



Using the Configuration Menu

This chapter provides a general introduction to the Configuration menu and describes the procedures for saving and restoring your configurations.

Here's what you'll find in this chapter:

- [Viewing the Configuration Menu, page 3-2](#)
- [Configuration Menu Options, page 3-2](#)
- [Using the Configuration Security Menu, page 3-3](#)
- [Using the Configuration Console Menu, page 3-4](#)
- [Using the Configuration Time Menu \(Time\), page 3-8](#)
- [Backing Up Your Configuration \(Dump\), page 3-9](#)
- [Restoring Your Configuration, page 3-10](#)

Viewing the Configuration Menu

After installation use the Configuration Menu commands to configure the bridge.

Navigation: Choose **Main > Configuration**

Option	Value	Description
1 - Radio	[menu]	- Radio network parameters
2 - Security	[menu]	- Network authentication
3 - Ethernet	[menu]	- Ethernet configuration
4 - Identity	[menu]	- Identification information
5 - Console	[menu]	- Control console access
6 - Time	[menu]	- Network Time Setup
7 - Dump		- Dump configuration to console

Enter an option number or name, "=" main menu, <ESC> previous menu
>

56508

Configuration Menu Options

Radio: sets radio network parameters, such as system ID, frequency, and bit rate. See Chapter 4, “Configuring the Radio Network.”

Security: enables Extensible Authentication Protocol (EAP) and connects to the Cisco Secure Access Control Server (ACS). See the following section “Using the Configuration Security Menu.”

Ethernet: sets the Ethernet parameters. See Chapter 5, “Configuring the Ethernet Port.”

Identity: sets various network identifiers such as node names, network ID, and Internet address. See Chapter 6, “Setting Network Identifiers.”

Console: controls access to the console system. See “Using the Configuration Console Menu” later in this chapter.

Time: sets the time server and other network time parameters. See “Using the Configuration Time Menu” later in this chapter.

Dump: backs up the configuration commands. See “Backing Up Your Configuration (Dump)” later in this chapter.

Using the Configuration Security Menu

From the Configuration Security Menu you can enable EAP and ensure added wireless security. The process for enabling EAP requires that you connect to your organization's Cisco ACS server, which requires a login and password, unique to your bridge. Follow your organization's procedures for obtaining the login and password for your bridge.

Navigation: Choose **Main > Configuration > Security**

Option	Value	Description
1 - Mode	[off]	- Authentication mode
2 - Username	[""]	- Login user name
3 - Userpwd		- Login password

Enter an option number or name, "=" main menu, <ESC> previous menu
> _

56513

To Enable EAP, follow these steps:

-
- Step 1** Choose **Security** from the Configuration menu. The Configuration Security menu appears.
- Step 2** Choose **Mode**. The following message appears:
Enter one of [off eap]
- Step 3** Choose **eap** and press **Enter** to return to the Configuration Security menu.
- Step 4** Choose **Username**. The following message appears:
Enter a string:
- Step 5** Enter your bridge's username and press **Enter** to return to the Configuration Security menu.
- Step 6** Choose **Userpwd**. The following message appears:
Enter a string:
- Step 7** Enter your bridge's password and press **Enter** to return to the Configuration Security menu.
- Step 8** Press **Escape** once to return to the Configuration menu or twice to return to the Main menu.



Caution

Perform all the steps in the above procedure. Even with **eap** enabled, the bridge will not pass data until you are connected to the ACS server.

Using the Configuration Console Menu

From the Configuration Console menu you can set up essential system parameters.

Navigation: Choose **Main > Configuration > Console**

Option	Value	Description
1 - Rpassword		- Set readonly privilege password
2 - Wpassword		- Set write privilege password
3 - Display		- Display the remote operator list
4 - Add		- Add an operator host
5 - Delete		- Remove an operator host
6 - Communities	[menu]	- SNMP community properties
7 - Type	[ansi]	- Terminal type
8 - Linemode	[off]	- Console expects complete lines

Enter an option number or name, "=" main menu, <ESC> previous menu
>

Setting Privilege Levels and Passwords (Rpassword, Wpassword)

You can restrict access to the menus by setting privilege levels and passwords. Privilege levels are set from the Main menu. Passwords are set from the Configuration Console menu.

There are three privilege levels:

- **Logged out (off):** denies access to all submenus. Users are only allowed access to the *privilege* and *help* options of the Main menu.
- **Read-only (readonly):** allows read-only privileges for all submenus. Only those commands that do not modify the configuration may be used.
- **Read/write (write):** allows users complete read and write access to all submenus and options.

Keep in mind the following when setting privilege levels and passwords:

- Only read-only and read/write privilege levels can be password protected.
- You can always go from a higher privilege level to a lower privilege level without a password. If you try to go to a higher privilege level, you must type the password.
- Passwords are case sensitive.

