Management Card and Serial Control Card for ServSwitch™ Multi

KV1608C-R3
KV1609C
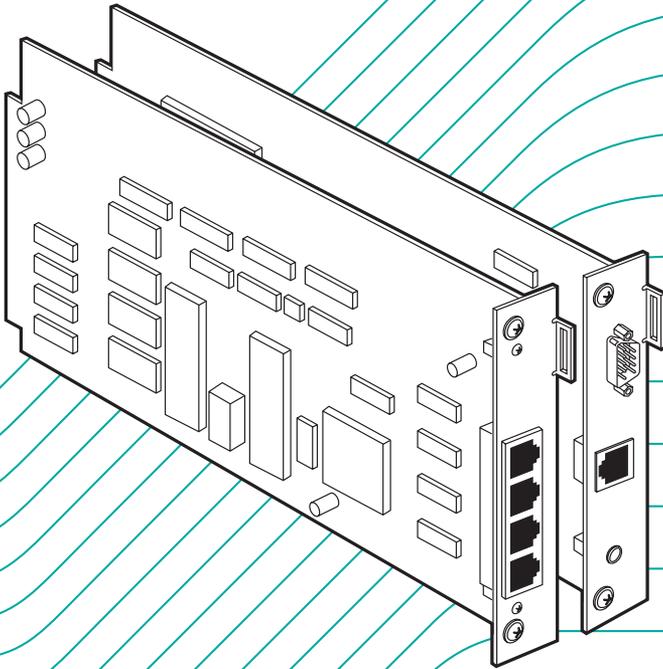
BLACK BOX®
NETWORK SERVICES

Welcome to the ServSwitch™ Family!

Thank you for purchasing a BLACK BOX® ServSwitch™ Brand KVM-switch accessory! We appreciate your business, and we think you'll appreciate the many ways that your enhanced keyboard/video/mouse switching system will save you money, time, and effort.

That's because our ServSwitch family is all about breaking away from the traditional, expensive model of computer management. You know, the one-size-fits-all-even-if-it-doesn't model that says, "One computer gets one user station, no more, no less." Why not a single user station (monitor, keyboard, and mouse) for multiple computers—even computers of different platforms? Why not a pair of user stations, each of which can control multiple computers? Why not multiple user stations for the same computer?

With our ServSwitch products, there's no reason why not. We carry a broad line of robust solutions for all these applications. Do you have just two PCs, and need an economical alternative to keeping two monitors, keyboards, and mice on your desk? Or do you need to share dozens of computers, including a mix of IBM® PC, RS/6000®, Apple® Macintosh®, Sun Microsystems®, and SGI® compatibles among multiple users with different access levels? Does your switch have to sit solidly on a worktable and use regular everyday cables? Or does it have to be mounted in an equipment rack and use convenient many-to-one cables? No matter how large or small your setup is, no matter how simple or how complex, we're confident we have a ServSwitch system that's just right for you.

The ServSwitch™ family from Black Box—the one-stop answer for all your KVM-switching needs!

<p align="center">✳</p>

This manual will tell you all about your new Management and Serial Control Cards for ServSwitch Multi™, including how to install and operate them. For an introduction to the Cards, see **Chapter 1**. The Management and Serial Control Card product codes covered in this manual are:

<p align="center">**KV1608C-R3**
KV1609C</p>

TRADEMARKS USED IN THIS MANUAL

BLACK BOX and the ◆ logo are registered trademarks, and ServSwitch, ServSwitch Multi, and ServSwitch Multi MX are trademarks, of Black Box Corporation.

Apple and Macintosh are registered trademarks of Apple Computer, Inc.

IBM, PC/AT, PS/2, and RS/6000 are registered trademarks of International Business Machines Corporation.

Microsoft, Windows, and HyperTerminal are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Sun and Sun Microsystems are registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

FEDERAL COMMUNICATIONS COMMISSION AND INDUSTRY CANADA RADIO-FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

EUROPEAN UNION DECLARATION OF CONFORMITY

This equipment has been tested and found to comply with the limits for a class A computing device in accordance with the specifications in the European standard EN55022. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses and can radiate radio-frequency energy, and if not installed and used in accordance with the instructions, might cause harmful interference to radio or television reception. However, there is no guarantee that harmful interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment on and off, you can correct the interference with one or more of the following measures:

(a) Reorient or relocate the receiving antenna.

(b) Increase the separation between the equipment and the receiver.

(c) Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

(d) Consult the supplier or an experienced radio/TV technician for help.

This equipment has also been tested and found to comply with European standard EN50082-1:1992.

$$C\epsilon$$

NORMAS OFICIALES MEXICANAS (NOM)
ELECTRICAL SAFETY STATEMENT

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.

2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.

3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.

4. Todas las instrucciones de operación y uso deben ser seguidas.

5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..

6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.

7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.

8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.

9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.

10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.

11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

Contents

Contents (continued)

1. Introduction

1.1 Overview

With the ServSwitch™ Multi Base Unit or Expansion Chassis or ServSwitch™ Multi MX (product codes KV150A-R2, KV160A-R2, and KV155A respectively), multiple users at your site can operate sets of servers and personal computers at the same time. Each ServSwitch Multi supports different types of external connections through a variety of plug-in cards.

Two of these types of plug-in cards are the Management Card (product code KV1608C-R3) and the Serial Control Card (product code KV1609C). The Management and Serial Control Cards work together to enable you to connect terminal-based file servers, network hubs, routers, and other serial server-room equipment to the ServSwitch Multi and control them using one keyboard, monitor, and mouse. This "terminal switching" requires at least one Management Card and one Serial Control Card in the system. The Management Card provides the menuing and advanced control features; Serial Control Cards provide four ports each for attaching equipment to the ServSwitch Multi system. From your Management Card, you may select any terminal in the system, regardless of which Serial Control Card it is attached to.

The Management Card functions similarly to a CPU Interface Card (KV2000C) in that you switch directly to it from your keyboard or with the ServSwitch Multi's on-screen menus or front-panel pushbuttons. It also supports telnet access to all functions from remote locations. Once you've switched to the Management Card, on-screen menus allow you to name and select the attached terminals in your ServSwitch Multi system. You can also configure data rate, data bits, stop bits, parity, and flow control for each terminal through the menus.

The Management Card has an onboard microprocessor that handles the Card's "Security Monitoring System" and "System Management Tools." With the Security Monitoring System, administrators can track all switching activity through a simple on-screen menu. Immediate feedback on logging and switching history is available for every system user. With the System Management Tools, network managers can display their ServSwitch Multi system configurations for easy troubleshooting. This menu-driven system shows the type of Card installed in each port and the current firmware and hardware revision of each. Information on the type of computer attached to each CPU Interface Card is also available.

The Management and Serial Control Cards are field-installable and flash-upgradable. Cards can be added or replaced without disassembling or powering down the system. This makes installation, configuration, and maintenance much easier.

1.2 The Cards and Cables Illustrated

The Management Card, shown in Figure 1-1, has an RJ-45 female 10BASE-T Ethernet jack for network and telnet control. It also has a DB9 male connector that functions as an EIA/TIA RS-232 serial interface (pinned out according to TIA-574, like the DB9 serial ports of an IBM® PC/AT® or PS/2® computer) so that you can upload security logs from the Card (see **Section 4.4.7**) or download firmware upgrades to the Card (see **Section 4.4.4**).
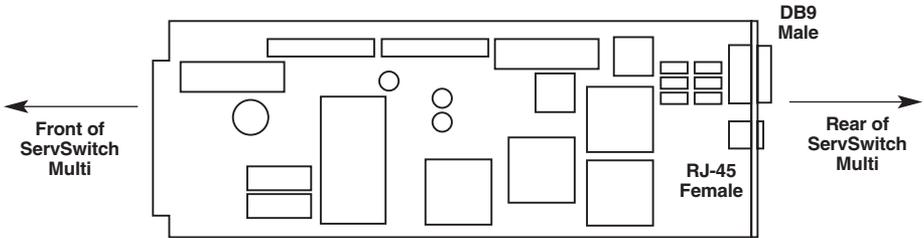
Figure 1-1. The Management Card.

