Establishing Security for the Catalyst 2600

The Catalyst 2600 allows you to use a console session to establish two types of security: one to protect the configuration of the Catalyst 2600 and one to limit the scope and access of users attached to the Catalyst 2600. This chapter provides information on the following:

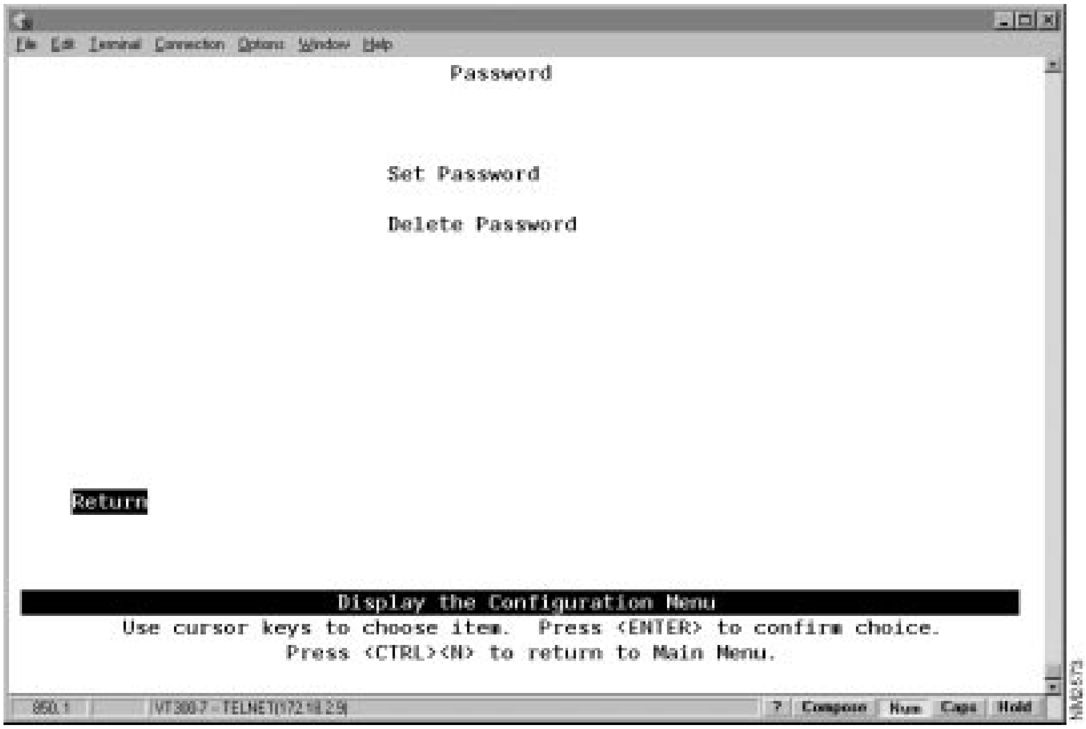
- Setting a Password
- Limiting Scope and Access

For information about setting up a console session, refer to “Planning for Configuration and Management”.

Setting a Password

The Catalyst 2600 allows you to set a password to protect its configuration. If you establish a password, users must enter it to obtain access to the Main Menu. To set a password, select **Password** on the Configuration Menu. The Password panel (Figure 6-1) is displayed.

Figure 6-1 Password Panel



```
                                Password


                          Set Password

                          Delete Password







   Return



                       Display the Configuration Menu
      Use cursor keys to choose item.  Press <ENTER> to confirm choice.
                 Press <CTRL><N> to return to Main Menu.
```

File Edit Terminal Connection Options Window Help
850, 1
VT300-7 - TELNET(172.18.2.9)
? Compose Num Caps Hold
H/N2573

To	Select	Then
Add a password…	**Set Password**	Press ENTER at the Old Password prompt and specify a new password.
Change the password…	**Set Password**	Specify the current password and the new password.
Delete the password…	**Delete Password**	Specify the current password.
Save your changes…	**Return**	

Note If you have forgotten your password, press the System Request button to access the System Request Menu, and then Clear NVRAM. This will clear the password, but will also reset all configuration parameters to their default value, clearing any values you have entered.