To set a privilege level, follow these steps:

Step 1 Select **Privilege** from the Main menu. The following message appears:

```
Enter one of [off, readonly, write] :
```

Step 2 Type the first letter of your selection and press **Enter**.

To set a password, follow these steps:

Step 1 Select **Configuration** from the Main menu.

Step 2 Select **Console** from the Configuration menu.

Step 3 Select the appropriate password option from the Configuration Console menu:

- **Rpassword:** for read-only privilege
- **WPassword:** for read/write privilege
- **None:** type this text string if no password is needed

Step 4 If you select **RPassword** or **WPassword**, the following message appears:

Enter one of [none, a password of between 5 and 10 characters] :

Step 5 Type your password and press any key. The following message appears:

Enter the password again, one of [none, a password of between 5 and 10 characters] :

Step 6 Retype your password for confirmation.



Note

After a privilege level is assigned, anyone attempting to access that level is prompted for the password; therefore, you can set various privilege levels for individuals, providing them with access to some options while denying them access to others. Remember that passwords are case sensitive. If an incorrect password is typed, the console pauses briefly before reprompting. The connection is dropped after three consecutive failures, and a severe error log is displayed.



Caution

Make sure you write down the passwords you have established and keep them in a safe place. If you forget your password, the bridge will have to be returned for factory servicing. Please contact Cisco Technical Support for further instructions.

Controlling Remote Access (Display, Add, Delete)

Use the *display*, *add*, and *delete* options to create and manage a list of hosts that are allowed access to the bridge's console system. The list controls access from Telnet, HTTP, or FTP. SNMP access is controlled separately on the Configuration SNMP Communities menu.

If the list of hosts is empty, any host in the infrastructure can attempt to connect. When the appropriate password is provided, the connection is made. If the list contains entries, any host not on the list cannot gain access. An entry in the list can be specified as an IP address or a MAC address.



Caution

The first MAC or IP address you add should be that of the PC you are using to Telnet or browse to the bridge.

Display

Displays a list of MAC or IP addresses of any stations permitted to access the bridge remotely.

Add

Adds a host to the remote host list. You are prompted for the address of the host to add.

Delete

Removes a host from the remote host list. You are prompted for the address of the host to remove.

Setting Up SNMP Communities (Communities)

The *communities* option contains a menu that allows control access to the SNMP agent. When you select the *communities* option, the Configuration SNMP Communities menu appears.

Navigation: Choose **Main > Configuration > Console > Communities**

```

Configuration Console Communities Menu

Option      Value      Description
1 - Display
2 - Add
3 - Remove
4 - Access
5 - Remote  [ off ]   - Allow remote NMS to change community info

Enter an option number or name, "=" main menu, <ESC> previous menu
> █
  
```

44763

Displaying Communities (Display)

The *display* option lists the communities you have set. When you select *display*, an SNMP communities list screen similar to the following appears.

Navigation: Choose **Main > Configuration > Console > Communities > Display**

```

SNMP Communities

public      - Read Only
proxy       - Read Only
private     - Read Only
regional    - Read Only
core        - Read Only

Enter space to redisplay, q[uit] : █
  
```

44764

An SNMP community consists of the following:

- **Name:** the default set of communities is *Public*, *Proxy*, *Private*, *Regional*, and *Core*. You can define up to six community names. When a Network Management Station (NMS) requests information from the unit's agent, the community name in the request must match one of the names on the SNMP communities list.
- **Access Mode:** displays the community access modes – *Read-Write* and *Read Only*. The default access mode is *Read Only*.
- **NMS IP Addresses:** (optional) displays a list of allowed NMS IP addresses of the community. You can define up to five IP addresses. The default setting is *Any*.
- **NMS NID (Node ID):** (optional) displays a list of allowed node IDs of the community. You can define up to five node IDs. The default setting is *Any*.

Adding a Community (Add)

Use the *add* option to add a new community to the SNMP communities list. The default community settings for the new community names are *Read Only access*, *Any NMS IP address*, and *Any NID*.

Removing a Community (Remove)

Use the *remove* option to remove a community from the SNMP communities list. You will be prompted for the name of the community to remove.

Setting a Community Access Mode (Access)

Use the *access* option to set a community access mode. Choose from the following two options.

- **Read-only (read):** allows *gets* and *get-nexts* on any readable variable.
- **Read/write (write):** allows *gets* and *get-nexts* on any variable, as well as *set* requests on writeable variables.

The default access setting for all community names is *Read Only access*.

**Note**

An error response is returned to the NMS if the NMS is trying a *set* request used with a community that has *Read Only access*.

Enabling Remote NMS to Change Community Setup (Remote)

The *remote* option controls whether the section of the custom MIB for the bridge allowing access to the community name configuration is enabled or disabled.