You can run 10BASE-T patch cable, like the Category 5 patch cable shown in Figure 1-4 on the next page, from the Management Card's RJ-45 jack to a 10BASE-T hub, router, or switch in your network. You can run a PC/AT type null-modem cable (shown in Figure 1-2) from the Management Card's DB9 serial port to a PC running a terminal emulator.
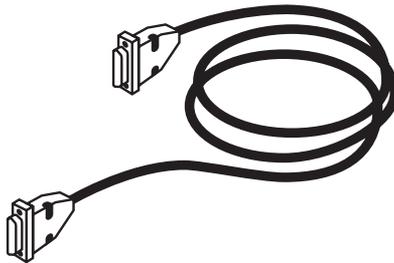
Figure 1-2. PC/AT type null-modem cable (EYN257H).

The Serial Control Card, shown in Figure 1-3, has four RJ-45 female connectors. These function as proprietarily pinned EIA/TIA RS-232 serial interfaces for connection to, and communication with, your servers, hubs, routers, etc.
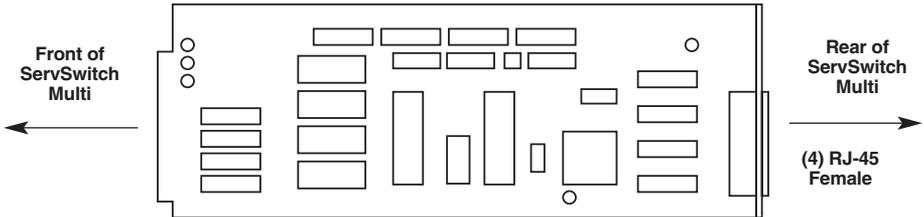
Figure 1-3. The Serial Control Card.

You can run a Category 5 twisted-pair patch cable (shown in Figure 1-4) from any port on the Serial Control Card to your equipment. To attach the cable to your equipment, you'll need a modular adapter (see **Section 2.2**).
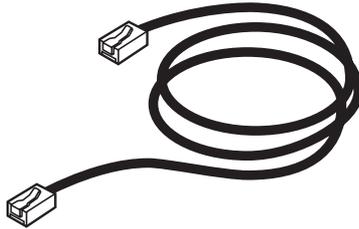
Figure 1-4. CAT5 stranded patch cable (EVMSL05).

2. Installation

2.1 Installing the Cards

To install a Management Card or Serial Control Card in a ServSwitch Multi or ServSwitch Multi MX, take these steps:

1. Position the ServSwitch Multi or MX so that its rear panel is facing you, as shown in Figure 2-1. Choose an available slot. In most cases, any slot that is covered with a blank (connectorless) panel will be available. However, note that on the Base Unit or MX, the local-console module on the far left end of the Switch's rear panel *is* covered by a blank panel but *is not* an available slot; no ServSwitch Multi Card of any type can be installed in that slot. Remember that the option slot (the slot just to the right of the local-console module, which has no corresponding front-panel LED or pushbutton) *is* an available slot and can host any card other than a CPU Interface Card.

BASE UNIT OR MX: **Local console module (not available)**   **Option slot (available)**   **Slots corresponding to lettered channels (all available)—MX will have fewer of these**

EXPANSION CHASSIS: **Slots corresponding to lettered channels (all available)**
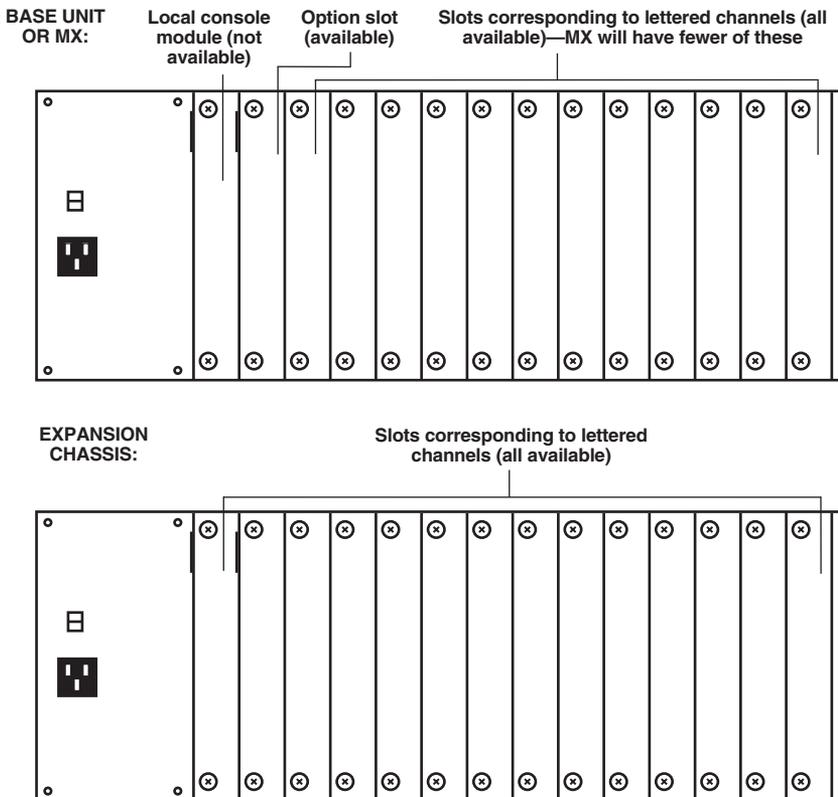
Figure 2-1. The ServSwitch Multi rear panels (as shipped from the factory).

2. *If your ServSwitch Multi manual is dated later than July 1998:* Once you've chosen the slot, write down the letter of the corresponding channel in the "Channel" field of this Card's record in a copy of the Management/Control Cards pages of the System-Configuration Chart (see **Appendix A** in your ServSwitch Multi manual). At this time you should also write down what appears on the Card's label (just to the right of the HD62 connector if you look at the connector from the rear) in the Chart's "Card-Label Information" field, and (if the ServSwitch Multi unit is part of a cascaded system) you should write down the Switch's address in the "Switch Address" field as well.

3. Remove the panel covering the available slot by unscrewing the two Phillips-head screws that hold it in place. (Save these screws; you'll be replacing them momentarily.)

4. If you look into the open slot on the Switch, you will see "guide tracks" that the top and bottom of the Card should slide along when you install it. Slide the new Management Card or Serial Control Card gently into the slot along these tracks, until the Card's connector or connectors line up flush with the back of the unit, as shown in Figure 2-2.
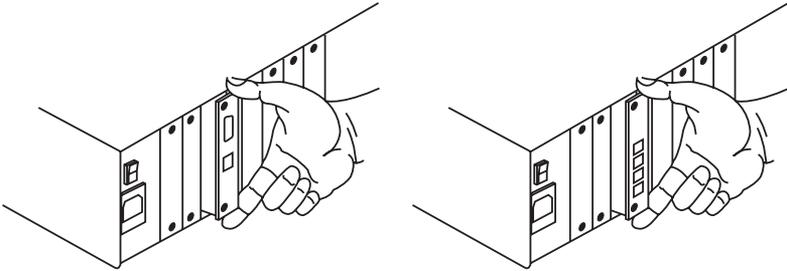
Figure 2-2. Inserting a Card in the Switch (Management Card shown at left, Serial Control Card shown at right).

5. Secure the Card in the Switch with the screws you removed in step 3. Retighten the screws completely, but do *not* overtighten them.

Repeat the above procedure for every Management Card or Serial Control Card in your system.

2.2 Attaching Devices to the Serial Control Card

The Serial Control Card has four ports available for attaching terminals, hubs, routers, and other serial equipment. To attach your devices to these ports, you will need:

- Category 5 UTP cables. We provide these cables, terminated with RJ-45 plugs, in many stock lengths from 1 to 100 feet (0.3 to 30.5 m) and in any custom length you might want.