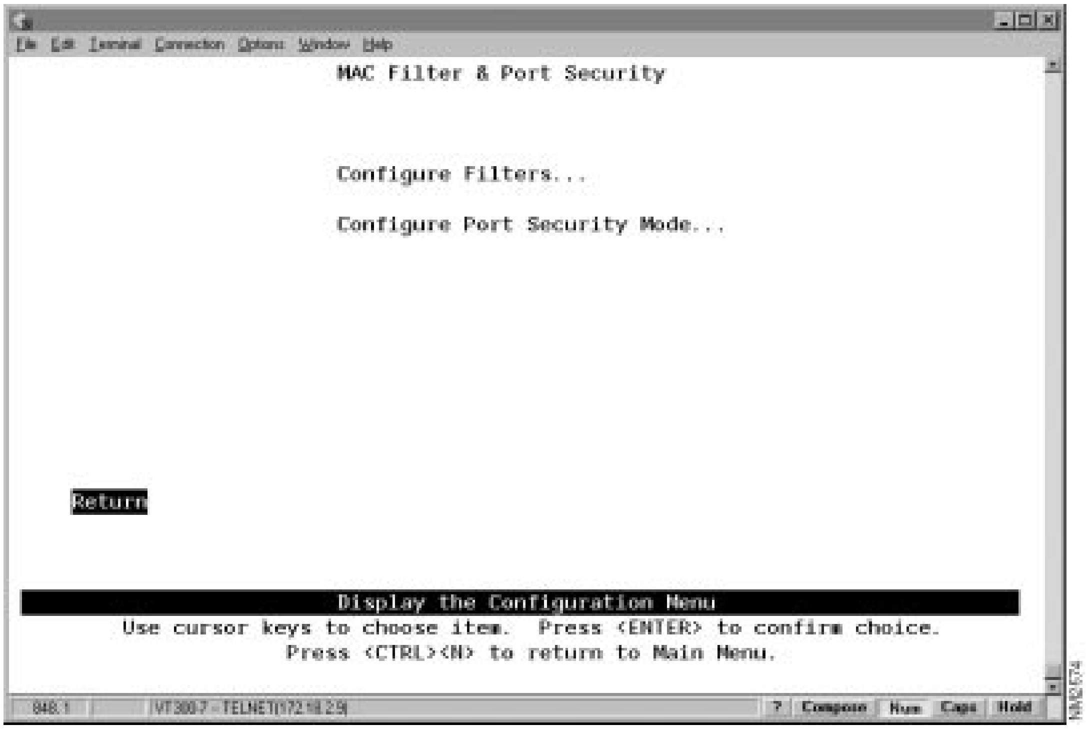
Limiting Scope and Access

For network security, you can isolate parts of your network by limiting the scope and access of your users. For example, you might want to limit access to a specific file server to a select group of users. To do this, you could:

- Attach the printer to a single port on the Catalyst 2600.
- Create a filter that blocks all data to that port except that which is explicitly allowed (using Port Security).
- Define a filter that explicitly allows data from the select group of users (based on MAC address) to be sent to that port (using MAC Filters).

To limit the scope and access of users on segments attached to the Catalyst 2600, select **MAC Filter & Port Security** from the Configuration Menu. The MAC Filter & Port Security panel (Figure 6-2) is displayed.

Figure 6-2 MAC Filter & Port Security Panel



```
                    MAC Filter & Port Security


                    Configure Filters...

                    Configure Port Security Mode...







   Return


                  Display the Configuration Menu
         Use cursor keys to choose item.  Press <ENTER> to confirm choice.
                  Press <CTRL><N> to return to Main Menu.
```

