KVM CONTROL OVER IP

KVM Switch and Control Over IP Module

SV431DI
SV831DI
SV1631DI

Instruction Guide

* Actual product may vary from photo

StarTech.com

The Professionals' Source For Hard-to-Find Computer Parts

Table of Contents

NOTE: Due to firmware upgrades, the information in this Instruction Guide may not be identical to what you see on your screen. Check www.startech.com for firmware upgrades or contact us if you encounter any difficulties. (June 23, 2004)

Introduction

Thank you for purchasing a StarTech.com KVM switch with remote IP access. Perfect for mission-critical server rooms or datacenters, the SV431DI, SV831DI and SV1631DI are all-in-one solutions for effective and efficient network management. The rock-solid, reliable KVM switch allows you to monitor and control multiple servers from one location. And thanks to KVM Control over IP, that location can be anywhere in the world. You will soon be able to view, control, and even reboot your servers from any location connected to the Internet. The innovative ultra-thin 3-in-1 KVM cables make installation easy while keeping your server room free of cable clutter.

With a range of security and expandability features to suit your network, the SV431DI, SV831DI and SV1631DI are the complete professional solution for network/server administrators.

Features

KVM Switch (SV431D, SV831D, SV1631D)

- Hot-pluggable to allow computers to be added or removed without worrying about having to reboot the other connected systems.
- "Keep-alive" feature draws power from PC keyboard ports if power is lost. Switch will continue to operate during power outage even if it loses power, retaining mouse control.
- Rugged, all-metal chassis for use in harsh environments and space-saving cabinets.
- Designed for guaranteed compatibility with Dell, Compaq, IBM and HP servers and systems.
- Compatible with all notebook computers.
- Compatible with Compaq Alpha systems.
- Fast switch-buttons for each port provide quick access to any connected system.
- High 1920x1440 resolution capability supports the most demanding applications.
- On-Screen Display (OSD) feature on some models allows PC selection from an On-Screen menu of user-defined computer names. Built-in OSD security keeps unwanted users out.
- A front panel pushbutton and status lights for each port make PC selection and switch status monitoring fast and easy.
- Can be cascaded to control up to 16 (SV431DI), 64 (SV831DI) or 136 (SV1631DI) PCs.
- Each PC name is user-definable via the OSD menu.
- Intelligent scan mode automatically switches through user-defined computers, scan rate is user selectable via OSD menu.
- Completely operating system independent. No software or drivers required.

KVM Control Over IP (SV1110IPEXT)

- Users can re-boot the hardware, access the BIOS, have full keyboard and mouse control - as if they are on location.
- Web-Based control allows the server(s) to be controlled from any browser, eliminating licensing costs and making the product easier to use.
- Advanced video detection algorithms provide excellent remote video quality and industry-leading performance.
- 128-Bit SSL encryption provides a secure remote connection.
- Flash upgrade capability.
- Extremely compact size – one of the smallest IP based KVMs on the market.

Before You Begin

To ensure a quick and easy console installation, please read through this section carefully before attempting to install the device.

Contents

This package should contain:

- 1 x SV1110IPEXT KVM Control Over IP
- 1 x StarView KVM Switch (SV431D, SV831D or SV1631D)
- 1 x 2 ft 3-in-1 cable
- 2 x AC power adapter (1 for KVM Control Over IP, 1 for KVM Switch)
- 1 x 3-prong power cord (for KVM Control Over IP)
- Rubber feet
- User manual

- **SV431DI:**
  2 x PS23N1THIN2 (2 foot KVM cable)
  2 x PS23N1THIN4 (4 foot KVM cable)
  2 x PS23N1THIN6 (6 foot KVM cable)