- Modular adapters to patch the RJ-45 plugs to your devices. We have these types available:

RJ-45 female to:	Pinned as*:	Product Code:
DB9 male	DCE	FA062M-DCE
DB9 male	DTE	FA062M-DTE
DB9 female	DCE	FA062F-DCE
DB9 female	DTE	FA062F-DTE
DB25 male	DCE	FA085M-DCE
DB25 male	DTE	FA085M-DTE
DB25 female	DCE	FA085F-DCE
DB25 female	DTE	FA085F-DTE

  * This column shows how the DB connector on the *adapter* is pinned out. Adapters pinned as DCE are designed to be connected to DTE devices such as PCs, terminals, etc. Adapters pinned as DTE are designed to be connected to DCE devices such as modems and most bridges and routers.

To attach a serial device to the ServSwitch Multi system, take these steps:

1. Attach the appropriate adapter to the serial port of your device.

2. Plug one end of your CAT5 cable into the RJ-45 socket on the adapter.

3. Plug the other end of the cable into the first available port on the rear of your Serial Control Card.

Repeat steps 1 through 3 for each device you want to connect to the Serial Control Card.

3. Initial Configuration

Once you install the Management Card and connect it to your network, you'll
need to configure it with your network's TCP/IP settings if you'll be using it for
remote access. **Sections 3.1** and **3.2** describe how to do this. **Section 3.3** lists the
other settings you'll need to configure to get your serial-control system going, and
points to the relevant sections elsewhere in the manual that give you point-by-point
descriptions of how to do it.

3.1 Automatic Network Configuration Using DHCP

By default, the Management Card will download the characteristics of the network
it's attached to using Dynamic Host Configuration Protocol (DHCP). However, the
Management Card will only attempt to receive network parameters from a DHCP
server when the Card is first reset. If you want to use DHCP to configure the
Management Card's network parameters, but didn't have an Ethernet connection
in place when the Card was first installed and powered on, you'll need to reset the
Management Card to allow it to communicate with your DHCP server.

   To reset the Management Card, take these steps:

   1. From a user station attached to a ServSwitch Multi User Card, select the
      Management Card the same way you would select a computer. The
      Management Card's User Option Menu should appear on your screen.

   2. From the User Option Menu, press "A" to display the Administrator Menu.

   3. From the Administrator Menu, press "N" to display the Network Parameter
      Menu.

   4. From the Network Parameter Menu, press the letter "R" to trigger the reset.

   5. When prompted to confirm that you want to reset the card, answer "Y".

3.2 Static Network Configuration

Instead of using DHCP, if you would rather manually set the Management Card with a static network configuration, take these steps:

1. From a user station attached to a ServSwitch Multi User Card, select the Management Card the same way you would select a computer. The Management Card's User Option Menu should appear on your screen.

2. Select option "A", Administrator Menu, and then "N", Network Options.

3. At the "Enter selection" prompt, press "7" to to toggle the DHCP setting to "disabled".

4. Use the other options in this menu ("1" through "6" and "8") to enter the appropriate settings for your network, then press "X" to exit the menu. Refer to **Section 4.6.3**.

3.3 Other Important Settings

After doing the basic network configuration in **Section 3.1** or **3.2**, use other configuration functions available through the Administrator Menu and Channel List to get your Management Card and Serial Control Cards up and running. Follow the directions in the indicated sections of this manual.

- Set an admin password, or disable security on the Management Card (see **Section 4.6.4**).

- Set the relative priority of User-Card vs. telnet sessions (see **Section 4.6.5**).

- Add your serial devices to the Management Card's internal database. Refer to the start of **Section 4.5**, then take the steps listed in **Section 4.5.3** for each of your devices. Make sure that the serial communication settings of your devices match those of the Serial Control Card port that they're attached to; see **Section 4.5.2**.

- Add your users to the Management Card's internal database. Refer to the start of **Section 4.6.6**, then take the steps listed in **Section 4.6.6.B** for each of your users.

4. Operation

4.1 Addressing Devices on the Serial Control Card

Since each Serial Control Card has four ports, channel addressing (for port-selection purposes) requires more than just a chassis number and slot letter. You must also designate which port on the Serial Control Card the device is attached to. Ports are numbered from top to bottom as shown in Figure 4-1.
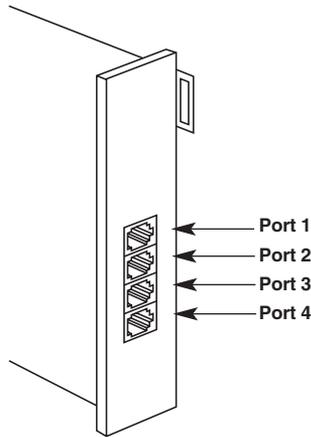
Figure 4-1. Port addresses on a Serial Control Card.

For example, the device attached to the second port on the Serial Control Card in slot D of chassis 15 would be addressed "l5D2".

4.2 Getting Started: The User Option Menu

When you first select your Management Card, the User Options Menu appears on your monitor:

```
      User Option Menu
   Revision: A-00   Address: 1-F
    --------------------------
    S    Security monitor
    M    Management tools
    O    Open a port session
    A    Administrator options
    X    eXit session
    --------------------------
    Enter selection:
```

Select "Security monitor" by pressing "S" to activate a three-part screen that includes an Active User List, an Alert Messages Window, and a Log Window. You can use these windows to track logging and switching activity for all system users, as well as to monitor for failed or unauthorized system activity.

Choose "Management tools" by pressing "M" to open a menu of basic system-management functions. You can use this menu to display system configuration, download information to the Card's flash ROM, transfer information between Cards, or upgrade the Card's firmware with TFTP.

If you want to open a port session, select "Open a port session" by pressing "O".

Select "Administrator options" by pressing "A" to perform administrator-level configuration and maintenance of the Card, such as network configuration and user administration.

These main selections are described in **Sections 4.3** through **4.6**. When you're finished, exit the menu system and end your session by pressing "X" followed by [Enter]. If you're using the Management Card through a telnet connection, your telnet client will then tell you that the session has been closed. If you're using the Management Card through a user station, and your Management-Card account is password-protected, you'll be logged out and the login prompt will appear on your screen. If you're using the Management Card through a user station, and your Management-Card account is *not* password-protected, pressing "X" won't have any effect—the User Options menu will remain on your screen.

4.3 Using the Security Monitor

Select the Security Monitor by pressing "S" at the User Option Menu. A screen like the one shown in Figure 4-2 will appear on your monitor.

```
+========= Active User List =========++----------- Alert Messages -----------+
|Chan  User            Selected Chan  ||Apr-20-01 14:40:38 Src: 4-C           |
|----- -------------- --------------  ||       LOGIN FAILED: INVALID PASSWORD |
|  1-F Administrator   Telnet         ||       Username: "Charlene"           |
|  1-H Administrator   1-A            ||                                      |
|  2-L Bernard         2-B            ||                                      |
|  3-C Georgia         3-A            ||                                      |
|  4-C Charlene        4-A            ||                                      |
|                                     ||                                      |
|                                     ||                                      |
|                                     ||                                      |
|                                     ||                                      |
+=====================================++--------------------------------------+
+- Log Window ---------------------------------------------------------------+
|Time & Date       ALERT Source Description                                  |
|----------------- ----- ------ --------------------------------------------  |
|May-20-01 15:06:06        1-L LOGIN:  SUCCESSFUL     User: Administrator     |
|May-20-01 15:06:11        1-E SELECT: User: "-- UNKNOWN -- "                 |
|                              Channel: 1-L                                  |
|Jun-09-01 15:41:59        1-F LOGIN:  SUCCESSFUL     User: Administrator     |
|Jun-09-01 15:43:39        1-H SELECT: User: "-- UNKNOWN -- "                 |
|                              Channel: 1-F                                  |
+---------------------------------------------------------------------------+
TAB Next window   - Page Up  + Page Down
```

Figure 4-2. The Security Monitor screen.

The Security Monitor features the Active User List, the Alert Messages Window, and the Log Window. Press the [Tab] key to select the active window. The active window will be displayed with a double line at the top and bottom of the window. The sample screen in Figure 4-2 shows the Active User list as the active window. Available options for the active window will appear at the bottom of the screen. You can press the "X" key at any time to return to the User Option Menu. Each window is described in the following subsections.

4.3.1 THE ACTIVE USER LIST

The Active User List shows which users are currently logged on and what channel they are switched to. Each user's address and name are listed as well as their selected computer channel.

