CHAPTER 5

Security Commands

This chapter describes the commands you use to configure router security.

Note The command syntax includes a combination of bold and regular uppercase and lowercase alphanumeric characters. You can enter commands in full or you can enter abbreviated forms of many commands. The abbreviated form consists of the first characters in each word of the syntax that appear in bold uppercase type in command syntax in this chapter. These characters represent the minimum you must enter for the command to be recognized and executed.

login

To log in to a remote router to make configuration changes, use the **login** command.

LOGin <**ipaddress>** | **<ethernetaddress>** | **RE**mote

Syntax Description

login Used without an argument or keyword, this command enables you to log in to a router that is directly connected to your terminal through the console port.

If access to the router has been restricted with the **set local access** command, you will be required to enter the router's system password before making any configuration changes.

ipaddress (Optional) Enables you to log in to a router on the same IP network or to a remote router connected across the ISDN line. The IP address must be in four-part dotted decimal format.

If access to the router has been restricted with the **set remote access** command, you will be required to enter the router's system password before making any configuration changes.

ethernetaddress (Optional) Used with bridging. Enables you to log in to a router on the same Ethernet segment or to a remote router connected across the ISDN line. The Ethernet address must be entered as 12 contiguous hexadecimal characters with no spaces.

If access to the router has been restricted with the **set remote access** command, you will be required to enter the router's system password before making any configuration changes.

remote (Optional) Used with Combinet Packet Protocol (CPP). Enables you to log in to a router connected across the ISDN line. This keyword should be used while in profile mode.

Default

None

Command Mode

None

Usage Guidelines

You can only log in to a remote router that is directly connected to your terminal or that has an active ISDN or Ethernet connection to your local router. After five minutes of no activity, you will be logged out of the remote router. Use the **logout** command to manually log out of the remote router.

Example

The following example enables you to log in to a remote router across the ISDN connection using the remote router's IP address:

```
Host> login 150.150.50.25
```

Related Commands

logout
set local access
set remote access

logout

To end any remote session initiated by the **login** command, use the **logout** command.

LOGOut

Syntax Description

This command does not contain any keywords or arguments.

Default

None

Command Mode

System level or in profile mode

Example

The following example ends a remote session initiated with the **login** command:

```
Host> logout
```

Related Command

login

reset callback receive number

To clear one or all router telephone numbers from which the router will receive callbacks, use the **reset callback receive number** command.

REset **CALLB**ackreceive **<number**> | **AL**l

Syntax Description

number Deletes the specified remote router telephone number that has been entered with the **set callback receive number** command.

all Deletes all remote router telephone numbers that have been entered with the **set callback receive numbe**r command for the active profile.

Default

None

Command Mode

Profile mode

Example

The following example deletes a telephone number of a remote router from which the router will accept callbacks:

```
Host:2503> reset callbackreceive 4085551234
```

Related Command

set callback receive number

reset caller id receive number

To delete one or all of the telephone numbers from which the router will receive calls when Caller ID is enabled, use the **reset caller id receive number** command:

REset **CALLI**dreceive **<number>** | **AL**l

Syntax Description

number Deletes the specified remote router telephone number that were entered with the **set caller id receive number** command.

all Deletes all remote router telephone numbers that were entered with the **set caller id receive number** command.

Default

None

Command Mode

System level

Example

The following example deletes a caller id receive number that has been entered with the **set caller id receive number** command:

```
Host> reset callidreceive 5559020
```

Related Command

set caller id receive number

reset password

To delete one or all of the host passwords, use the **reset password** command.

REset **PA**ssword **[AL**l**]**

Syntax Description

all	(Optional) Deletes all host passwords.

Default

None

Command Mode

System level

Usage Guidelines

This command does not delete client or system passwords. See the following section, “Examples,” for the procedure to change these passwords.

Examples

The following example deletes a single host password:

Step 1 Enter the **reset password** command:

```
Host> reset password client
```

Step 2 At the prompt, enter the host password that you want deleted. The password will not be echoed on the terminal:

```
Enter new Password: <host-password>
```

You have deleted one host password.

