view-name*
6. **exit**
7. **exit**
8. **show parser view** [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable view** **Example:** `Router> enable view`	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**parser view** *superview-name* **superview** **Example:** `Router(config)# parser view su_view1 superview`	Creates a superview and enters view configuration mode.
Step 4	**secret 5** *encrypted-password* **Example:** `Router(config-view)# secret 5 secret`	Associates a CLI view or superview with a password. **Note** You must issue this command before you can configure additional attributes for the view.
Step 5	**view** *view-name* **Example:** `Router(config-view)# view view_three`	Adds a normal CLI view to a superview. Issue this command for each CLI view that is to be added to a given superview.
Step 6	**exit** **Example:** `Router(config-view)# exit`	Exits view configuration mode.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 8	**show parser view** [**all**] **Example:** `Router# show parser view`	(Optional) Displays information about the view that the user is currently in. • **all**—Displays information for all views that are configured on the router. **Note** Although this command is available for both root and lawful intercept users, the **all** keyword is available only to root users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.

Monitoring Views and View Users

To display debug messages for all views—root, CLI, lawful intercept, and super, use the **debug parser view** command in privileged EXEC mode.

Configuration Examples for Role-Based CLI Access

This section contains the following configuration examples:

Configuring a CLI View: Example

The following example shows how to configure two CLI views, “first” and “second.” Thereafter, you can verify the CLI view in the running configuration.

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# secret 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# secret 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
!
```

```
!
Router(config-view)# do show run | beg view
parser view first
 secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show ip
 commands exec include show version
 commands exec include show
!
parser view second
 secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
 commands exec include-exclusive show ip interface
 commands exec include show ip
 commands exec include show
 commands exec include logout
!
```

Verifying a CLI View: Example

After you have configured the CLI views “first” and “second,” you can issue the **enable view** command to verify which commands are available in each view. The following example shows which commands are available inside the CLI view “first” after the user has logged into this view. (Because the **show ip** command is configured with the all option, a complete set of suboptions is shown, except the **show ip interface** command, which is using the include-exclusive keyword in the second view.)

```
Router# enable view first
Password:

00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information

Router# show ?

  ip       IP information
  parser   Display parser information
  version  System hardware and software status