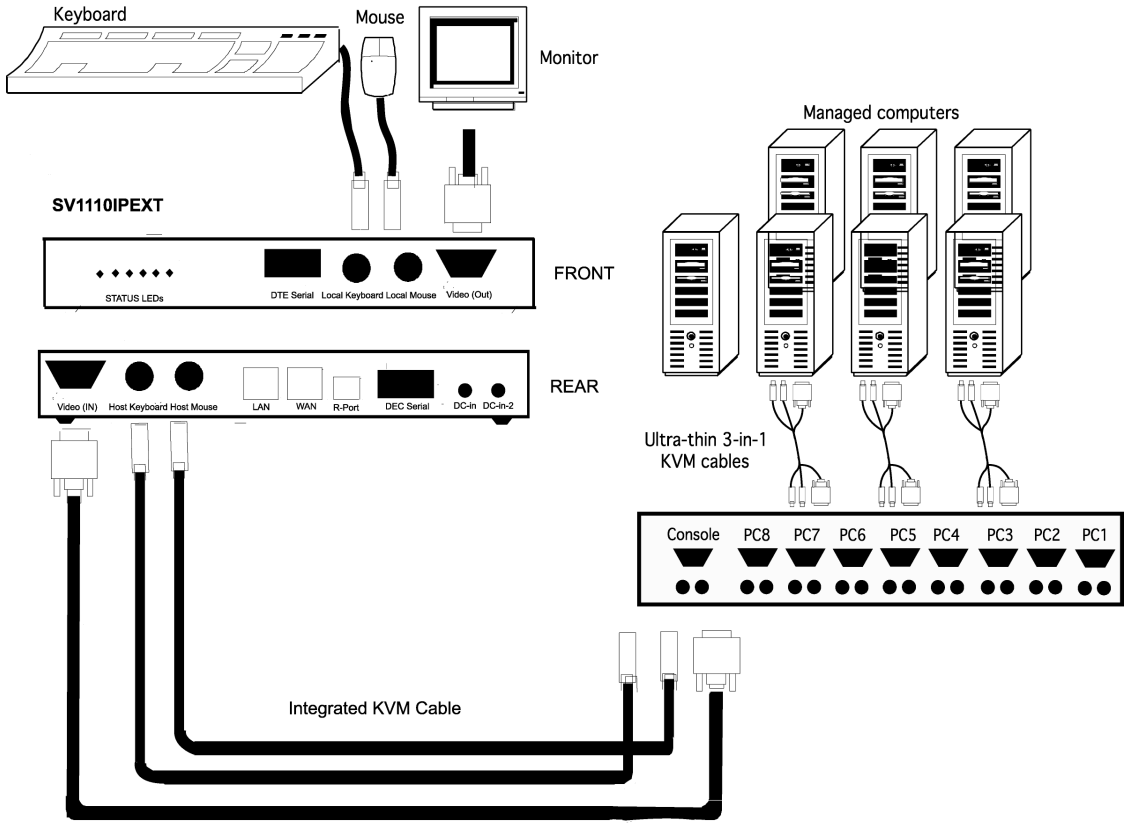
- **SV831DI:**
  2 x PS23N1THIN2 (2 foot KVM cable)
  2 x PS23N1THIN4 (4 foot KVM cable)
  3 x PS23N1THIN6 (6 foot KVM cable)
  3 x PS23N1THIN10 (10 foot KVM cable)

- **SV1631DI:**
  4 x PS23N1THIN2 (2 foot KVM cable)
  4 x PS23N1THIN4 (4 foot KVM cable)
  6 x PS23N1THIN6 (6 foot KVM cable)
  6 x PS23N1THIN10 (10 foot KVM cable)

NOTE: Throughout this manual “managed host” or “host computer” refers to the computer connected to the KVM Control Over IP. “Remote client” or “client computer” refers to the PCs connected to the KVMs that are used to access the host computer.

Installation

This section will guide you through the hardware installation of your SV831DI or SV1631DI. Please read through this section carefully and complete each step in the order listed.



1. Make sure all computers and devices are powered off.

2. Attach each of your managed computers to your StarView KVM switch using the ultra-thin 3-in-1 KVM cables. Use the 3-in-1 cables to connect one of the PC ports on the back of the switch to the computer's keyboard, mouse, and video ports. For information on cascading your KVM, see “Cascade Configuration.”

3. Attach your KVM switch to the SV1110IPEXT with the integrated KVM cable. Plug the male video connector (blue) into the **Console** monitor port on the KVM switch and plug the female end of the video cable (blue) into the **Video (In)** port on the back of the SV1110IPEXT. Plug the keyboard (purple) and mouse (green) connectors into the KVM switch's **Console** keyboard and mouse ports and plug the PS/2 connectors on the opposite end to the **Host Keyboard** and **Host Mouse** ports on the rear panel of the SV1110IPEXT.

4. Plug a keyboard and mouse into the **Local Keyboard** and **Local Mouse** ports on the front of the SV1110IPEXT.

5. Attach your monitor by connecting the monitor video cable to the **Video (Out)** port on the front of the SV1110IPEXT.