The following example deletes or changes client and system passwords:

Step 1 Enter the **set password** command with the correct keyword (either **client** or **system**):

```
Host> set password client
```

Step 2 To delete the password, press Return in response to the prompt. To change the password, enter the new password in response to the prompt. The password will not be echoed on the terminal.

```
Enter new Password: <new-password>
```

Step 3 If you entered a new password, you will be prompted to reenter it for confirmation:

```
Re-Type new Password: <new-password>
```

set callback

To enable the Cisco router to disconnect an incoming call and then call back the remote router, use the **set callback** command.

SEt **CA**llback **ON** | **OF**f

Syntax Description

on Enables callback.

off Disables callback.

Default

off (disabled)

Command Mode

Profile mode

Usage Guidelines

For the Cisco router to call back to the remote router, the Cisco router uses the number configured in the remote router with the **set ringback number** command.

Example

The following example enables callback for the profile 2503:

```
Host:2503> set callback on
```

Related Commands

set callback id
set callback receive number
set ringback number

set callback id

To enable the routers and to authenticate a caller before making a callback to the remote router, use the **set callback id** command:

SEt **CALLBACK**id **ON** | **OF**f

Syntax Description

on Enables callback authentication. The Cisco 750 series and the Cisco 760 series routers compare a calling router's telephone number to a list of numbers that it has configured with the **set callback receive number** command. If the remote router's telephone number matches one of these numbers, the Cisco router will make a callback to the remote router.

off Disables callback authentication. If callback is enabled with the **set callback** command, the Cisco router will make a callback to the remote router without authenticating it.

Default

off (disabled)

Command Mode

Profile mode

Usage Guidelines

Use the **set callback** command to enable the callback function before enabling this command.

Example

The following example enables callback authentication for the profile 2503:

```
Host:2503> set callbackid on
```

Related Commands

set callback
set callback receive number

set callback receive number

To enter telephone numbers used for authentication when callback authentication is enabled, use the **set callback receive number** command.

SEt **CALLBACKR**eceive <**number**>

Syntax Description

number Telephone number of any remote router that is authenticated before the Cisco router will make a callback. Use this command when the **set callback id** command is enabled. This number should contain any digits the Cisco router requires to complete the call to the remote router, for example access code and area code.

Default

No callback receive numbers are configured.

Command Mode

Profile mode

Usage Guidelines

To delete a callback receive number, use the **reset callback receive number** command.

Example

The following example configures a telephone number that will be authenticated before the Cisco router makes a callback on profile 2503’s connection:

```
Host:2503> set callback receive 5551234
```

Related Commands

set callback
set callback id
reset callback receive number

set caller id

To enable ISDN Caller ID authentication, use the **set caller id** command.

SEt **CALLE**rid **ON** | **OF**f

Syntax Description

on Enables ISDN Caller ID authentication.

off Disables ISDN Caller ID authentication.

Default

off (disabled)

Command Mode

System level

Usage Guidelines

This configuration applies to all ISDN connections. Caller ID is a service offered by the ISDN service provider in which the calling router is authenticated by its telephone number.

Example

The following example enables Caller ID checking for all ISDN connections:

```
Host> set callerid on
```

Related Command

set caller id receive number

set caller id receive number

To enter the ISDN telephone numbers from which the router will accept calls when Caller ID checking is enabled, use the **set caller id receive number** command.

SEt **CALLI**dreceive **<number**>

Syntax Description

number ISDN phone number of a remote router from which the router will accept calls when Caller ID checking is enabled with the **set caller id** command.

Default

No Caller ID receive numbers are configured.

Command Mode

System level

Usage Guidelines

To delete a telephone number set with this command, use the **reset caller id receive number** command.

Example

The following example enters the telephone number for a remote router that will be authenticated when Caller ID checking is enabled:

```
Host> set callidreceive 4085559020
```

Related Commands

set caller id
reset caller id receive number

set local access

To restrict commands that can be entered at the local configuration port, use the **set local access** command.