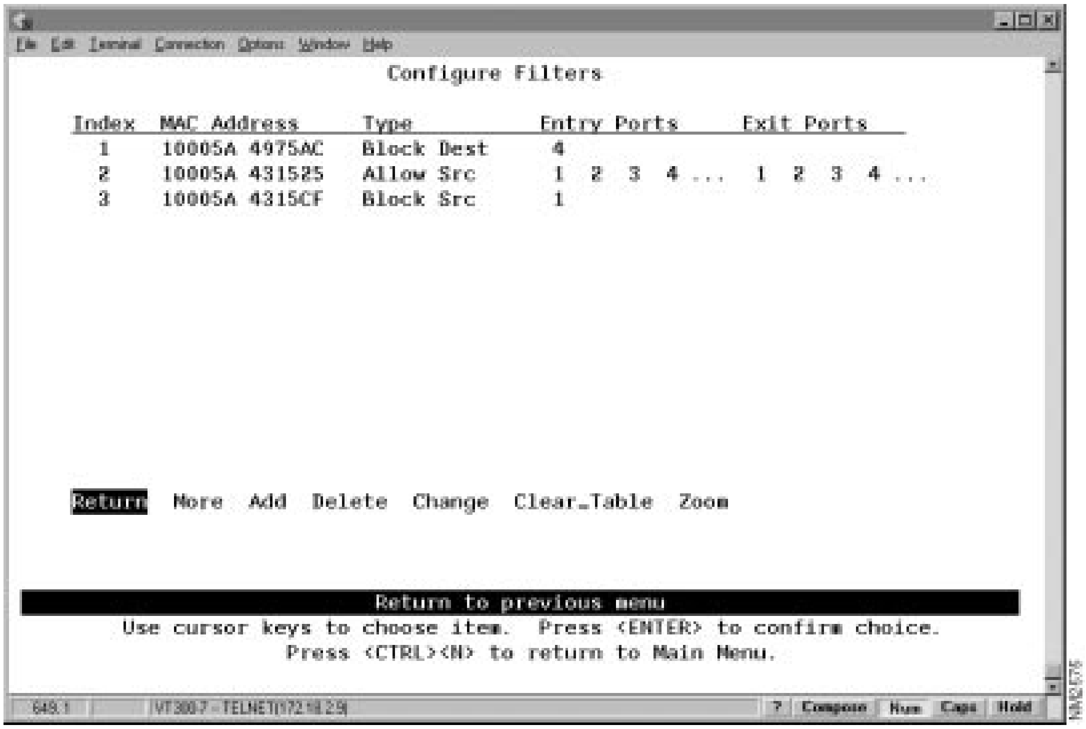
To	Select	Then
View or change MAC address filters…	**Configure Filters**	Refer to "Filtering Data Based on MAC Address."
View or change the port security…	**Configure Port Security Mode**	Refer to "Securing Ports."
Save your changes…	**Return**	

Filtering Data Based on MAC Address

To restrict certain users from communicating with other users or resources (such as printers or servers), select **Configure Filters** on the MAC Filter & Port Security panel. The Configure Filters panel (Figure 6-3) is displayed.

Note Filtering is based on source or destination MAC address. Source filters are not applied to frames that originate on the other side of a source-route bridge. Likewise, destination filters are not applied if the destination device is on the other side of a source-route bridge. If you are using source routing in your network, you should define your filters at the source-route bridges.

Figure 6-3 Configure Filters Panel


File Edit Terminal Connection Options Window Help
649.1
VT300-7 - TELNET(172.18.2.9)
? Compose Num Caps Hold
NW2575

```
                         Configure Filters

  Index  MAC Address      Type           Entry Ports       Exit Ports
    1    10005A 4975AC    Block Dest      4
    2    10005A 431525    Allow Src       1  2  3  4 ...   1  2  3  4 ...
    3    10005A 4315CF    Block Src       1









  Return  More  Add  Delete  Change  Clear_Table  Zoom



                       Return to previous menu
     Use cursor keys to choose item.  Press <ENTER> to confirm choice.
                 Press <CTRL><N> to return to Main Menu.
```

The following information is displayed on this panel:

- Index—The identifier of the filter.
- MAC Address—The MAC address contained in packets to be filtered.
- Type—The possible types are:
  - — Block any packet with Source Address—Block Src.
  - — Block any packet with Destination Address—Block Dest.
  - — Allow any packet with the designated Source Address To Port(s)—Allow Src.
  - — Force any packet with the designated Destination Address To Port(s)—Force Dest.

- Entry Ports—The input port where the filtering takes place. This applies to all filters.
- Exit Ports—The port, if any, that is to receive the filtered packets. This applies only to filters defined as “Allow any packet with the designated Source address to port(s)” or “Force any packet with the designated Destination Address to port(s).”

You can define up to 100 source or destination MAC addresses to be filtered at the port of entry into the Catalyst 2600. MAC addresses can be unicast, multicast (group), or broadcast. All 100 addresses can be associated with one port or divided among the available ports.