Router# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
```

```
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Router Discovery Protocol
.
.
.
```

Configuring a Lawful Intercept View: Example

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added:

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# end

! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
Password:

Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view
Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views

Router(config-view)#

! NOTE:LI View configurations are never shown as part of 'running-configuration'.

! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass
Router(config)# username lawful-intercept li-user2 password li-user2pass

! Displaying LI User information.
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

Configuring a Superview: Example

The following sample output from the **show running-config** command shows that “view_one” and “view_two” have been added to superview “su_view1,” and “view_three” and “view_four” have been added to superview “su_view2”:

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

Additional References

The following sections provide references related to Role-Based CLI Access.

Related Documents

Related Topic	Document Title
SNMP, MIBs, CLI configuration	*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*, Release 12.3
Privilege levels	*Cisco IOS Security Configuration Guide*, Release 12.3

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents only new and modified commands.

New Commands in Cisco IOS Release 12.3(7)T and 12.2(33)SRB

- **commands (view)**
- **li-view**
- **name (view)**
- **parser view**
- **show parser view**

New Commands in Cisco IOS Release 12.3(11)T and 12.2(33)SRB

- **parser view superview**
- **view**

New Command in Cisco IOS Release 12.3(14)T

- **secret**

Modified Commands in Cisco IOS Release 12.3(7)T and 12.2(33)SRB

- **enable**
- **show users**
- **username**

Modified Commands in Cisco IOS Release 12.3(11)T and 12.2(33)SRB

- **commands (view)**

commands (view)

To add commands or an interface to a command-line interface (CLI) view, use the **commands** command in view configuration mode. To delete a command or an interface from a CLI view, use the **no** form of this command.

Syntax for Adding and Deleting Commands to a View

commands *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [*command*]

no commands *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [*command*]

Syntax for Adding and Deleting Interfaces to a View

commands *parser-mode* {**include** | **include-exclusive**} [**all**] [**interface** *interface-name*] [*command*]

no commands *parser-mode* {**include** | **include-exclusive**} [**all**] [**interface** *interface-name*] [*command*]

Syntax Description

parser-mode	Mode in which the specified command exists. See Table 1 in the "Usage Guidelines" section for a list of available options for this argument.
include	Adds a specified command or a specified interface to the view and allows the same command or interface to be added to an additional view.
include-exclusive	Adds a specified command or a specified interface to the view and excludes the same command or interface from being added to all other views.
exclude	Denies access to commands in the specified parser mode. **Note** This keyword is available only for command-based views.
all	(Optional) A "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface within a specified interface to be part of the view.
interface *interface-name*	(Optional) Interface that is added to the view.
command	(Optional) Command that is added to the view. **Note** If no commands are specified, all commands within the specified parser mode are included or excluded, as appropriate.

Defaults

If this command is not enabled, a view will not have adequate information to deny or allow access to users.

Command Modes

View configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	The **exclude** keyword and the **interface** *interface-name* option were added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If a network administrator does not enter a specific command (via the *command* argument) or interface (via the **interface** *interface-name* option), users are granted access (via the **include** or **include-exclusive** keywords) or denied access (via the **exclude** keyword) to all commands within the specified parser-mode.

parser-mode Options

Table 1 shows some of the keyword options for the *parser-mode* argument in the **commands** command. The available mode keywords vary depending on your hardware and software version. To see a list of available mode options on your system, use the **commands ?** command.

Table 1 parser-mode Argument Options

Command	Description
accept-dialin	VPDN group accept dialin configuration mode
accept-dialout	VPDN group accept dialout configuration mode
address-family	Address Family configuration mode
alps-ascu	ALPS ASCU configuration mode
alps-circuit	ALPS circuit configuration mode
atm-bm-config	ATM bundle member configuration mode
atm-bundle-config	ATM bundle configuration mode
atm-vc-config	ATM virtual circuit configuration mode
atmsig_e164_table_mode	ATMSIG E164 Table
cascustom	Channel-associated signalling (cas) custom configuration mode
config-rtr-http	RTR HTTP raw request Configuration
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map config mode
crypto-transform	Crypto transform config modeCrypto transform configuration mode
dhcp	DHCP pool configuration mode
dspfarm	DSP farm configuration mode
exec	EXEC mode
flow-cache	Flow aggregation cache configuration mode
gateway	Gateway configuration mode
interface	Interface configuration mode

Table 1 parser-mode Argument Options (continued)

Command	Description
interface-dlci	Frame Relay DLCI configuration mode
ipenacl	IP named extended access-list configuration mode
ipsnacl	IP named simple access-list configuration mode
ip-vrf	Configure IP VRF parameters
lane	ATM Lan Emulation Lecs Configuration Table
line	Line configuration mode
map-class	Map class configuration mode
map-list	Map list configuration mode
mpoa-client	MPOA Client
mpoa-server	MPOA Server
null-interface	Null interface configuration mode
preaut	AAA Preauth definitions
request-dialin	VPDN group request dialin configuration mode
request-dialout	VPDN group request dialout configuration mode
route-map	Route map configuration mode
router	Router configuration mode
rsvp_policy_local	RSVP local policy configuration mode
rtr	RTR Entry Configuration
sg-radius	RADIUS server group definition
sg-tacacs+	TACACS+ server group
sip-ua	SIP UA configuration mode
subscriber-policy	Subscriber policy configuration mode
tcl	Tcl mode
tdm-conn	TDM connection configuration mode
template	Template configuration mode
translation-rule	Translation Rule configuration mode
vc-class	VC class configuration mode
voiceclass	Voice Class configuration mode
voiceport	Voice configuration mode
voipdialpeer	Dial Peer configuration mode
vpdn-group	VPDN group configuration mode

Examples

The following example shows how to add the privileged EXEC command **show version** to both CLI views “first” and “second.” Because the **include** keyword was issued, the **show version** command can be added to both views.

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
```

```
Router(config-view)# commands exec include show version
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include show version
```