6. Using standard Ethernet patch cables, connect the **LAN** and/or **WAN** ports on the back of the SV1110IPEXT to your network (usually a router, hub/switch, or wall outlet).

   NOTE: The **LAN** and **WAN** ports are factory-configured with different settings that can affect the configuration method you wish to use with the SV1110IPEXT. See “Configuration Methods Explained” on page 8 for more details.

7. Power on your KVM Control Over IP Console, your KVM Switch, and your computers.

IMPORTANT: If you connected the optional **WAN** connector on the SV1110IPEXT to your network, you **must** also connect the optional second AC/DC adapter to the unit. This provides a load-balancing feature between the two power sources and allows the unit to function if one adapter fails.

NOTE: If you are using cables other than those provided in the package or branded by StarTech.com, ensure that the cables are of high quality and use the minimum possible distance necessary. Low quality or excessively long (particularly video) cables between the host computer and the SV1110IPEXT could degrade performance.

IMPORTANT: The SV1110IPEXT is convection-cooled. Ensure the vents on both sides are unobstructed.

USING YOUR KVM CONTROL OVER IP

SV1110IPEXT

Required Cables and Hardware

All applications

- 1 x Straight-through Ethernet patch cable (to connect the unit to your LAN)
  StarTech.com part number: M45PATCHxxxx

To use the optional dedicated WAN port

- An additional straight-through Ethernet patch cable to connect the unit directly to a dedicated WAN/Internet connection
  StarTech.com part number: M45PATCHxxxx
- Second power adapter
  StarTech.com part number: EUPACABCONS

Configuration via serial port

- 1 x Straight-through RS-232 serial cable with 9-pin DB9 male/female connectors
  StarTech.com part number: MXT100

To install the SV1110IPEXT into a rack or cabinet

- 1 x Rack kit (supports up to two units)
  StarTech.com part number: 1110EXTRACK

1110EXTRACK

Disabling Mouse Acceleration on the Host Computer

Many operating systems offer a feature called mouse acceleration that allows the user to adjust the responsiveness of the cursor on the screen to physical movements of the mouse. While this is usually a beneficial interface enhancement, it can interfere with the operation of the SV1100IPEXT and should be disabled on the host computer before a remote session is attempted. Follow the instructions below to disable mouse acceleration for the operating system installed on the host computer.

Windows 98

1. From the Control Panel, click on **Mouse**.
2. From **Mouse Properties**, click on **Motion** tab.
3. Make sure the Pointer speed bar is centered and **Acceleration** is set to **None**.

Windows 2000

1. From the Control Panel, Click on **Mouse**.
2. From **Mouse Properties**, click on **Motion** tab.
3. Make sure that the Pointer speed bar is centered and **Acceleration** is set to **None**.

Windows XP and Windows Server 2003

1. Go to **Pointer Options** and turn off **Enhance Pointer Precision**.
2. Make sure that the Pointer speed bar is centered.

Linux, Unix and X-Windows

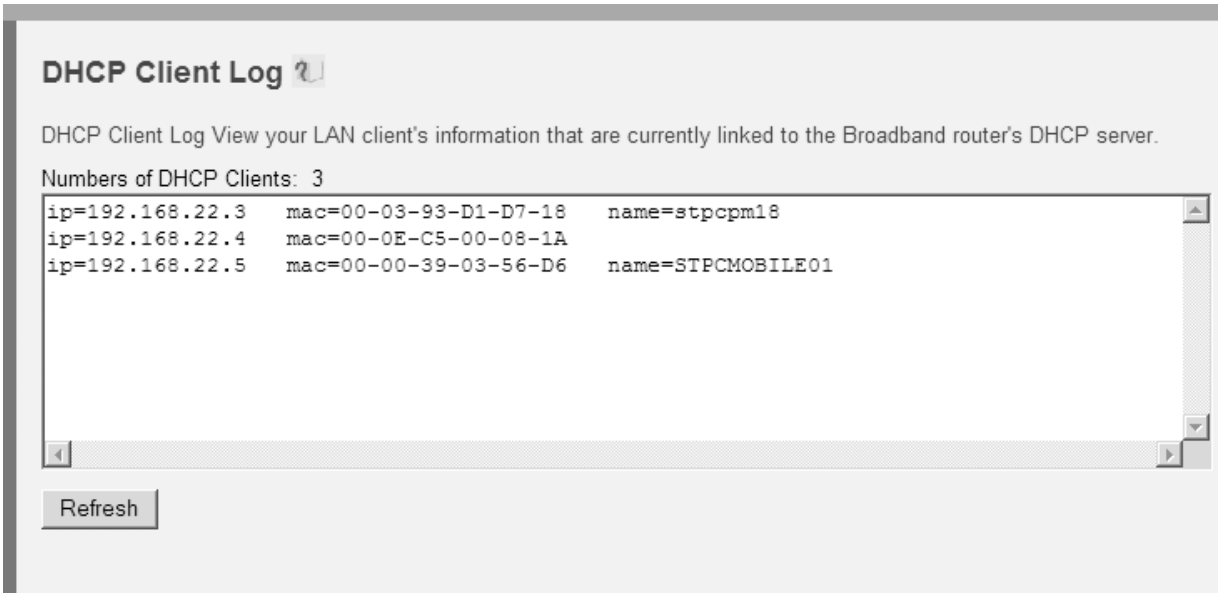
1. Add this command to your xinitrc, xsession or other startup script:
   xset m 0/0 0

