



Passwords and Privileges Commands

This chapter describes the commands used to establish password protection and configure privilege levels. Password protection lets you restrict access to a network or a network device. Privilege levels let you define what commands users can issue after they have logged in to a network device.

For information on how to establish password protection or configure privilege levels, refer to the “Configuring Passwords and Privileges” chapter in the *Cisco IOS Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the “Passwords and Privileges Configuration Examples” section located at the end of the “Configuring Passwords and Privileges” chapter in the *Cisco IOS Security Configuration Guide*.

enable password

To set a local password to control access to various privilege levels, use the **enable password** command in global configuration mode. To remove the password requirement, use the **no** form of this command.

enable password [**level** *level*] {*password* | [*encryption-type*] *encrypted-password*}

no enable password [**level** *level*]

Syntax Description

level <i>level</i>	(Optional) Level for which the password applies. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the no form of the command, the privilege level defaults to 15 (traditional enable privileges).
<i>password</i>	Password users type to enter enable mode.
<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 5. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

Defaults

No password is defined. The default is level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines



Caution

If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command with the **level** option to define a password for a specific privilege level. After you specify the level and the password, give the password to the users who need to access this level. Use the **privilege level** configuration command to specify commands accessible at various levels.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you copy and paste into this command a password that has already been encrypted by a Cisco router.



Caution

If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If the **service password-encryption** command is set, the encrypted form of the password you create with the **enable password** command is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
- Must not have a number as the first character.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password *abc?123*, do the following:
 - Enter **abc**.
 - Type **Ctrl-v**.
 - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter *abc?123* at the password prompt.

Examples

The following example enables the password “pswd2” for privilege level 2:

```
enable password level 2 pswd2
```

The following example sets the encrypted password “\$1\$i5Rkls3LoyxzS8t9”, which has been copied from a router configuration file, for privilege level 2 using encryption type 7:

```
enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

Related Commands

Command	Description
disable	Exits privileged EXEC mode and returns to user EXEC mode.
enable	Enters privileged EXEC mode.
enable secret	Specifies an additional layer of security over the enable password command.
privilege	Configures a new privilege level for users and associate commands with that privilege level.
service password-encryption	Encrypts passwords.
show privilege	Displays your current level of privilege.

enable secret

To specify an additional layer of security over the **enable password** command, use the **enable secret** command in global configuration mode. To turn off the **enable secret** function, use the **no** form of this command.

enable secret [*level level*] {*password* | [*encryption-type*] *encrypted-password*}

no enable secret [*level level*]

Syntax Description

<i>level level</i>	(Optional) Level for which the password applies. You can specify up to sixteen privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or in the no form of the command, the privilege level defaults to 15 (traditional enable privileges). The same holds true for the no form of the command.
<i>password</i>	Password for users to enter enable mode. This password should be different from the password created with the enable password command.
<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available for this command is 5. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).
<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

Defaults

No password is defined. The default level is 15.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines



Caution

If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command to provide an additional layer of security over the enable password. The **enable secret** command provides better security by storing the enable secret password using a non-reversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you paste into this command an encrypted password that you copied from a router configuration file.

**Caution**

If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If you use the same password for the **enable password** and **enable secret** commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the **enable secret** command provides.

**Note**

After you set a password using the **enable secret** command, a password set using the **enable password** command works only if the **enable secret** is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image. Additionally, you cannot recover a lost password that has been encrypted by any method.

If **service password-encryption** is set, the encrypted form of the password you create here is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters
- Must not have a number as the first character
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password *abc?123*, do the following:
 - Enter **abc**.
 - Type **Ctrl-v**.
 - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter **abc?123** at the password prompt.

Examples

The following example specifies the enable secret password of “greentree”:

```
enable secret greentree
```

After specifying an enable secret password, users must enter this password to gain access. Any passwords set through enable password will no longer work.

```
Password: greentree
```

The following example enables the encrypted password “\$1\$FaD0\$Xyti5Rkls3LoyxzS8”, which has been copied from a router configuration file, for privilege level 2 using encryption type 5:

```
enable password level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

■ enable secret

Related Commands	Command	Description
	enable	Enters privileged EXEC mode.
	enable password	Sets a local password to control access to various privilege levels.

password

To specify a password on a line, use the **password** command in line configuration mode. To remove the password, use the **no** form of this command.

password *password*

no password

Syntax Description

<i>password</i>	Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, hello 21 is a legal password, but 21 hello is not. The password checking is case sensitive. For example, the password Secret is different than the password secret.
-----------------	---

Defaults

No password is specified.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When an EXEC process is started on a line with password protection, the EXEC prompts for the password. If the user enters the correct password, the EXEC prints its normal privileged prompt. The user can try three times to enter a password before the EXEC exits and returns the terminal to the idle state.