SEt **LO**calaccess **ON** | **PA**rtial | **PRO**tected

Syntax Description

on	Sets commands to be performed without restriction.
partial	Sets commands to be performed with partial restrictions.
protected	Sets commands to be performed with system password only.

See Table 5-1 for a summary of each keyword's security level.

Default

Enabled on for all commands

Command Mode

System level

Example

The following example configures local configuration access to protected:

```
Host> set local access protected
```

Table 5-1 describes the **set local access** command settings.

Table 5-1 Set Local Access Command Settings

Commands	On	Partial	Protected
call	See Note[1]		P[2]
demand		P	P
disconnect			P
help			P
log commands			P
login			
logout			
reboot			P
reset commands		P	P
set commands		P	P
show commands			P
software load		P	P
test commands			P
timeout		P	P
unset commands		P	P
upload			P
version			P
CD			P
Establish			P
Ping			P

Commands	On	Partial	Protected
Release			P
Unlearn			P

1. Note: An empty cell indicates that the command can be performed remotely without restrictions.
2. P indicates that a system password must be entered before performing the **`set local`** command at the local configuration port.

Related Command

set password

set remote access

To restrict remote configuration access to the router, use the **set remote access** command.

SEt **RE**moteaccess **OFF | PRotected** | **PArtial**

Syntax Description

off	No remote login sessions are allowed.
protected	Sets commands to be performed with system password only.
partial	Sets commands to be performed with partial restrictions.

Default

off

Command Mode

System level.

Example

The following example configures the router for protected remote access:

```
Host> set remote access protected
```

Table 5-2 describes the **set remote access** command settings.

Table 5-2 Set Remote Access Command Settings

Commands	Partial	Protected	Off
call	See Note[1]	P[2]	X[3]
demand	P	P	X
disconnect		P	X
help		P	X
log commands		P	X
login			X
logout			X
reboot		P	X
reset commands	P	P	X
set commands	P	P	X
show commands		P	X
software load	P	P	X
test commands		P	X
timeout	P	P	X
unset commands	P	P	X
upload		P	X
version		P	X
CD			P
Establish			P
Ping			P

Commands	Partial	Protected	Off
Release			P
Unlearn			P

1. Note: An empty cell indicates that the command can be performed remotely without restrictions.
2. P indicates that a system password must be entered before this command can be performed remotely.
3. X indicates that this command cannot be performed remotely.

Related Command

set password

set ppp authentication

To set the PPP authentication that is performed for incoming and outgoing ISDN calls, use the **set ppp authentication** command.

SEt **PP**p **AU**thentication **IN**coming | **OU**tgoing **[CH**ap**] [PA**p**] [NO**ne**]**

Syntax Description

incoming Applies the authentication method to incoming WAN calls.

outgoing (Optional) Applies the authentication method to outgoing WAN calls.

chap (Optional) Enables the challenge Handshake Authentication Protocol (CHAP) authentication. You must have a CHAP host secret configured with the **set ppp password** command and a User ID configured with the **set system name** command.

pap (Optional) Enables Password Authentication Protocol (PAP) to be performed. You must have a PAP host password configured with the **set ppp password** command, and a User ID configured with the **set system name** command.

none (Optional) No authentication is performed.

Defaults

incoming chap
outgoing chap

Command Mode

System level or profile mode

Usage Guidelines

You can specify different authentication type. You may specify one, two, or all of the authentication options. They will be negotiated in the following order: **chap**, **pap**, **none**. If the **none** keyword is not specified and authentication fails, the call will be terminated.

Note This command has no effect on how the Cisco router responds to remote authentication requests. The Cisco router always responds to PAP or CHAP authentication requests. A client password or secret must be configured with the **set ppp password** command to make the authentication response succeed (unless a Null password or secret is being used by the peer).