When this window is active, you have three control options: Press [PgUp] (the page-up key) to view the previous page of users, [PgDn] (the page-down key) to view the next page of users, [Home] to move to the top of the user list, [End] to move to the bottom of the user list, or [Tab] to make a different window active.

```
+========== Active User List ==========+
|Chan  User             Selected Chan  |
|----- --------------- --------------  |
|  1-F Administrator    Telnet          |
|  1-H Administrator    1-A             |
|  2-L Bernard          2-B             |
|  3-C Georgia          3-A             |
|  4-C Charlene         4-A             |
|                                       |
|                                       |
|                                       |
|                                       |
+=======================================+
```

Figure 4-3. The Active Users List.

4.3.2 THE ALERT MESSAGE WINDOW

The Alert Message Window lists any failed or unauthorized command and, for user-station connections, turns the window red to alert administrators to the message. Pressing the space bar clears the alert by removing the red background. The message itself remains on-screen until the window is full, then is replaced by newer messages. The date, time, user name, channel, and unauthorized activity are listed for each message.

When this window is active, you have two control options: Press [Space] (the space bar) to clear an alert or [Tab] to make a different window active.

```
+=========== Alert Messages ===========+
|Apr-20-01 14:40:38 Src: 4-C            |
|       LOGIN FAILED: INVALID PASSWORD  |
|       Username: "Charlene"            |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
+=======================================+
```
Figure 4-4. The Alert Message Window.

Enter a remote chassis' address, or press [Enter] at the prompt to see information on the local chassis. This will bring up a screen like that shown in Figure 4-6, displaying the selected ServSwitch Multi's current configuration.

```
                        EPROM   FLASH
Chan  Card Type  HW Rev FW Rev  FW Rev   Serial #    Other Information
----  ---------  ------ ------  ------   ----------  ----------------
 3-A  XPAC       B03    * A-05   -NA-    0123456789  PC + PS/2 mouse
 3-B  XPAC       C00    * B03C   -NA-    1234567890  No cable attached
 3-C  Empty
 3-D  Empty
 3-E  Empty
 3-F  Empty
 3-G  Empty
 3-H  XPXT       A00      XB84  * XF82   2345678901  P1[N/C] P2[  4-F]
 3-I  XPXT       A00      XB84  * XF82   3456789012  P1[N/C] P2[  5-F]
 3-J  XPLU       C00    * B03C   -NA-    4567890123
 3-K  XPDU       D01      C01C  * C04A   5678901234
 3-L  XPXR       A00      XC15  * XG18   6789012345
 3-M  XPXR       A00      XC15  * XG18   7890123456
 3-N  LCI        C00    * B02B   -NA-    8901234567
* - Indicates active device
```

Figure 4-6. The configuration display.

NOTES

1. The "Chan" column lists the channel address of each component (Card or module). For Base Units, the option slot will always be listed as channel "M", and the local-console module will always be listed as channel "N". For MXs, the local-console module will always be listed as channel "E".

2. The "Card Type" column shows what type of component it is: "LCI"=Local-console module, "XPAC" = CPU Interface Card, "XPLU" = Universal User Interface Card, "XPDU" = User Interface Card with On-Screen Display, "XPXT" = regular Transmit Card, "XPXR" = regular Receive Card, "XPST" = CAT5 Transmit Card, "XPSR" = CAT5 Receive Card, "XPIQ" = older (original or "-R2" version) Management Card, "XPIB" = newer ("-R3" version) Management Card, and "XPSI" = Serial Control Card.

3. The "HW Rev" column lists the revision level of the component's hardware.

4. The "EPROM FW Rev" column lists the revision level of the component's original firmware (that is, the firmware burned into its EPROMs at the factory).

5. The "FLASH FW Rev" column lists the revision level of the most recent firmware (if any) that has been downloaded to the component's flash ROMs.

6. The "Serial #" column lists the component's serial number. Unless the component is an eval, demo, or special unit, the serial number should always be numeric.

7. The "Other Information" column shows the Switch's best guess of what the component is attached to (if anything) based on the states of the ground leads of the component's connector(s).

8. What "* - Indicates active device" means is that the asterisk shows whether the component is running using the firmware in its EPROMs or the firmware in its flash ROMs.

4.4.2 DISPLAY FLASH ROM STATUS

When you choose option 2 from the Management Tools menu, you'll be prompted to enter a channel address (the default address in brackets will be the address of the Management Card itself):

```
Display Flash ROM status

Channel address [1-F]:
```

Enter a remote address or leave the field blank for the local channel (that is, for the Management Card). The firmware type and current firmware-revision level of the selected Card—which can be any type of ServSwitch Multi Card—will be displayed as shown below.

```
                 FLASH
Pos Flash Type FW Rev
--- ---------- ------
 1  XPIB       -NA-
 2  Available
 3  Available
 4  Available
 5  Available
 6  Available
 7  Available
 8  Available
 9  Available
```

The "Pos" column shows which "slot" in the Card's memory a firmware program is stored in: Management Cards have nine of these, numbered 1 through 9; all other Cards have only one, numbered 1. The "Flash Type" indicates what type of Card the program is designed for—see Note 2 on the previous page for explanations of what these abbreviations mean—or says "Available" if the slot is empty. The "FW Rev" column indicates the revision level of the program, or says "–NA–" if (as is the case with the Management Card/XPIB firmware in slot one) the firmware can't be transmitted to any other Card.

4.4.3 DOWNLOAD LOCAL TO REMOTE FLASH ROM (CROSSLOAD FIRMWARE BETWEEN CARDS)

If the Management Tools serial-port function is enabled (you can check this by selecting option 10), you can use option 3 to transfer firmware from the local Management Card to any other ServSwitch Multi Card in your system that you can transmit to. When you select this option, the local Management Card checks the firmware programs it has loaded in its memory, then displays descriptions of them on screen (see the last paragraph on the previous page for what each column means).

```
Download local to Remote Flash ROM

Validating Flash ROM files...

     FLASH
Pos Flash Type FW Rev
--- ---------- ------
 1  XPIB       -NA-
 2  XPLU       C-02
 3  XPXR       C-04
 4  XPXT       C-04
 5  Available
 6  Available
 7  Available
 8  Available
 9  Available
```

The Card then prompts you for the numbered slot in its flash memory where the program you want to transfer is stored (the program in position 1 can't be transferred to any other Card; the default position in brackets is always #2):

```
Local Flash ROM number (2..9) [2]:
```

Then the Card prompts you for the address of the Card that will be *receiving* the firmware program (the default address in brackets is the Management Card's):

```
Channel address [2-M]:
```

Finally you're prompted for the number of the slot in the *other* Card's memory where you want *that* Card to store the program ("1" is the default option, and is the only valid option for any type of Card other than Management Cards):

```
Remote Flash ROM (1..9) [1]:
```

Type in the number of your desired slot or press [Enter] to accept the default value. As soon as you do so—provided the addresses and the file are all valid—the transfer begins. Depending on whether the transfer succeeds or not, one of these messages will be displayed:

```
Flash ROM download was SUCCESSFUL
Flash ROM download FAILED
```

4.4.4 DOWNLOAD SERIAL PORT TO FLASH ROM (DOWNLOAD FIRMWARE TO A CARD)

Option 4 allows you to transfer firmware upgrades from your computer to the flash memory of any local Card through the Management Card's serial port. When you select this option, the Management Card will prompt you to set your computer's COM (serial) port to the settings required for the transfer to work (38,400 bps, 8 data bits, 1 stop bit, and no parity):

```
Download Serial Port to Flash ROM

Configure your COM port for the following:

  Baud rate: 38400
  Data bits: 8
  Stop bits: 1
  Parity: None
```

You will be prompted for the channel address of the Card you're downloading the firmware to (press [Enter] to accept the default address in brackets, which will be that of the Management Card itself):

```
Channel address [3-H]:
```

You will then be prompted for the number of the slot in that Card's flash memory that you want the firmware program to be installed in ("1" is the default option, and is the only valid option for any type of Card other than Management Cards):

Local Management Card: `Local Flash ROM number (1..9) [1]:`
Any other Card: `Flash ROM number (1..7) [1]:`

Once you provide this information, you'll be prompted to

```
Start XMODEM download now
```

Anytime after the second line appears, begin transmitting the new firmware to the Management Card using the XMODEM protocol. (You can use a null-modem cable such as our product code EYN257H to connect the Card to the computer: Attach one end of this cable to the Card's DB9 male serial port and the other end to the computer's serial port.) Depending on whether the transfer succeeds or not, one of these messages will be displayed:

```
Flash ROM download was SUCCESSFUL
Flash ROM download FAILED
```

If you have difficulty, call Black Box for technical support.

