12 Switch Security

With the commands from the Security menu, you can configure system security parameters such as the password and logout time. The menu also provides a command for rebooting the switch. Enter

security

at the prompt to enter the Security menu. Press **?** to see the following list of commands:

Command	Security Menu
pw	Set a new password for a login account
reboot	Reboot this system (allowed if the user is “admin”)
timeout	Configure Auto Logout Time
layer2auth	Enable/Disable layer2 user authentication
secuser	Configure Secure Access user definitions
secproto	Configure Secure Access user list
seclog	Show Secure Access log

Main Interface | File Security | Summary System | VLAN Services | Networking Help

The **pw**, **reboot**, **secuser**, **secproto**, and **seclog** commands are described in the following sections. For information on configuring the Auto Logout Time (the **timeout** command), refer to the **uic** command, which is described in Chapter 8, “The User Interface.” The **layer2auth** command displays if you have the **rav.img** installed on your switch. For information on the **layer2auth** command, see the *Switched Network Solutions User Manual*.

Changing Passwords

The UI provides three types of login accounts—Administrator, Diagnostics, and User. The Administrator login provides full access to all functions. The only login name for an Administrator account is **admin**. The Diagnostics login also has full access to all functions plus a command for running switching module tests. The only login name for Diagnostics is **diag**. The User login is restricted and is used primarily for read-only functions. The only login name for the User account is **user**.

The initial password for all three accounts is **switch**. If you log in as diag you can change the passwords for the **diag**, **admin**, **user** login accounts. If you log in as **admin**, however, you can only change the passwords for the **admin** and **user** login accounts. And if you log in as **user** you can only change the password for the **user** login account. To change the password, complete the following steps. Remember that the User Inferface does not echo (display) the password characters.

1. From the prompt, enter

   pw <account-name>

   The **<account-name>** is the user login name (**diag**, **admin**, **user**) for which you want to change the password. The following prompt displays:

   Changing password for account:<account-name>
   Old password:

2. Enter the old password and press **<Enter>**. If you enter the old password incorrectly, you will receive the message

   Authentication failure

   and the command will terminate. You will then need to start over from **Step 1** above.

   If you answered the old password correctly, the following prompt displays:

   New password:

3. Enter the new password (you are allowed up to 18 characters) and press **<Enter>**. The following prompt displays:

   Retype new:

4. Re-enter the new password to confirm it and press **<Enter>**.

The passwords are stored encrypted in the **mpm.cnf** file. If you forget your password, you will have to delete the **mpm.cnf** file which will cause the passwords to revert to the default.

♦ Caution ♦

Deleting the **mpm.cnf** file will also remove all of your configuration data and restore everything back to factory settings.

Rebooting the Switch

The **reboot** command should only be executed during network down time and when no data is being transmitted across the network. Also, you should ensure that all configuration information has been saved first. Note that the **reboot** command is only available to the **admin** and the **diag** logins.

♦ Caution ♦

Rebooting the switch will disconnect a Telnet connection to the User Interface and will interrupt the network connections on the switching modules.

To reboot the switch from the command line, enter

```
reboot
```

at the prompt and press **<Enter>**. The following prompt will display:

```
Confirm?  (n)              :
```

Enter **Y**. The following message displays:

```
System going down immediately...
switch[489917b0]: System rebooted by admin
```

The switch will now take at least a minute to start up again. (If you are connected to the User Interface with a serial connection, you will see the switch display start-up related information.) The following message displays when the reboot is complete:

```
Welcome to the Alcatel OmniSwitch! (Serial # xxxx)
login :
```

You will have to log in again.

Secure Switch Access

Secure Switch Access is a filtering program that prevents unauthorized access to the switch by allowing you to define a list of authorized users and the IP protocol(s) to which each user has access. The IP protocols supported by Secured Switch Access are FTP, telnet, SNMP, TFTP, HTTP, and a custom IP protocol. If Secure Switch Access is enabled for an IP protocol, then only authorized users can access that protocol. All access violations are logged. If an IP protocol is not secured, it is accessible to all users.

Configuring Secure Switch Access Users Database

The **secuser** command allows you to view and configure the database of secure access users. This database includes information on user names, source IP addresses, source MAC addresses, and the physical ports receiving user data.

The following is a sample **secuser** display:

```
                Secure Access Users Database

List       (l) :
Create     (c):
Delete     (d):
Modify     (m):
Find       (f):
Help       (h):
Quit       (q):
Enter selection:
```

Select an option by entering its letter value at the prompt. To exit this menu, enter **q** (Quit). Descriptions and sample displays for each of the options are as follows:

List

This is a list of all authorized secure access users. The list includes information on the users's name, IP Address, MAC Address, and physical port receiving the user's data. The following is sample display:

User Name	Source IP Address	Source MAC Address	Slot #	Port #
beth	198.34.56.10	0:23:da:67:97:e4	4	1
scott	ANY	ANY	7	3
nichole	172.14.25.13	0:32:e4:a3:6f:e4	2	1
chris	198.34.56.15	ANY	ANY	ANY

The value **ANY** displays if a field is left blank when configuring user information through the **Create (c)** option. The **Any** value signifies a "don't care" condition. When an inbound packet is checked against a User Name to establish authorized access, the **ANY** ("don't care") fields are not checked.