The following example shows how to allow users in the view “first” to execute all commands that start with the word “show” except the **show interfaces** command, which is excluded by the view “second”:

```
Router(config)# parser view first
Router(config-view)# secret 5 secret
Router(config-view)# commands exec include all show
!
Router(config)# parser view second
Router(config-view)# secret 5 myview
Router(config-view)# commands exec include-exclusive show interfaces
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.

enable

To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** command in user EXEC or privileged EXEC mode.

enable [*privilege-level*] [**view** [*view-name*]]

Syntax Description

privilege-level	(Optional) Privilege level at which to log in.
view	(Optional) Enters into root view, which enables users to configure CLI views. **Note** This keyword is required if you want to configure a CLI view.
view-name	(Optional) Enters or exits a specified command-line interface (CLI) view. This keyword can be used to switch from one CLI view to another CLI view.

Defaults

Privilege-level 15 (privileged EXEC)

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **view** keyword and *view-name* argument were integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the **enable password** global configuration command, you are prompted to enter the password before being allowed access to privileged EXEC mode. The password is case sensitive.

If an **enable** password has not been set, only enable mode can be accessed through the console connection.

Security levels can be set by an administrator using the **enable password** and **privilege level** commands. Up to 16 privilege levels can be specified, using the numbers 0 through 15. Using these privilege levels, the administrator can allow or deny access to specific commands. Privilege level 0 is associated with user EXEC mode, and privilege level 15 is associated with privileged EXEC mode.

For more information on defined privilege levels, see the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference* publications.

If a level is not specified when entering the **enable** command, the user will enter the default mode of privileged EXEC (level 15).

Accessing a CLI View

CLI views restrict user access to specified CLI and configuration information. To configure and access CLI views, users must first enter into root view, which is accomplished via the **enable view** command (without the *view-name* argument). Thereafter, users are prompted for a password, which is the same password as the privilege level 15 password.

The *view-name* argument is used to switch from one view to another view.

To prevent dictionary attacks, a user is prompted for a password even if an incorrect view name is given. The user is denied access only after an incorrect view name and password are given.

Examples

In the following example, the user enters privileged EXEC mode using the **enable** command. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is the greater than symbol (>), and the prompt for privileged EXEC mode is the number sign (#).

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

This following example shows which commands are available inside the CLI view “first” after the user has logged into this view:

```
Router# enable view first

Password:

00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information

Router# show ?

  ip       IP information
  parser   Display parser information
  version  System hardware and software status

Router# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
```

```
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Router Discovery Protocol
.
.
.
```

The following command shows how to issue the **enable view** command to switch from the root view to the CLI view "first":

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view

Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all

Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view "first."
Router# enable view first
Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view "first."
Router# show parser view

Current view is 'first'
```

Related Commands

Command	Description
disable	Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.
enable password	Sets a local password to control access to various privilege levels.
privilege level (global)	Sets a privilege level for a command.
privilege level (line)	Sets a privilege level for a command for a specific line.

li-view

To initialize a lawful intercept view, use the **li-view** command in global configuration mode.

li-view *li-password* **user** *username* **password** *password*

Syntax Description

li-password	Associates the lawful interface view with a password. The password can contain any number of alphanumeric characters. **Note** The password is case sensitive.
user *username*	User who can access the lawful intercept view.
password *password*	Associates a password with the specified **user** *username* option; that is, the user must provide the specified password to access the view.

Defaults

A lawful intercept view cannot be accessed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Like a command-line interface (CLI) view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that stores information about calls and users.

Commands available in lawful intercept view belong to one of the following categories:

- Lawful intercept commands that should not be made available to any other view or privilege level.
- CLI that are useful for lawful intercept users but do not need to be excluded from other views or privilege levels.

Note Only a system administrator or a level 15 privilege user can initialize a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added to the view:

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# end
```

```
! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
Password:

Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view
Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views

Router(config-view)#

! NOTE:LI View configurations are never shown as part of 'running-configuration'.

! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass
Router(config)# username lawful-intercept li-user2 password li-user2pass

! Displaying LI User information.
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
show users	Displays information about the active lines on the router.
username	Establishes a username-based authentication system.

name (view)

To change the name of a lawful intercept view, use the **name** command in view configuration mode. To return to the default lawful intercept view name, which is "li-view," use the **no** form of this command.

name *new-name*

no name *new-name*

Syntax Description

new-name	Lawful intercept view name.

Defaults

A lawful intercept view is called "li-view."

Command Modes

View configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Only a system administrator or a level 15 privilege user can change the name of a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view and change the view name to "myliview":

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# name myliview
Router(config-view)# end
```

Related Commands

Command	Description
li-view	Creates a lawful intercept view.
parser view	Creates or changes a CLI view and enters view configuration mode.

parser view

To create or change a command-line interface (CLI) view and enter view configuration mode, use the **parser view** command in global configuration mode. To delete a view, use the **no** form of this command.

parser view *view-name*

no parser view *view-name*

Syntax Description

view-name	View name, which can include 1 to 30 alphanumeric characters. The *view-name* argument must not have a number as the first character; otherwise, you will receive the following error message: "Invalid view name."

Defaults

A CLI view does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

A CLI view is a set of operational commands and configuration capabilities that restrict user access to the CLI and configuration information; that is, a view allows users to define what commands are accepted and what configuration information is visible.

After you have issued the **parser view** command, you can configure the view via the **secret 5** command and the **commands** command.

To use the **parser view** command, the system of the user must be set to root view. The root view can be enabled via the **enable view** command.

Examples

The following example show how to configure two CLI views, "first" and "second."

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# secret 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# secret 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
```

```
Router(config-view)# command exec include logout
Router(config-view)# exit
```