4.4.5 SEARCH FOR CONNECTED CHASSIS

Choose option 6 to search your ServSwitch Multi system for all connected chassis. You will be prompted for the range of chassis numbers you want to search. Enter the first and last chassis numbers for your search or press Enter to accept the default values of 1 and 25. After you have entered these values, the Card will search for chassis with addresses in that range, and list on screen the ones it finds.

```
Search for connected chassis

First chassis number [1]:
Last chassis number [25]:

Searching...done

Chassis units found:
```

4.4.6 SET DATE AND TIME

Choose option 7 to set the date and time for your Management Card. This is used to time-stamp the events in the security log.

```
Set Date and Time

Current date is Fri 02-04-2000
Enter new date (mm-dd-yy):

Current time is 10:26:26a
Enter new time:
```

4.4.7 TRANSFER SECURITY LOG

The Management Card's "security log" (the contents of its Log Window—see **Section 4.3.3**) begins to overwrite itself after 1000 entries. If you want to keep a permanent record of it, you can upload it in file format to a TFTP server on your network. (For more information about using the Card with TFTP servers, see **Section 4.4.9**.) If, rather than downloading this file periodically, you'd like the information to be continuously transmitted to a "log host" server, see **Section 4.6.3**.

When you select option 8 at the Management Tools menu, you will be prompted for several values. Type these in and press [Enter], or press [Enter] without typing anything to accept the default values in brackets:

- The date and time of the first log record that you want to transfer. (The default date and time are those of the oldest record in the log.) All records appearing in the log since that date and time will be sent.

- The server's host name or TFTP address. (The default address is that of the source of the most recent TFTP transfer or telnet session, or "0.0.0.0" if this Card hasn't been involved in any transfers or sessions yet.)

- The remote filename (default is "security.log") that you want the log to be saved under.

Once you've entered these values, the log transfer will begin. The data will be formatted the same way it is in the Log Window. Each line of ASCII text ends with carriage-return and line-feed codes.

```
Transfer security log

Date of first log record [ May-08-2001 ]:
Time of first log record [ 15:13:21 ]:

Finding Security Event Log Records
  that have occurred since: May-08-2001 15:13:21

437 Records found.
Preparing to transfer them to TFTP Server...

TFTP Transmit Security Log

Enter TFTP Server IP address
 or Host name [0.0.0.0]:

Enter Remote filename:

Transferring Security Event Log Records
  that have occurred since: May-08-2001 15:13:21

nn Records transferred
```

When the transfer is complete, press any key to return to the Management Tools menu. If there is any question about whether the transfer was successful, compare the number of records in the file with the number of records that the Card says it transferred. Repeat the transfer if the numbers don't match.

4.4.8 TRANSFER CHANNEL LIST

You can use the Channel List menu to edit the local Management Card's channel list in any of several ways (see **Section 4.5**). Once you finish making your desired changes, you can choose option 9 at the Management Tools menu in order to send the new and improved channel list to another Management Card elsewhere in your system—or to receive the list from another Card if there's a better version elsewhere, or if changes you made to the local Card's list turn out to have been mistaken. When you select this option, these lines will be displayed on the screen:

```
Transfer Channel List

Configure Transfer Settings

   Press SPACE to change, ENTER to accept

Transfer Option: Transmit
```

You can can press [Enter] to accept the default "Transmit" option, so that the local Management Card sends its channel list to the remote Card, which replaces its own list with the local Card's. Or you can toggle to "Receive," so that the local Card overwrites its own list with the remote Card's. Either way, you'll be prompted for the address of the remote Card (the default address in brackets will be that of the local Card):

```
Channel address [0-H]:
```

Once you enter the address (chassis number followed by slot letter) of the remote Management Card, you'll be prompted for the administrator password of that Card, to verify that you have the right to order this transfer. Once you enter the remote Card's admin password, the transfer begins. You will receive one of these messages to indicate the result of the attempted transfer:

```
Successfully completed
Disconnected from remote
Invalid remote password
Remote channel busy
No response from remote
```

If the transfer is successful, the Card will reset itself. This will probably take at least 45 seconds; if you're accessing the Card through a telnet connection, it might take twice that long until the Card reinitializes its network presence.

Note that you can transfer the channel list *from* an older (original or "-R2") Management Card *to* a newer ("-R3") Management Card, but not vice versa. If you

want to do this, keep in mind that because the older Cards don't maintain a user list, any user list in the newer Card will be erased.

4.4.9 TFTP RECEIVE UPGRADE

You can use option 11 in conjunction with a TFTP (Trivial File Transfer Protocol) server to upgrade your Management Card to a new version of its firmware. If you don't have a TFTP server, we recommend a Windows based freeware server called PumpKIN (©1997, 1998 by Klever Group, Inc. [http://www.klever.net], written by Michael Krelin). You should be able to find PumpKIN at the Klever Group Web site (look for a file called "PumpKINinstall.exe"); if not, call Black Box for technical support.

Double-click on the "PumpKINinstall.exe" icon and follow the onscreen instructions to install PumpKIN. Once it's installed, take these steps to configure it:

1. Run PumpKIN and click its "Options" button. In the screen that appears, the "Server" tab should be selected by default; if it isn't, select it.

2. In the "TFTP File System Root (Download Path)" field, type in the pathname of the directory you want to use as your TFTP file system's root directory—for example, "C:\tftpfiles".

3. In the section labeled "Read Request Behavior," you must have "Give All Files" or "Always Prompt Before Giving Files" selected. Other options can be set differently depending on how you'll be using TFTP with the Management Card, and on whether you'll be using TFTP with any other equipment.

When you're ready to upgrade the Management Card's firmware, the Card will try to connect to a TFTP server to get the firmware file. By default, it will look in the TFTP file system's root directory for a file called "kv1608c.bin", although the actual filename might be different (Black Box Technical Support will be able to tell you the name of the file you'll need). Take these steps to upgrade the Card's firmware:

1. Make sure that the upgrade file, whatever it's named, has been downloaded and placed in the TFTP file system's root directory (which you set up in step 2 above).

2. Establish a telnet session to the Management Card. Refer to your telnet client's documentation if you're not sure how to do this.

3. Select System Management Tools option 11, "TFTP Receive Upgrade",.from the Management Tools menu.

4. You will first be prompted for the IP address of your TFTP server, as shown below. The default address in brackets will be that of the device that was the source of the most recent telnet session, or "0.0.0.0" if this is the Card's first telnet session. Press [Enter] to accept the default value, or type in the proper address and press [Enter].

5. You'll then be prompted for the "remote filename" (the name of the upgrade file). Type this in and press [Enter], or simply press [Enter] without typing anything to accept the default filename, "kv1608c.bin".

```
TFTP Receive Upgrade

Enter TFTP Server IP address
  or Host name [0.0.0.0]:

Enter Remote filename [KV1608C.BIN]:
```

After the Management Card receives the upgrade file, you will receive one of these messages to indicate the result of the attempted transfer:

```
Successfully completed
Disconnected from remote
Invalid remote password
Remote channel busy
No response from remote
```

If the transfer is successful, you'll be prompted to press any key to reset the Card. Once you do, the Card will reset itself. This will take at least 45 seconds; if you're accessing the Card through a telnet connection, it might take twice that long until the Card reinitializes its network presence. The Card will begin running its new firmware, and you'll have to re-establish a connection to it.