Configuration Methods Explained

The SV1110IPEXT offers three distinct methods for configuring the unit for your network. The method that will work best for you will depend on your level of experience and your specific network configuration.

Accessing Web Configuration Using DHCP

This method requires that your network implement DHCP (Dynamic Host Configuration Protocol), usually on a server or network access device such as a router that dynamically allows devices to join the network without pre-configuration. It also assumes that you will have easy access to your network's DHCP log, since you will need to know the IP address of the unit to complete the configuration over your Web browser. (If you are unsure of how to access your network's DHCP log, contact your System Administrator for details.) If the unit is powered on and connected to the network via the **LAN** port on the rear panel, it will automatically attempt to lease an IP address using DHCP. Before you can begin the configuration process, you will need to access the DHCP log from your file server or other device that acts as the DHCP server on the network. A simple DHCP log looks similar to the following:



The information displayed for your own network may vary significantly from the data displayed in the above image, but should supply (at minimum) three essential details: IP address, MAC address, and device (or machine) name for the computers and other devices connected to your network. The values for the SV1110IPEXT tested above are as follows:

IP Address: 192.168.22.4
MAC Address: 00-0E-C5-00-08-1A
Device Name: (none)

The easiest way to identify your SV1110IPEXT on the network is by its MAC address, a unique hardware identifier that is specific to your unit. The MAC address of the unit can be found on a white sticker on the bottom of the SV1110IPEXT. **Write down this number and keep it for future reference.** Once you locate the MAC address of your unit in the DHCP log, you can match it to its leased IP address and proceed with the Web configuration.

NOTE: Once you have located the IP address of the SV1110IPEXT and wish to proceed with the Web configuration, do not power off the unit or your DHCP server, since the KVM might lease a different IP address. Should this happen, re-examine the DHCP log to verify the IP address again.

NOTE: DCHP functionality is not affected if you also connected the **WAN** port on the SV1100IPEXT to your network (see below).

Accessing Web Configuration Using Static IP

Since some networks rely on static IP addresses (every device has a pre-configured IP address that does not change), the DHCP access method described above is not applicable in those situations. To accommodate this type of installation, the **WAN** port on the rear panel of the SV1110IPEXT is factory-configured with its own IP address.

NOTE: If you connected the **LAN** port on the rear panel of the unit to your network but did not connect the **WAN** port, you must disconnect the Ethernet cable from the **LAN** port and move it to the **WAN** port before attempting a static IP installation. (If desired, you can return the cable to the **LAN** port if you configure it with a static IP address during the configuration process.) If you have connected *both* the **LAN** and **WAN** ports on the KVM to your network, you may proceed with a static IP Web configuration.

The following are the default values for the **WAN** port, configured at the factory:

IP Address: 192.168.1.123
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254
Broadcast: 192.168.1.255

To access the Web configuration for this product, you will need to configure the workstation you are using to the same subnet (255.255.255.0) and also assign it a valid IP address. For details on how to change the IP address of your computer (if necessary), consult your documentation or System Administrator for assistance.

NOTE: It is advisable to verify whether another device on your network is using the same IP address as the SV1110IPEXT *before* connecting it to the network to avoid a conflict. Should an IP address conflict occur with another device on the network, power off the conflicting device or assign it another IP address before continuing the installation.