After you have successfully created a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_CREATED: view 'first' successfully created.
```

After you have successfully deleted a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_DELETED: view 'first' successfully deleted.
```

Related Commands

Command	Description
commands (view)	Adds commands to a CLI view.
secret 5	Associates a CLI view or a superview with a password.

parser view superview

To create a superview and enter view configuration mode, use the **parser view superview** command in global configuration mode. To delete a superview, use the **no** form of this command.

parser view *superview-name* **superview**

no parser view *superview-name* **superview**

Syntax Description

superview-name	Superview name, which can include 1 to 30 alphanumeric characters. The *superview-name* argument must not have a number as the first character.

Defaults

A superview does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

A superview consists of one or more command-line interface (CLI) views, which allow users to define what commands are accepted and what configuration information is visible. Superviews allow a network administrator to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.

Superviews contain the following characteristics:

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview; that is, you must add commands to the CLI view and add that CLI view to the superview.
- Users who are logged into a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.

Adding CLI Views to a Superview

You can add a view to a superview only after a password has been configured for the superview (via the **secret 5** command). Thereafter, issue the **view** command in view configuration mode to add at least one CLI view to the superview.

Note Before adding a CLI view to a superview, ensure that the CLI views that are added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Examples

The following sample output from the **show running-config** command shows that "view_one" and "view_two" have been added to superview "su_view1," and "view_three" and "view_four" have been added to superview "su_view2":

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.
view	Adds a normal CLI view to a superview.

secret

To associate a command-line interface (CLI) view or a superview with a password, use the **secret** command in view configuration mode.

secret {*unencrypted-password* | **0** *unencrypted-password* | **5** *encrypted-password*}

Syntax Description

unencrypted-password	Nonencrypted password. A password can contain any combination of alphanumeric characters. The password is case sensitive. This clear-text password will be encrypted using the Message Digest 5 (MD5) method.
0	Specifes that an unencrypted password will follow.
5	Specifes that an encrypted password will follow.
encrypted-password	Encrypted password that you enter and that is copied from another router configuration.

Defaults

User cannot access a CLI view or superview.

Command Modes

View configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

A user cannot access any commands within the CLI view or superview until the **secret** command has been issued.

Note The password cannot be removed, but you can overwrite it.

Examples

The following examples show how to configure two CLI views, “first” and “second,” and associate each view with a password:

CLI View “first”

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view first
Router(config-view)#
*Dec  9 05:20:03.039: %PARSER-6-VIEW_CREATED: view 'first' successfully created.
Router(config-view)# secret firstpassword
Router(config-view)# secret secondpassword
% Overwriting existing secret for the current view
Router(config-view)# secret 0 thirdpassword
% Overwriting existing secret for the current view
Router(config-view)# secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
% Overwriting existing secret for the current view
```

```
Router(config-view)# secret 5 invalidpassword
ERROR: The secret you entered is not a valid encrypted secret.
To enter an UNENCRYPTED secret, do not specify type 5 encryption.
When you properly enter an UNENCRYPTED secret, it will be encrypted.

Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command configure include all ip
Router(config-view)# exit
```

CLI View "second"

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view second
Router(config-view)#
*Dec 30 06:11:52.915: %PARSER-6-VIEW_CREATED: view 'second' successfully created.
Router(config-view)# secret mypasswd
Router(config-view)# commands exec include ping
Router(config-view)# end

Router# show running-config

parser view second
 secret 5 $1$PWs8$lz3lSx6OqAnFrUx2hkI0w0
 commands exec include ping
!
```