4.5 Using the Channel List

Select the Channel List by pressing "O" (for "Open a port session") at the User Option Menu. It will appear on your monitor, labeled "Terminal Control Panel Channel List".

```
    Terminal Control Panel
         Channel List
    ------------------------------
     <Name>              Address
-->  ModemPool             1C1       <--
     router_1              1C2
     web_server            1C3



     Search:
    ------------------------------
    Enter: Open session  Ctrl-S: port Settings
    Ctrl-E: Edit         Ctrl-D: Delete channel
    Ctrl-A: Add channel  Ctrl-X" eXit channel list
    '-' Sort by address  '+' Sort by name
    Ctrl-T: Go to Top    Ctrl-B: Go to Bottom
    Ctrl-R: Remote close session
```

The Channel List will display all devices that (a) are connected to Serial Control Cards, (b) have been added to the Management Card's database, and (c) you have access rights to. Use your keyboard's up- and down-arrow keys to highlight a specific device, or use keyboard shortcuts to take you to the top or bottom of the list. To quickly locate an attached device, start typing in its name at the "Search" prompt; the Card will scroll down the list to the first device whose name matches the characters you've typed in so far. When the device you want is highlighted, press [Enter] to select it.

The Channel List can be cross-loaded to other Management Cards in your system, as described in **Section 4.4.8**. This can be a particularly useful shortcut after you've added, edited, or deleted devices as described in **Sections 4.5.3** through **4.5.5**.

You can use the keyboard commands listed below the "Search" prompt to navigate the menu and to perform the session-related functions described in the rest of this section. The letter characters in these commands are shown as uppercase, but can be entered either as uppercase or lowercase.

Press These Keys...	...To Do This
[↑], [↓] (up, down arrows)	Move the highlight bar up and down through the available channels and ports.
[Ctrl]-"T"	Move the highlight bar to the top of the Channel List.
[Ctrl]-"B"	Move the highlight bar to the bottom of the Channel List.
[–] (keypad minus)	Sort the Channel List by address. Brackets ("<>") around the Address heading will confirm that sorting by address is the active sort order.
[+] (keypad plus)	Sort the Channel List by name. Brackets ("<>") around the Name heading will confirm that sorting by name is the active sort order.
[Enter]	Open a session with the selected (highlighted) device. See **Section 4.5.1**.
[Ctrl]-"S"	Change the settings of the selected (highlighted) Serial Control Card port, including the data rate, data bits, stop bits, etc. See **Section 4.5.2**.
[Ctrl]-"E"	Edit the selected (highlighted) channel's name or address. See **Section 4.5.4**.
[Ctrl]-"D"	Remove the selected (highlighted) channel. See **Section 4.5.5**.
[Ctrl]-"A"	Add a new channel to your menu. See **Section 4.5.3**.
[Ctrl]-"R"	Close another user's session if you have administrator rights to that user's account. See **Section 4.5.6**
[Ctrl]-"X"	Exit the Channel List and return to the User Options menu.

4.5.1 OPENING, CONTROLLING, AND CLOSING A SESSION

To open a serial-port session with an attached device:

1. At the Channel List, use the keyboard's arrow keys and/or the search function to highlight the device you want to communicate with.

2. Press the [Enter] key to open a session with that device.

If you're working with the Management Card through a ServSwitch Multi user station, press [Alt] along with the letter "B" to send a break or break condition to the device during a session, or press [Alt] along with "C" to close the session and return to the User Options menu.

If you're working with the Management Card through a telnet connection, send a telnet "break" command to bring up the Management Card's Break menu. (This command varies among telnet clients—consult your client's manual if you're not sure how to do it. Unfortunately, the basic Telnet client included with Microsoft Windows doesn't support this command at all.) At the Break menu, press "B" to send a break character and return to the current session, press "R" to return to the session without sending a break, or "C" to close the current session.

4.5.2 CHANGING PORT SETTINGS

Once you've connected a new serial device to a port on one of your Serial Control Cards, you can adjust the settings of this port to match those of the device:

1. At the Channel List, use the keyboard's arrow keys and/or the search function to highlight the device whose Serial Control Card port you want to configure.

2. Press [Ctrl] along with the letter "S" to edit the port's settings. The Port Settings menu should appear:

```
     Terminal Control Panel
         Port Settings
    -------------------------------
    Name              web_server
    Address           1C3
 --> Baud rate        9600         <--
    Data bits         8
    Stop bits         1
    Parity            None
    Flow control      Xon/Xoff
    -------------------------------
    Space - change   Enter - commit
    x - eXit and discard changes
```

NOTE

If, after pressing [Ctrl]-S, you receive the message "ERROR: Serial port did not respond," the Management Card cannot retrieve the current serial-port settings from the Serial Control Card. Verify that the port address is correct, and that the Serial Control Card is actually installed in that slot. (For example, if the address of a device is "1C4", it should be attached to Port 4 of a Serial Control Card installed in slot C of ServSwitch Multi chassis 1.) If the Serial Control Card is installed in a different chassis from the Management Card, you might also want to verify that the expansion cabling between the chassis hasn't been disconnected or broken.

3. Use your keyboard's up- and down-arrow keys to highlight a characteristic that you want to change.

4. Use the spacebar to toggle through the available settings for that characteristic. When you reach the setting you want, press [Enter] to save that setting or "X" to exit the menu without saving the change.

4.5.3 ADDING A DEVICE

To add a new device to the Channel List, press [Ctrl] along with the letter "A". You'll be prompted to enter a name for the device, and then the device's port address.

NOTES

Keep in mind that the addresses of devices attached to Serial Control Cards are comprised of the ServSwitch Multi chassis number, followed by the Serial Control Card's slot number, followed by the port number on the Card. Refer to Section 4.1**.**

You can add devices to the list that you haven't physically attached yet, but until you actually install the devices, you won't be able to edit their entries as described in Section 4.5.2**.**

When you've finished typing in the address, press [Enter] to save the information and be returned to the Channel List, which will contain the new entry you just added.

```
 Add a Port

 Enter port name: mail_server
 Enter port address: 1C4

    Terminal Control Panel
          Channel List
  -----------------------------
   <Name>              Address
-->  mail_server        1C4        <--
     ModemPool          1C1
     router_1           1C2
     web_server         1C3




 Search:
 -----------------------------
 Enter: Open session  Ctrl-S: port Settings
 Ctrl-E: Edit         Ctrl-D: Delete channel
 Ctrl-A: Add channel  Ctrl-X" eXit channel list
 '-' Sort by address  '+' Sort by name
 Ctrl-T: Go to Top    Ctrl-B: Go to Bottom
 Ctrl-R: Remote close session
```

4.5.4 EDITING A DEVICE

To edit the name or address of an existing device in the Channel List, take these steps:

1. At the Channel List, use the keyboard's arrow keys and/or the search function to highlight the device whose entry you went to edit.

2. Press [Ctrl] along with the letter "E".

3. Type in a new name for the device, or press [Enter] without typing anything else to keep the old name.

4. Type in a new address for the device, or press [Enter] without typing anything else to keep the old address. The changes will be saved and you'll be returned to the Channel List, which will reflect the changes you just made.

```
      Edit Port

       web_server              1C3

  Enter new name [web_server]:
  Enter new address [1C3]: 1D1

         Terminal Control Panel
              Channel List
      ------------------------------
       <Name>              Address
-->    mail_server           1C4      <--
       ModemPool             1C1
       router_1              1C2
       web_server            1D1




      Search:
      ------------------------------
      Enter: Open session  Ctrl-S: port Settings
      Ctrl-E: Edit         Ctrl-D: Delete channel
      Ctrl-A: Add channel  Ctrl-X" eXit channel list
      '-' Sort by address  '+' Sort by name
      Ctrl-T: Go to Top    Ctrl-B: Go to Bottom
      Ctrl-R: Remote close session
```

4.5.5 DELETING A DEVICE

To delete a device from the Channel List, take these steps:

1. At the Channel List, use the keyboard's arrow keys and/or the search function to highlight the device whose entry you went to edit.