Create

This option allows you to create a new authorized user in the secure access database. The following is a sample display:

```
Create User
-----------------
Enter User:

Enter IP Address ( [a.b.c.d] ) :
Enter MAC Address ( [XXYYZZ: AABBCC] ) :
Is this MAC in Canonical or Non-Canonical (C or N) [C] :
Enter Slot :
Enter Port :
```

After you have created an authorized user, the information is automatically saved in the secure access database and the **secuser** submenu re-displays. To review your new configuration, simply select the list (**l**) option. Descriptions of the fields are as follows:

Enter User: The name of the new user. The name must be at least one character long and no more than 24 characters. You cannot leave this field blank.

Enter IP Address ([a.b.c.d]): The user's IP address. The address must be in the displayed format **([a.b.c.d]).** If you enter a value here, the user may access the switch only from this IP address. If you leave this field blank, a value of **ANY** will display on the secure access list, allowing this user access to the switch from any IP address.

Enter MAC Address (**([XXYYZZ: AABBCC])**): The user's MAC address. The address must be in the displayed format (**([XXYYZZ: AABBCC])**). If you enter a value here, the user may access the switch only from this source Mac address. If you leave this field blank, a value of **ANY** will display on the secure access list, allowing this user access to the switch from any MAC address.

Is this MAC in Canonical or Noncanonical (C or N) [C] : The format of the specified MAC address. Typically, ethernet MAC addresses are in canonical format while token ring and FDDI MAC addresses are in noncanonical format. The default is canonical **(C)**. You can leave this field blank.

Enter Slot: The module on the switch receiving data from this authorized user. If you leave this field blank, a value of **ANY** will display on the secure access list, allowing the authorized user to send data through any module on the switch.

Enter Port: The port on the module receiving data from the authorized user. If you enter a value here, you should also specify a slot in the above field. If you leave this field blank, a value of **ANY** will display on the secure access list, allowing the authorized user to send data through any port on the module (if one is specified) or on the switch (if no slot is specified).

Delete

This option allows you to delete a user from the secure access list. The following is a sample display:

```
Delete User
-----------------
Enter user:
```

Note that once you enter a user, that user will be deleted from the secured access database with no further notice.

Modify

This option allows you to modify information on an existing secured access user. Enter the name of the user you wish to modify, as follows:

```
Modify User
-----------
Enter user: beth
```

The user's existing information will display, followed by options for modification, as follows:

```
                          Source IP       Source MAC      Slot    Port
User Name                 Address         Address         #       #
-------------------------------------------------------------------------------------------------
beth                      ANY             10.2.8.13       5       2

Enter IP Address ( [a.b.c.d] ) :
Enter MAC Address ( [XXYYZZ: AABBCC] ) :
Is this MAC in Canonical or Non-Canonical (C or N) [C] :
Enter Slot :
Enter Port :
```

To change a value, type in the new value at the prompt. If you do not wish to modify a particular field, simply press **Enter** at the prompt and the existing user information will remain unchanged. To change a field to **ANY** privilege, enter a value of **0** at the prompt. Descriptions of the fields in the above display are provided earlier under the option *List* on page 12-4.

Find

This option allows you to find information on a specified user in the secured access database. You must know the user's name in order to use this search feature. The following is a sample display:

```
Find User
---------
Enter User: beth
```

To find a user in the database, simply enter the name of the user at the prompt. If the user you enter is a valid one, information on that user will display, as follows:

```
                          Source IP       Source MAC      Slot    Port
User Name                 Address         Address         #       #
-------------------------------------------------------------------------------------------------
beth                      ANY             10.2.8.13       5       2
```

Configuring Secure Access IP Protocols

The **secproto** command allows you to view the list of secure access IP protocols, to enable security globally or for a specific IP protocol, and to define an access list for each IP protocol. To use this command, enter:

```
secproto
```

A screen similar to the following displays:

```
                    Secure Access IP Protocols

1) FTP Security Enabled          : Yes
    11) Access List              : Beth, Chris
2) Telnet Security Enabled       : No
    21) Access List              : Beth
3) SNMP Security Enabled         : Yes
    31) Access List              :
4) TFTP Security Enabled         : Yes
    41) Access List              : Scott
5) HTTP Security Enabled         : No
    51) Access List              :
6) Custom Security Enabled       : Yes
    61) Access List              : Nichole
    62) Protocol                 :
    63) Port Service             :
7) One-touch Global Security :
    71) One-touch Access List    :

Command { Item=Value/?/Help?Quit/Redraw/Save}      (Redraw)    : save
```

♦ Note ♦

If security is enabled (**yes**) for a protocol and there are no users defined on its access list, then the protocol is essentially inaccessible to all users. For example, SNMP in the above sample display, is configured as inaccessible.