To	Select	Then
Add a filter…	**Add**	Specify the filter type, the MAC address, and ports. The port numbers should be listed from lowest to highest and separated by spaces. If you do not specify a port number, the filter will be applied to all ports.
Change a filter…	**Change**	Specify the index number of the filter to be changed and enter the new information.
Delete a filter…	**Delete**	Specify the index number of the filter to be deleted.
Delete all filters…	**Clear_Table**	Confirm the deletion of all filters.
Display the complete list of Entry Ports and Exit Ports for a filter…	**Zoom**	Specify the index number.
Save your changes…	**Return**	

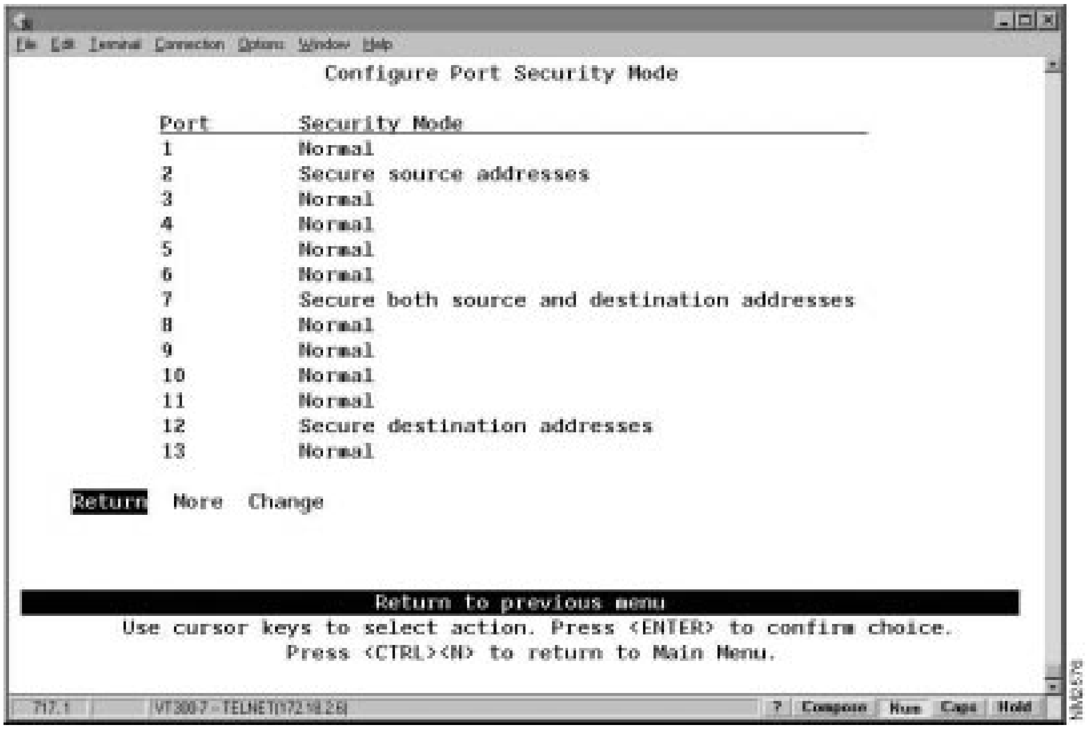
Note If you set up a filter for broadcast packets, hosts on the other side of the Catalyst 2600 will not see the ARP broadcast packets. To prevent this, allow time for the Catalyst 2600 to learn the host addresses before implementing the filter.

Note If you are defining a filter for a TokenChannel, the filter must be defined for all ports in the TokenChannel.

Securing Ports

The Catalyst 2600 also allows you to totally block (secure) communication at selected ports, unless explicitly allowed by a MAC filter. Addresses that have been allowed or forced by a configured filter are not blocked. To define the security attributes of each port, select **Configure Port Security Mode** on the MAC Filter & Port Security panel. The Configure Port Security Mode panel (Figure 6-4) is displayed.

Figure 6-4 Configure Port Security Mode Panel



```
                    Configure Port Security Mode

         Port       Security Mode
         1          Normal
         2          Secure source addresses
         3          Normal
         4          Normal
         5          Normal
         6          Normal
         7          Secure both source and destination addresses
         8          Normal
         9          Normal
         10         Normal
         11         Normal
         12         Secure destination addresses
         13         Normal

    Return  More  Change



                       Return to previous menu
       Use cursor keys to select action. Press <ENTER> to confirm choice.
                 Press <CTRL><N> to return to Main Menu.
```

The following information is displayed on this panel:

- Port—The port identifier.
- Security Mode—The level of security defined for that port. The possible values include:
  - — Normal—No security mode is defined for a port. This is the default.
  - — Secure source addresses—Block all source addresses, except those allowed by a configured filter.
  - — Secure destination addresses—Block all destination addresses, except those forced by a configured filter.
  - — Secure both source and destination addresses—Block all source and destination addresses, except those allowed or forced by a configured filter.

To	Select	Then
Change the security mode for a port…	**Change**	Specify the port and the desired security mode.
Save your changes…	**Return**	