2. Press [Ctrl] along with the letter "D".

3. The device's current name and address will be displayed, and you will be asked whether you really want to delete it from the list. Type "Y" to delete the device or "N" to keep it, then press [Enter]. You'll be returned to the Channel List, which will reflect the deletion if you went through with it.

```
        web_server              1D1

        Delete this port? (y/n):

           Terminal Control Panel
                 Channel List
       -----------------------------
        <Name>                  Address
  -->   mail_server             1C4        <--
        ModemPool               1C1
        router_1                1C2




        Search:
        -----------------------------
        Enter: Open session  Ctrl-S: port Settings
        Ctrl-E: Edit         Ctrl-D: Delete channel
        Ctrl-A: Add channel  Ctrl-X: eXit channel list
        '-' Sort by address  '+' Sort by name
        Ctrl-T: Go to Top    Ctrl-B: Go to Bottom
        Ctrl-R: Remote close session
```

4.5.6 REMOTELY CLOSING A SESSION

Because the Management Card can only support one open session at a time, it might sometimes be necessary to close another user's session before you can open your own. If you have administrator access to the Management Card that that user is connected to, take these steps to close his or her session remotely:

1. At the Channel List, use the keyboard's arrow keys and/or the search function to highlight the device whose session you want to close.

2. Press [Ctrl] along with the letter "R".

3. The device's current name and address will be displayed, and you will be asked for the administrator password for the remote user (that is, for the remote user's Management Card). Type in this password and press [Enter]. If the password is correct, the session will be closed and you'll be returned to the Channel List. If the password is entered incorrectly, you'll get two more chances to get it right; after the third failure, the other Management Card will refuse further communication attempts for approximately 15 minutes.

```
Close any remote sessions with:

mail_server          1C4

Administrator password for remote user:
```

4.6 Using the Administrator Menu

Select the Administrator Menu by pressing "A" at the User Option Menu. The
Administrator Menu will appear on your monitor. To exit this menu and return to
the User Option Menu, press "X". The menu's available functions are described in
the rest of this section.

```
      Administrator Menu
   Revision: A-00     Address: 1-F
    --------------------------
    D     Delete database
    I     Idle timeout (Not implemented.)
    N     Network options
    P     Change admin Password
    S     Session priority
    U     User list
    X     eXit admin options
    --------------------------
    Enter Selection:
```

4.6.1 DELETING A DATABASE

It might sometimes be necessary—especially when you're moving a Management
Card from one ServSwitch Multi system to another—to completely erase either or
both of the two databases that the Card maintains: the security logs and the
channel and user lists. To do so, take these steps:

1. At the Administrator Menu, press "D" to bring up the Delete Database Menu.

```
    Delete Database Menu
    --------------------------
    1. Security Logs
    2. Channel List and User List
    --------------------------
    Enter selection or X to exit:
```

2. Press "1" to delete the Card's security logs, "2" to delete the channel and user
   lists, or "X" or [Esc] to abort the deletion and return to the Administrator Menu.

3. You will be asked to confirm the deletion. Press "Y" followed by [Enter] to
   proceed with it, or "N" followed by [Enter] to cancel it and return to the
   Delete Database Menu. If you confirm the deletion, the Card will perform it
   and then reset itself. This will take at least 45 seconds; if you're accessing the
   Card through a telnet connection, it might take twice that long until the Card
   reinitializes its network presence.

4.6.2 SETTING THE IDLE TIMEOUT (NOT IMPLEMENTED)

This function is not implemented in the current version of the Management Card, but it will become available in a future firmware release. When it is, the "idle timeout" will be the amount of time a session is allowed to remain open after all keyboard activity stops. Once this timeout expires, the idle session will be automatically closed; the user will be returned to the User Options Menu. To set the length of this timeout—which you can do now, to prepare for the future, even though the timeout itself isn't supported yet—take these steps:

1. At the Administrator Menu, press "I" to bring up the Idle Timeout screen.

2. You will be prompted to enter a number of minutes from 0 to 60. Type in this number and press [Enter]. The new timeout value will be displayed on your screen. You can then press any key to return to the Administrator Menu.

```
          Idle Timeout
      --------------------------
      Current setting: 10 minutes

      Enter new timeout value [0-60]: 30

      New setting is 30 minutes

      Press any key to continue...
```

4.6.3 SETTING NETWORK OPTIONS

To reset the Management Card or change some of its network settings, type "N" at the Administrator Menu. The Network Parameter Menu will appear on your monitor.

```
              Network Parameter Menu
      -----------------------------------------------
      1. Node IP Address   = 170.20.3.44
      2. Network Mask      = 255.255.0.0
      3. Default Gateway   = 170.20.3.251
      4. DNS Servers        = 0.0.0.0, 0.0.0.0, 0.0.0.0
      5. User Node ID      = 2nd Floor MIS Control
      6. Ethernet Speed    = Auto Negotiation
      7. DHCP              = Disabled
      8. Loghost IP Address = 0.0.0.0
      -----------------------------------------------
      Node Ethernet Address = 00:E0:76:02:00:28
      ENTER (1-7) to change values
      ENTER (x) to exit
      ENTER R to reset the card
      -----------------------------------------------
      Enter Selection:
```

If you want to change one of the listed network parameters, you can press the corresponding number from "1" to "8". You will be prompted for the new value that you want to set the parameter to. Type in the new value and press [Enter] to save the change, or press [Esc] or [Enter] without typing anything else to keep the old value. In either case, you'll be returned to the Network Parameter Menu.

   Most of this menu's options are self-explanatory. As for the others: The "User Node ID" is a name up to 15 displayable characters long that you can give the Card; it will appear in the login prompt, as well as in the security-log records (see **Section 4.3.3**). The default value is a null string (no name). The default setting of "Ethernet Speed" is "Auto Negotiation"—the Card will negotiate the best available data rate with your hub or router. Some devices don't respond properly, though, so you might have to force the data rate to "10 Half" (10 Mbps, half-duplex), "10 Full" (10 Mbps, full duplex), "100 Half" (100 Mbps, half-duplex), or "100 Full" (100 Mbps, full duplex). Only disable DHCP if the Card's network parameters must be entered manually rather than derived automatically (see **Chapter 3**). The "Loghost IP Address" is the address of a remote host computer running a logging program such as syslog, to which the Card can transmit a mirror of the event records that normally appear in its Log Window (see **Section 4.3.3**). If you activate this feature, you'll be able to maintain a continuous record of Management Card activity without needing to transfer the security log as described in **Section 4.4.7**.

If you want to reset the Management Card, press "R". You will be asked to confirm this choice. Press "Y" followed by [Enter] to perform an immediate reset, or "N" followed by [Enter] to cancel it. If you go ahead with it, the Card beeps, becomes deselected, and resets itself. This will probably take at least 45 seconds; if you're accessing the Card through a telnet connection, it might take twice that long until the Card reinitializes its network presence. You can then reselect the Card; depending on whether security is enabled, you will then see either the User Options Menu or the login prompt.

4.6.4 CHANGING THE ADMIN PASSWORD

To set or change your admin password, take these steps:

CAUTION!

Be very careful when you do this, and keep a record of the password in a secure location. If the password is botched or forgotten, you'll have to call Black Box Technical Support and arrange to return the Card to the factory!

1. At the Administrator Menu, press "P".

2. You will be prompted for the current administrator password. If this password has previously been set, type in the current password followed by [Enter]. If you haven't yet set a password for this Management Card, simply press [Enter] without typing in anything else. (The factory-default admin password is a null string—that is, no password at all.)

3. You will then be prompted for the new password. Either type in a password up to eight displayable characters long followed by [Enter], or just press [Enter] without typing in anything else to turn off any existing password and disable the Management Card's password security.

4. If you enter a new password, you will be asked to enter it a second time for verification. Type it in again and press [Enter] to save it as the new password and return to the Administrator Menu.

   If you just press [Enter] to disable password security, you will be asked to confirm this disablement as shown below. Type "Y" [Enter] to confirm the change or "N" [Enter] to cancel it; either way, you'll be returned to the Administrator Menu. Note that even though the prompt says, "Disable User Password", it is in fact the admin password you are disabling.

```
Enter new administrator password:

Disable User Password? (y/n): y
```

5. To test any new password you've set, press "X" to return to the User Option Menu, then press "X" again to exit the menu system altogether. If the administrator password has been set correctly, a login prompt should now be displayed. Log in using the username "admin" and the new password.