To change a **Security Enabled** value, enter the line number for the parameter, followed by an equal sign (**=**), and then **yes** or **no** at the colon (:) prompt. For example, to enable security for SNMP, you would enter:

```
3=yes
```

To add a user to an access list, enter the line number for the parameter, followed by an equal sign (**=**), and then the user's name at the colon prompt as follows:

```
11=Andy
```

Conversely, to remove an existing user from an access list, enter the line number for the parameter, followed by an equal sign (**=**), a negative sign (**-**), and then the user's name as follows:

```
11= -Beth
```

♦ Note ♦

If the user you add to an access list does not exist in the secure access database, then you will be prompted to create that user. To view the list of secure access users, use the **secuser** command. For more information, see *Configuring Secure Switch Access Users Database* on page 12-4.

You can enter commands by entering just the first letter of the command. For example, you can select **Quit** by entering **q** and **<Enter>**.The question mark option (**?**) and the **Help** option provide reference and instructional information on using this command. The **Quit** option exits this command without saving configuration changes. The **Redraw** option refreshes the screen.

When you are done entering new values, type **save** at the colon (:) prompt and all new parameters will be saved. The following sections describe the options you can alter through this submenu.

1) FTP Security Enabled

Indicates whether or not secure access is enabled for File Transfer Protocol (FTP) on the switch. **Yes** means secure access is enabled for FTP services, and only users on FTP's access list have authorization. **No** indicates that secure access is not enabled for FTP services, and all users can access the switch through FTP.

11) Access List. This is a list of authorized FTP users.

2) Telnet Security Enabled

Indicates whether or not secure access is enabled for Telnet service on the switch. **Yes** means secure access is enabled, and only users on Telnet's access list have authorization. **No** indicates that secure access is not enabled for Telnet service, and all users can access to the switch through Telnet.

21) Access List. This is a list of authorized Telnet users.

3) SNMP Security Enabled

Indicates whether or not security is enabled for Simple Network Management Protocol (SNMP) on the switch. **Yes** means security is enabled for SNMP services, and only users on SNMP's access list are authorized. **No** indicates that secure access is not enabled for SNMP services, and all users can access the switch through SNMP.

31) Access List. This is a list of authorized SNMP users.

4) TFTP Security Enabled

Indicates whether or not security is enabled for Trivial Transfer Protocol on the switch. **Yes** means security is enabled for TFTP services, and only users on TFTP's access list are authorized. **No** indicates that security is not enabled for TFTP services, and all users can access the switch through TFTP.

41) Access List. This is a list of authorized TFTP users.

5) HTTP Security Enabled

Indicates whether or not security is enabled for HyperText Transfer Protocol (HTTP) on the switch. **Yes** means that security is enabled for HTTP, and only users on HTTP's access list are authorized. **No** indicates that security is not enabled for HTTP, and all users can access the switch through HTTP.

6) Custom Security Enabled

Indicates whether or not security is enabled for the custom IP protocol specified in line 62. **Yes** means that security is enabled for the custom IP protocol, and only users on that protocol's access list are authorized. **No** indicates that security is not enabled for the custom IP protocol, allowing all users access to the switch through that protocol.

61) Access List. This is a list of authorized users for the custom IP protocol specified in line 62.

62) Protocol. The IP protocol number that you wish to include as a secured access protocol (IP protocol field in the IP header). You may define only one custom IP protocol.

63) Port Service. The Custom IP protocol's destination port.

7) One-touch Security

This option allows you to conveniently set one **Security Enabled** value for all secure access protocols. Enter **yes** to enable security for all secure access IP protocols. Enter **no** to disable security for all secure access IP protocols. Any value entered here only initially has a global effect. If you wish to set a different value for **Telnet Security Enabled**, for example, enter the line number for Telnet, followed by an equal sign (**=**) and then the new value.

Viewing Secure Access Violations Log

The **seclog** command displays a log of all secure access violations.

♦ Note ♦

To begin logging of access violations, you must enable **Security Violations** from the **Configure Misc.** submenu of the **swlogc** command. For more information on the **swlogc** command, see Chapter 14, "Switch Logging."

To view the secure access violations log, enter

```
seclog
```

The following is a sample display:

```
                    Secure Access Violations Log

                                                                Slot/   Elapsed Time
Time                Protocol    Source IP          Attempts     Intf      (secs)
------------------- ----------  -----------------  ----------  -------  ----------
12:49:02            FTP         172.23.8.801            1       5/1         23
03:15:34            Telnet      198.20.2.101           10       2/3        240
```

Descriptions of the fields are as follows:

Time

The first time the access violation occurred.

Protocol

The IP protocol for which the violation occurred.

Source IP

The source IP address of the unauthorized user.

Attempts

The number of access attempts made by this user within the sample period (5 minutes).

Slot/Intf

The physical port that received the unauthorized user information.

Elapsed Time (secs)

The duration (in seconds) from the first unauthorized access to the end of the sampling period.