The following is an example of **show running-config** output for a situation in which the **secret** command has been configured using a level 5 encrypted password:

```
Router: show running-config

parser view first
 secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
 commands configure include all ip
 commands exec include configure terminal
 commands exec include configure
 commands exec include show version
 commands exec include show
!
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

show parser view

To display command-line interface (CLI) view information, use the **show parser view** command in privileged EXEC mode.

show parser view [**all**]

Syntax Description

all	(Optional) Displays information about all CLI views that are configured on the router.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The **show parser view** command will display information only about the view that the user is currently in. This command is available for both root view users and lawful intercept view users—except for the **all** keyword, which is available only to root view users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view.

The **show parser view** command cannot be excluded from any view.

Examples

The following example shows how to display information from the root view and the CLI view “first”:

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view
Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all
Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view “first.”
Router# enable view first
Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view “first.”
Router# show parser view
Current view is 'first'
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

show users

To display information about the active lines on the router, use the **show users** command in privileged EXEC mode.

show users [**all**] [**lawful-intercept**]

Syntax Description

all	(Optional) Specifies that all lines be displayed, regardless of whether anyone is using them.
lawful-intercept	(Optional) Displays lawful-intercept users.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The **lawful-intercept** keyword was introduced.
12.2(33)SRB	The **lawful-intercept** keyword was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command displays the line number, connection name, idle time, hosts (including virtual access interfaces), and terminal location. An asterisk (*) indicates the current terminal session.

If the **lawful-intercept** keyword is issued, the names of all users who have access to a configured lawful intercept view will be displayed. To access the **show users lawful-intercept** command, you must be an authorized lawful-intercept-view user.

Examples

The following is sample output from the **show users** command:

```
Router# show users
     Line          User           Host(s)       Idle Location
     0 con 0                      idle
*    2 vty 0       user1          idle           0   SERVICE1.CISCO.COM
```

The following is sample output identifying an active virtual access interface:

```
Router# show users

Line         User      Host(s)                Idle    Location
*  0 con 0             idle                   01:58
  10 vty 0             Virtual-Access2         0      1212321
```

The following is sample output from the **show users all** command:

```
Router# show users all
      Line      User         Host(s)     Idle  Location
*   0 vty 0   user1        idle         0    SERVICE1.CISCO.COM
    1 vty 1
       2 con 0
       3 aux 0
       4 vty 2
```

Table 2 describes the significant fields shown in the displays.

Table 2 show users Field Descriptions

Field	Description
Line	Contains three subfields: • The first subfield (0 in the sample output) is the absolute line number. • The second subfield (vty in the sample output) indicates the type of line. Possible values follow: con—console aux—auxiliary port tty—asynchronous terminal port vty—virtual terminal • The third subfield (0 in the * sample output) indicates the relative line number within the type.
User	User using the line. If no user is listed in this field, no one is using the line.
Host(s)	Host to which the user is connected (outgoing connection). A value of idle means that there is no outgoing connection to a host.
Idle	Interval (in minutes) since the user has entered something.
Location	Either the hard-wired location for the line or, if there is an incoming connection, the host from which incoming connection came.

The following sample output from the **show users lawful intercept** command, shows three LI-View users on the system—li_admin, li-user1, and li-user2":

```
Router# show users lawful-intercept
li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.
li-view	Creates a lawful intercept view.
show line	Displays the parameters of a terminal line.
username	Establishes a username-based authentication system.

username

To establish a username-based authentication system, use the **username** command in global configuration mode. Use the **no** form of this command to remove an established username-based authentication.

username *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}

username *name* **password** *secret*

username *name* [**access-class** *number*]

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]

username *name* **dnis**

username *name* [**nocallback-verify**]

username *name* [**noescape**] [**nohangup**]

username *name* [**privilege** *level*]

username *name* **user-maxlinks** *number*

username [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*

no username *name*

Syntax Description

name	Host name, server name, user ID, or command name. The name argument can be only one word. Blank spaces and quotation marks are not allowed.
nopassword	No password is required for this user to log in. This is usually most useful in combination with the **autocommand** keyword.
password	Specifies a possibly encrypted password for this username.
password	Password a user enters.
encryption-type	Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.
encrypted-password	Encrypted password a user enters.
password	Password to access the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.