4.6.5 SETTING SESSION PRIORITY

The Management Card can be accessed in either of two ways: either through a keyboard/video/mouse user station attached to a User Card with On-Screen Display, or through an Ethernet telnet session. However, only one of these session types can be active at any given time. To assign which type of session (if any) gets preferential treatment, you can assign a "session priority" scheme. There are three settings available:

• The "Mutual Exclusion" setting establishes normal "first come, first served" access: If a user on a User Card selects the Management Card first, any telnet user attempting to select the Management Card will be denied access; they'll receive a "KVM console in use" message instead. And if a telnet user is the first to select the Management Card, any User-Card users trying to switch to the Management Card's channel will remain on their previously selected channel and will receive the message "Unable to select channel. Reason: Channel in privacy mode."

• The "Console Session" setting gives User-Card users higher priority all the time, even if a telnet user is already connected to the Management Card. In this setting, if a User-Card user selects the Management Card, any existing telnet session will be closed and the telnet user will receive a "KVM console in use" message. After that, any telnet user that tries to connect to the Management Card during the User-Card user's session will receive the same message and will be denied access.

• The "Telnet Session" setting gives telnet users higher priority all the time, even if a User-Card user is already connected to the Management Card. In this setting, if a telnet user selects the Management Card, any existing User-Card session will be closed and that user's screen will go blank. They'll have to switch to another channel to resume operation. After that, any User-Card user that tries to switch to the Management Card's channel during the telnet user's session will receive a "Channel in privacy mode" message and will remain on their previously selected channel instead.

To set the session priority, take these steps:

1. At the Administrator menu, press "S" to bring up the Session Priority menu. The current session-priority setting will be shown above the menu.

2. Type the number corresponding to your desired setting, then press [Enter] to save the change or type "X" to cancel it. Either way, you'll be returned to the Administrator Menu.

```
  Current Session Priority: Mutual Exclusion

 Session Priority Menu
 ----------------------
   1. Mutual Exclusion
   2. Console Session
   3. Telnet Session
 ----------------------
  Enter Selection or X to exit:
```

4.6.6 ADMINISTERING USERS

To administer your users, press "U" at the Administrator Menu. The Terminal Control Panel User List (or just "User List" for short) will appear on your monitor.

```
        Terminal Control Panel
              User List
    -----------------------------
    Name                Password
--> Elizabeth           Enabled <--
    Gil                 Enabled
    John                Enabled



    Search:
    -------------------------------
    Ctrl-S: Setup access  Ctrl-E: Edit
    Ctrl-A: Add user      Ctrl-D: Delete user
    Ctrl-T: Go to Top     Ctrl-B: Go to Bottom
    Ctrl-X: eXit user list
```

The User List will display all users that you've added to the Management Card's database. From here, you can add, edit, or delete user configurations. Use your keyboard's up- and down-arrow keys to highlight a specific user, or press [Ctrl] along with "T" or "B" to take you to the top or bottom of the list respectively. To quickly locate an particular user, start typing in their name at the "Search" prompt; the Card will scroll down the list to the first username that matches the characters you've typed in so far. When the user you want is highlighted, press [Enter] to select their account.

   The rest of this section describes the other available User-List functions. When you've finished working with the User List, press [Ctrl] along with "X" to return to the Administrator Menu.

4.6.6.A Setting User Access

To set a user's access rights to the devices in your system, highlight that user in the User List and press [Ctrl] along with "S". The Access Setup screen will appear on your monitor.

```
        Terminal Control Panel
     Access Setup: John
     ----------------------------
     Name                Access
 --> mail_server           Yes       <--
     ModemPool             No
     web_server            No
     router_1              No



     Search:
     ------------------------------
     Ctrl-L: toggLe access Ctrl-S: Set all
     Ctrl-T: Go to Top     Ctrl-B: Go to Bottom
     Ctrl-X: eXit user list
```

If you want to change a user's access rights to a particular device, use your keyboard's up- and down-arrow keys or the search function to highlight the device, then press [Ctrl] along with "L" to toggle whether the user can access that device. If you want to enable or disable a user's access to all devices at once, highlight a device with the desired access setting ("Yes" for enabled or "No" for disabled), then press [Ctrl] along with "S" to set the user's access rights to all devices in the list to match. To move the display to the top of the device list, press [Ctrl] along with "T"; to move it to the bottom of the list, press [Ctrl] along with "B".

Unlike the Management Card's other menus, you'll press [Ctrl] along with "X" to save your changes and return to the User List. Press [Esc] (the escape key) to return to the User List without saving your changes.

4.6.6.B Adding Users
To add a user to the Management Card's database, take these steps:

1. At the User List, press [Ctrl] along with "A".

2. You will be prompted to enter a name up to fourteen displayable characters long for the user. (The names "admin", "administrator", and "root" are reserved and may not be assigned to non-admin users.) Type in the name and press [Enter].

3. You'll then be prompted to enter a password up to eight displayable characters long for that user. Type in the password and press [Enter] to save the new user account with the selected password. You'll be returned to the User List.

    If you're not using password security, or if this user just doesn't need a password, press [Enter] at the prompt without typing in anything else. You'll be asked whether you really want to disable the password. Press "Y" followed by [Enter] to save the new user account without a password and return to the User List, or press "N" followed by [Enter] to cancel the change and return to the user list. Any new account will be displayed in the User List right away.

    ```
    Add a User

    Enter user name: Kelly
    Enter user password:
    ```

4.6.6.C Editing Users
To edit a user in the Management Card's database, take these steps:

1. At the User List, use the keyboard's arrow keys and/or the search function to highlight the user you want to edit.

2. Press [Ctrl] along with "E".

3. Type in a new username up to fourteen displayable characters long for this user and press [Enter], or press [Enter] without typing in anything else to keep the existing username.

4. Type in a new password up to eight displayable characters long for this user and press [Enter] to save the changes and return to the User List.
   To turn off the password so that the user doesn't have to log in, press [Enter] without typing anything else. You'll be asked whether you really want to disable the password. Press "Y" followed by [Enter] to save the edited user account without a password, or press "N" followed by [Enter] to cancel the change. In either case, you'll be returned to the User List; any changes you make will be reflected there. You can also press [Esc] at any time to return to the User List without changing anything.

```
        Edit User

        John            Password enabled

    Enter new name [John]:

    Enter user password: newpass
```

4.6.6.D Deleting Users

To delete a user from the Management Card's database, take these steps:

1. At the User List, use the keyboard's arrow keys and/or the search function to highlight the user you want to delete.

2. Press [Ctrl] along with "D".

3. The username will be displayed followed by a "Delete this user?" prompt, as shown below. Press "Y" followed by [Enter] to delete the selected user account, or press "N" followed by [Enter] to keep the account. In either case, you'll be returned to the User List; any deletion will be reflected in the list.

```
Elizabeth

Delete this user? (y/n):
```

5. Troubleshooting

5.1 Calling Black Box

If you determine that your Management Card or Serial Control Card is malfunctioning, *do not attempt to alter or repair it*. Its components are not user-serviceable. Contact Black Box Technical Support at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem;

- when the problem occurs;

- the components involved in the problem—that is, what types of computers, what type of keyboard, brand of mouse, make and model of monitor, etc.;

- any particular application that, when used, appears to create the problem or make it worse; and

- the results of any testing you've already done.

Filling out a copy of the Problem Report in **Appendix B** in your ServSwitch Multi manual should provide most of the information we need to get started.

5.2 Shipping and Packaging

If you need to transport or ship your Management Card or Serial Control Card or your ServSwitch Multi:

- Package it carefully. We recommend that you use the original container.

- Before you ship the unit back to Black Box for repair or return, contact us to get a Return Authorization (RA) number.

BLACK BOX®
NETWORK SERVICES

Customer Support Information:
FREE tech support 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**.
Mailing address: **Black Box Corporation**, 1000 Park Dr., Lawrence, PA 15055-1018
World-Wide Web: **www.blackbox.com** • E-mail: **info@blackbox.com**

Doc. No. 590-188-001 Rev. A