Examples

The following example removes the password from virtual terminal lines 1 to 4:

```
line vty 1 4
no password
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.

privilege

To configure a new privilege level for users and associate commands with that privilege level, use the **privilege** command in global configuration mode. Use the **no** form of this command to revert to default privileges for the specified command.

privilege *mode* [**all**] {**level** *level* | **reset**} *command-string*

no privilege *mode* [**all**] {**level** *level* | **reset**} *command-string*

Syntax Description

<i>mode</i>	Configuration mode for the specified command. See Table 36 in the “Usage Guidelines” section for a list of options for this argument.
all	(Optional) Changes the privilege level for all the suboptions to the same level.
level <i>level</i>	Specifies the privilege level you are configuring for the specified command or commands. The level argument must be a number from 0 to 15.
reset	Resets the privilege level of the specified command or commands to the default and removes the privilege level configuration from the running-config file. Note If you use the no form of this command to reset the privilege level to the default, the default form of this command will still appear in the configuration file. To completely remove a privilege configuration, use the reset keyword.
<i>command-string</i>	Command associated with the specified privilege level. If the all keyword is used, specifies the command and subcommands associated with the privilege level.

Defaults

User EXEC mode commands are privilege level 1.

Privileged EXEC mode and configuration mode commands are privilege level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(22)S, 12.2(13)T	The all keyword was added.

Usage Guidelines

The password for a privilege level defined using the **privilege** global configuration command is configured using the **enable secret** command.

Level 0 can be used to specify a more-limited subset of commands for specific users or lines. For example, you can allow user “guest” to use only the **show users** and **exit** commands.


Note

There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included.

When you set the privilege level for a command with multiple words, note that the commands starting with the first word will also have the specified access level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15—unless you set them individually to different levels. This is necessary because you can't execute, for example, the **show ip** command unless you have access to **show** commands.

To change the privilege level of a group of commands, use the **all** keyword. When you set a group of commands to a privilege level using the **all** keyword, all commands which match the beginning string are enabled for that level, and all commands which are available in submodes of that command are enabled for that level. For example, if you set the **show ip** keywords to level 5, **show** and **ip** will be changed to level 5 and all the options that follow the **show ip** string (such as **show ip accounting**, **show ip aliases**, **show ip bgp**, and so on) will be available at privilege level 5.

Table 36 shows some of the keyword options for the mode argument in the **privilege** command. The available mode keywords will vary depending on your hardware and software version. To see a list of available mode options on your system, use the **privilege ?** command.

Table 36 Mode Argument Options

Command	Description
accept-dialin	VPDN Accept-dialin group configuration mode
accept-dialout	VPDN Accept-dialout group configuration mode
address-family	Address family configuration mode
alps-ascu	ALPS ASCU configuration mode
alps-circuit	ALPS circuit configuration mode
atm-bm-config	ATM VC bundle-member configuration mode
atm-bundle-config	ATM VC bundle configuration mode
atm-vc-config	ATM virtual circuit (VC) configuration mode
atmsig_e164_table_mode	ATMSIG E164 Table
cascustom	CAS custom configuration mode
config-rtr-http	SAA/RTR HTTP raw request configuration mode
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map configuration mode
crypto-transform	Crypto 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

Table 36 Mode Argument Options (continued)

Command	Description
interface	Interface configuration mode
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 Request-dialin group configuration mode
request-dialout	VPDN Request-dialout group configuration mode
route-map	Route map configuration mode
router	Router configuration mode
rsvp-local-policy	RSVP local policy configuration mode
rtr	SAA/RTR configuration mode
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 configuration 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 set the **configure** command to privilege level 14 and establish SecretPswd14 as the password users must enter to use level 14 commands:

```
privilege exec level 14 configure
enable secret level 14 SecretPswd14
```

The following example shows how to set the **show** and **ip** keywords to level 5. The suboptions coming under **ip** will also be allowed to users with privilege level 5 access:

```
Router(config)# privilege exec all level 5 show ip
```

The following two examples demonstrate the difference in behavior between the **no** form of the command and the use of the **reset** keyword.

```
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no privilege exec level 3 configure terminal
Router(config)# end
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 15 configure terminal
privilege exec level 15 configure
```

Note that in the **show running-config** output above, the privilege command for “configure terminal” still appears, but now has the default privilege level assigned.

To remove a previously configured privilege command entirely from the configuration, use the **reset** keyword, as shown in the following example:

```
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# privilege exec reset configure terminal
Router(config)#
Router# show running-config | include priv
privilege configure all level 3 interface
Router#
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
privilege level	Sets the default privilege level for a line.

privilege level

To set the default privilege level for a line, use the **privilege level** command in line configuration mode. To restore the default user privilege level to the line, use the **no** form of this command.

privilege level *level*

no privilege level

Syntax Description

<i>level</i>	Privilege level associated with the specified line.
--------------	---

Defaults

Level 15 is the level of access permitted by the enable password.