- **On:** when remote is enabled an NMS with write access will be able to change the configuration and access rights for the community names.
- **Off:** when remote is enabled an NMS will be able to change this part of the configuration.

Setting the Terminal Type (Type)

Sets the terminal type to Teletype (TTY), ANSI, or Colour.

If the terminal or emulation program you are using supports the ANSI escape sequences, you should use ANSI.

- **Teletype mode:** displays text with little or no formatting. Screens are not cleared prior to new screens appearing.
- **ANSI mode:** provides text in a formatted manner. In addition, the screen is cleared before each new screen is displayed.
- **Colour mode:** provides text in ANSI mode with text and background color added.

Enabling Linemode (Linemode)

Enable *linemode* when working with Telnet and terminal emulators that do not send characters when typed, but rather saves them until you press **Return** at the end of a line.

The Console does not automatically complete any typed commands or information when a space or carriage return is inserted.

To enable linemode, choose **Main > Configuration > Console > Linemode**.

**Note**

Some Telnet programs automatically invoke linemode by sending the appropriate Telnet commands when they connect to the bridge.

Using the Configuration Time Menu (Time)

Use the Time menu to set time parameters.

Navigation: Choose **Main > Configuration > Time**

Configuration Time Menu		
Option	Value	Description
1 - Time_server	[000.000.000.000]	- Time protocol server
2 - Sntp_server	[000.000.000.000]	- Network time server
3 - Offset	[0]	- GMT offset in minutes
4 - Dst	[off]	- Use daylight saving time

Enter an option number or name, "=" main menu, <ESC> previous menu
> █

44777

Configuration Time Menu Options

- **Time_server:** when there is an address of a time protocol server in this parameter, the bridge sends a request to that server to acquire the time from that server.
- **Sntp_server:** when there is an address of a Simple Network Time Protocol (SNTP) server in this parameter, the bridge sends a request to that server to acquire the time from that server.
- **Offset:** this option sets the number of minutes offset from Greenwich Mean Time. This must be set properly.
- **Dst:** when Daylight Savings Time (DST) is set to *on*, the bridge automatically adjusts for DST changes in spring and fall.

Saving Configuration Parameters

There is no explicit method or command to save your configuration changes. Changes you make are automatically saved to nonvolatile Flash memory each time you set or modify a parameter. This ensures the configuration is maintained during power failures or intentional power outages.

Most configuration settings become effective as soon as the command is executed. Those that do not immediately become effective are noted in the command information.

Backing Up Your Configuration (Dump)

Once you have set the configuration parameters for the bridge, use the *Dump* option to dump the configuration commands to the Telnet session. Capture these as text and save them as an ASCII file using the logging option on the Telnet program.

Navigation: Choose **Main > Configuration > Dump**

To back up configurations, follow these steps:

**Note**

Commands may vary depending on the communications program used.

Step 1 Connect to bridge using Telnet.

Step 2 From Telnet's Terminal pull-down menu, choose **Start Logging** and name the file.

Step 3 Choose **Main Menu > Configuration > Dump**.

The following message appears:

```
Enter one of [all, non-default, distributable, ident, radio, filter, other]:
```

Step 4 Type one of the following options after the colon:

- **All:** to display the entire configuration.
- **Non-default:** to display only the configuration options that are different from the original default settings.
- **Distributable:** to display only the configuration options that are not considered unique to this bridge. You can use the menu sequence **Main > Diagnostics > Load > Distribute** to send this configuration to other bridges in the infrastructure.
- **Identity:** to display only configuration options pertaining to the bridge's network identifiers. See Chapter 6, "Setting Network Identifiers."
- **Radio:** to display only configuration options pertaining to the bridge's radio network parameters. See Chapter 4, "Configuring the Radio Network."
- **Filter:** to display only configuration options pertaining to the bridge's filters. See Chapter 9, "Using Filters."
- **Other:** to display other configuration options.

Step 5 Type one of the following options:

- **Standard:** to display the configuration in normal readable text form.
- **Encoded:** to display each configuration command by a unique number. This type of configuration is the best to save because the number never changes during the life of the product. Text may change or move as more items are added to the menus.

After you have typed one of these options, the configuration commands appear on the screen.

Step 6 Press **Enter**.

Step 7 Press **Enter** again to refresh screen.

Step 8 Choose **Stop Logging** from Terminal pull-down menu. See Step 2.

**Note**

You can also use the *Config* option to back up your configuration. See Chapter 11, “Performing Diagnostics.”

Restoring Your Configuration

If your configuration is ever lost or corrupted, you can restore it by using the *Load* option from the Diagnostics Load menu to move the configuration file into the bridge. The system automatically restores your configuration based on these commands.