Examples

The following example sets the router to use incoming PAP authentication for incoming calls.

```
Host> set PPP authentication incoming pap
```

The following example sets the router to use outgoing pap authentication for outgoing calls.

```
Host> set PPP authentication outgoing pap
```

Related Command

set system name

set ppp callback request/reply

Use the **set ppp callback request/reply** command to set the callback mode for point-to-point encapsulation. This command ensures a level of callback security.

SEt **PPP CA**llback **RE**quest | **RE**ply **ON | OF**f **| AL**ways

Syntax Description

request Specifies whether the router will request a callback when it receives or places a call.

reply Specifies whether the router will agree to a callback when requested to do so by the remote router.

on Enables callback.

off Disables callback.

always Forces callback at all times.

Default

off (disabled)

Command Mode

Profile mode

Usage Guidelines

When the calling unit's request is set to On, the calling unit initiates a callback request. If the callback request is acknowledged by the called unit, the call will stay connected until one of the following occurs:

- The call is disconnected by the called unit, and the callback is made subsequently by the called unit.
- The callback is acknowledged by the called unit, but the callback is not attempted by the called unit. This could happen if the called unit callback reply is set to Off for that profile, or the called unit is a product that does not support callback.
- If the calling unit request is set to always, the calling unit disconnects the call after the acknowledgment process. If the called unit reply is set to On or Always, then the called unit will make a callback to the calling unit.
- If the called unit reply is set to Always, the called unit will disconnect the original call. The called unit attempts a callback.

Example

The following example sets the profile to reply always:

```
Host> set ppp callback reply always
```

Related Commands

set number
set security
set ringback
show security

set ppp password

To configure the passwords used during PAP and CHAP PPP authentication, use the **set ppp password** command.

SEt **PPP <PA**ssword | **SE**cret**> <HO**st | **CL**ient**>**

Syntax Description

password	Used for PAP authentication.
secret	Used for CHAP authentication.
host	Profile configurations used by the Cisco router to authenticate a remote router. The remote router's client password or secret must match the Cisco router's host password or secret.
client	Local system configurations used by the remote router to authenticate the Cisco router. The Cisco router's client password or secret must match the remote router's host password or secret.

Default

No passwords or secrets are configured.

Command Mode

System level or profile mode

Usage Guidelines

Configure host passwords and secrets while in profile mode. Configure client passwords and secrets at the system level.

Examples

The following example configures the router with a PAP client password:

Step 1 Enter the **set ppp password client** command:

```
Host> set PPP password client
```

Step 2 At the prompt, enter your client password. Your password will not be echoed on the terminal:

```
Enter new Password:
```

Step 3 At the prompt, reenter your client password for confirmation:

```
Re-Type new Password:
```

You have configured the Cisco router with a PAP client password.

The following example deletes the PAP client password:

Step 1 Enter the **set ppp password client** command:

```
Host> set PPP password client
```

Step 2 At the prompt, press Return:

```
Enter new Password: <Return>
```

Step 3 At the prompt, press Return again:

```
Re-Type new Password: <Return>
```

You have deleted the Cisco router PAP client password.

Related Command

set ppp authentication

set password

To set the password, use the **set password** command.

SEt **PA**ssword **HO**st **| SY**stem | **CL**ient

Syntax Description

host Configures the host password that is used to authenticate remote ISDN calls when using CPP. The Cisco router compares its list of host passwords to the remote router's client password to authenticate the call. The host keyword can consist of a combination of 1 to 16 characters. The Cisco router can be configured with multiple host passwords. This keyword should be used while in profile mode. Any host password configured at the system level is inherited by all user-created profiles.

system Configures the system password that is used to authenticate users requesting a local or remote configuration session. The system keyword can consist of a combination of 1 to 16 characters. The Cisco router can have one system password. This keyword should be used at the system level only.

client Configures the client password that is sent by the router when making an ISDN connection When using CPP. The remote router compares the Cisco router's client password to its list of host passwords to authenticate the call.The client keyword can consist of a combination of 1 to 7 characters. The Cisco router can be configured with one client password per profile. This keyword should be used while in profile mode.

Default

No passwords are configured.