Level 1 is normal EXEC-mode user privileges.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Users can override the privilege level you set using this command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level.

You can use level 0 to specify a subset of commands for specific users or lines. For example, you can allow user “guest” to use only the **show users** and **exit** commands.

You might specify a high level of privilege for your console line to restrict line usage.

Examples

The following example configures the auxiliary line for privilege level 5. Anyone using the auxiliary line has privilege level 5 by default:

```
line aux 0
 privilege level 5
```

The following example sets all **show ip** commands, which includes all **show** commands, to privilege level 7:

```
privilege exec level 7 show ip route
```

This is equivalent to the following command:

```
privilege exec level 7 show
```

The following example sets the **show ip route** to level 7 and the **show** and **show ip** commands to level 1:

```
privilege exec level 7 show ip route
privilege exec level 1 show ip
```

Related Commands	Command	Description
	enable password	Sets a local password to control access to various privilege levels.

service password-encryption

To encrypt passwords, use the **service password-encryption** command in global configuration mode. To restore the default, use the **no** form of this command.

service password-encryption

no service password-encryption

Syntax Description This command has no arguments or keywords.

Defaults No encryption

Command Modes Global configuration

Release	Modification
10.0	This command was introduced.

Usage Guidelines The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **more system:running-config** command is entered.



Caution

This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.



Note

You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

Examples The following example causes password encryption to take place:

```
service password-encryption
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
key-string (authentication)	Specifies the authentication string for a key.
neighbor password	Enables MD5 authentication on a TCP connection between two BGP peers.

show privilege

To display your current level of privilege, use the **show privilege** command in EXEC mode.

show privilege

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines Use this command to display your current level of privilege.

Examples The following example shows sample output from the **show privilege** command. The current privilege level is 15.

```
Router# show privilege
Current privilege level is 15
```

Related Commands	Command	Description
	enable password	Sets a local password to control access to various privilege levels.
	enable secret	Specifies an additional layer of security over the enable password command.

username

To establish a username-based authentication system, use the **username** command in global configuration mode.

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*

Syntax Description

<i>name</i>	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.
<i>password</i>	Password a user enters.
<i>encryption-type</i>	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.
<i>encrypted-password</i>	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.

<i>secret</i>	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.
<i>number</i>	(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.
<i>command</i>	(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.
<i>telephone-number</i>	(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.
<i>rotary-group-number</i>	(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.
<i>line-number</i>	(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.
<i>ending-line-number</i>	(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 <i>line-number</i> and <i>ending-line-number</i> 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.
<i>level</i>	(Optional) Number between 0 and 15 that specifies the privilege level for the user.

user-maxlinks	Limit the user's number of inbound links.
<i>number</i>	User-maxlinks limit for inbound links.
lawful-intercept	(Optional) Configures lawful intercept users on a Cisco device.
<i>name</i>	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.
<i>privilege-level</i>	(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.
<i>view-name</i>	(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 <i>password</i>	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: <ul style="list-style-type: none"> • username <i>name</i> [callback-dialstring <i>telephone-number</i>] • username <i>name</i> [callback-rotary <i>rotary-group-number</i>] • username <i>name</i> [callback-line [tty] <i>line-number</i> [<i>ending-line-number</i>]] • username <i>name</i> [nocallback-verify]
12.3(7)T	The following keywords and arguments were added: <ul style="list-style-type: none"> • lawful-intercept • view • <i>view-name</i>

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_1.” It also defines a password for a remote server named “server_r.”

```
hostname server_1
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_1
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
```

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.

username secret

To encrypt a user password with Message Digest 5 (MD5) encryption, use the **username secret** command in global configuration mode.

```
username name secret {[0] password | 5 encrypted-secret}
```

Syntax Description

<i>name</i>	Username.
0	(Optional) Clear text password, which will be MD5 encrypted.
<i>password</i>	Clear text password.
5 encrypted-secret	MD5-encrypted text string, which will be stored as the encrypted user password.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use the **username secret** command to configure a username and MD5-encrypted user password. The optional **0** keyword enables MD5 encryption on a clear text password; the **5** keyword enters an MD5 encryption string and saves it as the user MD5-encrypted secret. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

The **username secret** command provides an additional layer of security over the username password. It also provides better security by encrypting the password using nonreversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Use MD5 as the encryption type if you paste into this command an encrypted password that you copied from a router configuration file.

Examples

The following example shows how to configure username “abc” and enable MD5 encryption on the clear text password “xyz”:

```
username abc secret xyz
```

The following example shows how to configure username “cde” and enter an MD5 encrypted text string that is stored as the username password:

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
username	Establishes a username-based authentication system.

■ username secret