secret	For CHAP authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
access-class	(Optional) Specifies an outgoing access list that overrides the access list specified in the **access-class** line configuration command. It is used for the duration of the user's session.
number	(Optional) Access list number.
autocommand	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and contain embedded spaces, commands using the **autocommand** keyword must be the last option on the line.
command	(Optional) The command string. Because the command can be any length and contain embedded spaces, commands using the **autocommand** keyword must be the last option on the line.
callback-dialstring	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
telephone-number	(Optional) For asynchronous callback only: telephone number to pass to the DCE device.
callback-rotary	(Optional) For asynchronous callback only: permits you to specify a rotary group number. The next available line in the rotary group is selected.
rotary-group-number	(Optional) For asynchronous callback only: integer between 1 and 100 that identifies the group of lines on which you want to enable a specific username for callback.
callback-line	(Optional) For asynchronous callback only: specific line on which you enable a specific username for callback.
tty	(Optional) For asynchronous callback only: standard asynchronous line.
line-number	(Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you want to enable a specific username for callback. Numbering begins with zero.
ending-line-number	(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as **tty**), then *line-number* and *ending-line-number* are absolute rather than relative line numbers.
dnis	Do not require password when obtained via DNIS.
nocallback-verify	(Optional) Authentication not required for EXEC callback on the specified line.
noescape	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
nohangup	(Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the **autocommand** keyword) has completed. Instead, the user gets another EXEC prompt.
privilege	(Optional) Sets the privilege level for the user.
level	(Optional) Number between 0 and 15 that specifies the privilege level for the user.

user-maxlinks	Limit the user's number of inbound links.
number	User-maxlinks limit for inbound links.
lawful-intercept	(Optional) Configures lawful intercept users on a Cisco device.
name	Host name, server name, user ID, or command name. The name argument can be only one word. Blank spaces and quotation marks are not allowed.
privilege	(Optional) Sets the privilege level for the user.
privilege-level	(Optional) Number between 0 and 15 that specifies the privilege level for the user.
view	(Optional) For command-line interface (CLI) view only: associates a CLI view name with the local authentication, authorization, and accounting (AAA) database.
view-name	(Optional) For CLI view only: view name, which was specified via the **parser view** command, that is to be associated with the AAA local database.
password *password*	Password to access the CLI view.

Defaults

No username-based authentication system is established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The following keywords and arguments were added: • **username** *name* [**callback-dialstring** *telephone-number*] • **username** *name* [**callback-rotary** *rotary-group-number*] • **username** *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]] • **username** *name* [**nocallback-verify**]
12.3(7)T	The following keywords and arguments were added: • **lawful-intercept** • **view** • *view-name*
12.2(33)SRB	The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SRB: • **lawful-intercept** • **view** • *view-name*

Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

Multiple **username** commands can be used to specify options for a single user.

Add a username entry for each remote system with which the local router communicates and from which it requires authentication. The remote device must have a username entry for the local router. This entry must have the same password as the local router's entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for the Challenge Handshake Authentication Protocol (CHAP). Add a username entry for each remote system from which the local router requires authentication.

Note To enable the local router to respond to remote CHAP challenges, one **username** *name* entry must be the same as the **hostname** entry that has already been assigned to the other router.

Note To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1 (for example, 0 or 2 through 15).

Note Per-user privilege levels override virtual terminal (VTY) privilege levels.

CLI and Lawful Intercept Views

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that stores information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view, by default, if no other privilege level or view name has been explicitly specified.

If there is no *secret* specified and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. CHAP debugging information is available using the **debug ppp negotiation, debug serial-interface,** and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example implements a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router:

```
username who nopassword nohangup autocommand show users
```

The following example implements an information service that does not require a password to be used. The command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example implements an ID that works even if all the TACACS+ servers break. The command takes the following form:

```
username superuser password superpassword
```

The following example enables CHAP on interface serial 0 of "server_l." It also defines a password for a remote server named "server_r."

```
hostname server_l
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

When you look at your configuration file, the passwords will be encrypted, and the display will look similar to the following:

```
hostname server_l
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

In both of the following configuration examples, a privilege level 1 user is denied access to privilege levels higher than 1:

```
username user privilege 0 password 0 cisco

username user 2 privilege 2 password 0 cisco
```

The following example removes the username-based authentication for user 2:

```
no username user 2
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
callback forced-wait	Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
ppp callback (PPP client)	Enables a PPP client to dial into an asynchronous interface and request a callback.
show users	Displays information about the active lines on the router.

view

To add a normal command-line interface (CLI) view to a superview, use the **view** command in view configuration mode. To remove a CLI view from a superview, use the **no** form of this command.

view *view-name*

no view *view-name*

Syntax Description

view-name	CLI view that is to be added to the given superview.

Defaults

A superview will not contain any CLI views until this command is enabled.

Command Modes

View configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Before you can use this command to add normal views to a superview, ensure that the following steps have been taken:

- A password has been configured for the superview (via the **secret 5** command).
- The normal views that are to be added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Examples

The following sample output from the **show running-config** command shows that “view_one” and “view_two” have been added to superview “su_view1,” and “view_three” and “view_four” have been added to superview “su_view2”:

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.