Command Mode

System level (System Password)

Profile (Client Password)

Both (Host Password)

Usage Guidelines

The **set password** system command should be preceded with the **set remote access** command. After entering the command you will be prompted to enter the password. When configuring a host password, you will also be prompted for a user name to associate with the password. This user name can consist of a combination of 1 to 7 characters.

To delete or change passwords, use the **reset password** command.

Example

The following example configures a host password for profile 2503:

Step 1 Enter the **set password host** command:

```
Host:2503> set password host
```

Step 2 At the prompt, enter your host password. Your password will not be echoed on the screen:

```
Enter new Password: <password>
```

Step 3 At the prompt, reenter your host password again for confirmation:

```
Re-Type new Password: <password>
```

Step 4 At the prompt, enter the user name you wish to associate with the host password:

```
Enter User Name: JohnDoe
```

Related Command

reset password

show security

To display the router’s security configurations, use the **show security** command.

SHow **SE**curity **[AL**l**]**

Syntax Description

all (Optional) In profile mode, displays all security configurations. This keyword has no effect when used in the profile mode.

Usage Guidelines

Use this command at the system level with the **all** keyword to display all security configurations. Use this command while in profile mode to display the security configurations for that profile.

Example

The following example shows output from the **show security** command at the system level:

```
Host> show security
System Parameters
    Security
      Access Status            ON
      System Password          NONE
      Remote Configuration     PROTECTED
      Local Configuration      ON
      Caller ID Security       OFF
      Caller Id Numbers
PPP Security
      PAP Client Password      NONE
      CHAP Client Secret       NONE
Profile Parameters
    Callback ID Security       OFF
    CPP Security
      Client Password          NONE
      Callback                 OFF
      Callback Numbers
```

```
Profile Parameters
    Callback ID Security       OFF
    CPP Security
      Client Password          NONE
      Callback                 OFF
      Callback Numbers
```

Table 5-3 lists the significant fields shown in the display.

Table 5-3 Show Security Field Descriptions

Field	**Description**
System Parameters	Security configurations that apply to the system level.
Access Status	Indicates if remote access is enabled. Can be On or Off.
System Password	Indicates if a system password has been entered with the **set password** system command. Can be none or exists.
Remote Configuration	Remote access restriction as configured with the **set remote access** command.
Local Configuration	Local configuration restriction as configured with the **set local access** command.
Caller ID Security	Indicates if Caller ID is enabled. Can be On or Off.
Caller ID Number	The phone numbers entered with the **set caller id receive number** command.
PPP Authentication In	The PPP authentication method used for incoming calls. Can be PAP, CHAP, *none*, or any combination of these three. Set with the **set ppp authentication** in command.
PAP Client Password	Indicates if a PAP client password has been entered with the **set ppp password** command. Can be none or exists.
CHAP Client Secret	Indicates if a CHAP client secret has been entered with the **set ppp password** command. Can be none or exists.
Profile Parameters	Security configurations that apply to the profile. If you are using the **show security** command at the system level, these configurations make up the profile template for security parameters.
Client Password	Indicates if a client password has been configured with the **set password** command. Can be none or exists.

Field	Description
Callback	Indicates if callback is enabled. Can be On or Off.
Callback ID Security	Indicates if callback authentication is enabled. Can be On or Off.
Callback Numbers	Numbers entered with the **set callback id receive number** command.
Number of Host Passwords	Number of host passwords that have been entered with the **set password** command.
Host Passwords	Lists the user names. An asterisk (*) indicates that a password exists for the user.
PPP Authentication out	PPP authentication method used for outgoing calls. Can be PAP, CHAP, none, or any combination of these three. Set with the **set ppp authentication** out command.
PAP Host Password	Indicates if a PAP host password has been entered with the **set ppp password** command. Can be none or exists.
CHAP Host Secret	Indicates if a CHAP host secret has been entered with the **set ppp password** command. Can be none or exists.
Callback Request	Indicates if the router will request a callback from the remote unit, can be on or off.
Callback Reply	Indicates if the router will perform a callback if requested to do so by the remote router, can be on or off.