NOTE: Not all IP addresses are valid for a given subnet. If you are required to change your subnet (and therefore IP address) to configure the unit, be sure the IP address you choose is within the allowable range for the 255.255.255.0 subnet.

Once your computer is configured to the same subnet as the SV1110IPEXT, you can use the IP address **192.168.1.123** to access the Web configuration system.

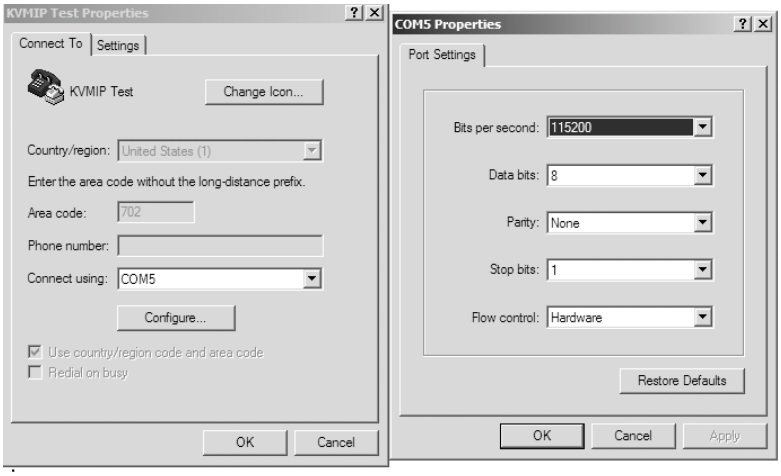
Accessing Terminal Configuration Using a Serial Cable

Configuring the SV1110IPEXT using a serial cable is the best choice if you need to pre-configure the unit before attaching it to a network, i.e. when sending to a branch office, customer site, etc. In general, the Web configuration is far preferable because of its intuitive interface and the fact that you do not have to be within close physical proximity to do the configuration. However, if you wish to use the serial cable method to configure the SV1110IPEXT, you can use any typical communication software package (**UNIX:** tip, cu, kermit, minicom; **Windows:** HyperTerminal, kermit).

Using a DB9 male-to-female (straight-through, not null-modem) connect the end of the cable with the **male** connector to the **DCE Serial** port on the rear panel of the SV1110IPEXT. Connect the end with the **female**

connector to the serial port on the computer you are using to configure the unit. Configure the terminal software with "8N1" settings:

Connection speed: 115200 bps
No. of bits: 8
Parity: None
Stop bits: 1



A sample HyperTerminal configuration

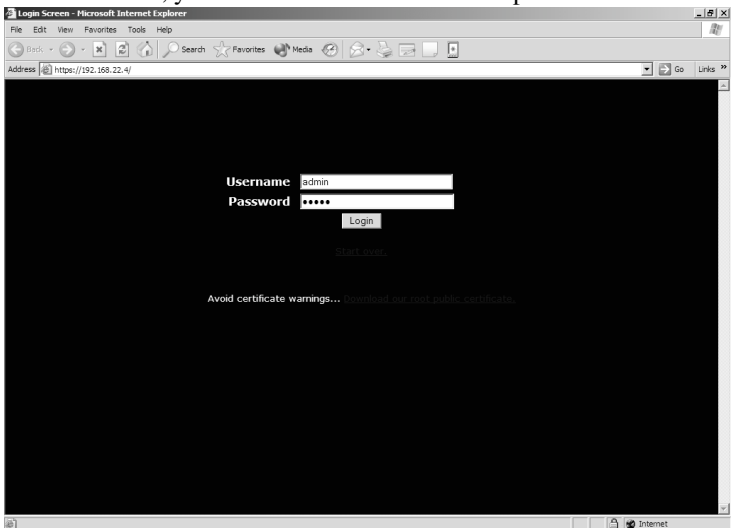
Configuring the SV1110IPEXT

Using the Web Interface

The Web interface is the most intuitive way to configure the SV1110IPEXT. It also offers a Java-based VNC client that you can use to control the host computer from a remote location. The SV1110IPEXT supports any industry-standard HTML Web browser. You can access the Web interface by opening your Web browser and entering the IP address of the SV1110IPEXT you wish to access/configure. The IP address will be either a) the address assigned by your DHCP server as identified in the previous section, or b) 192.168.1.123 if your network uses static IP addressing.

The Login Screen

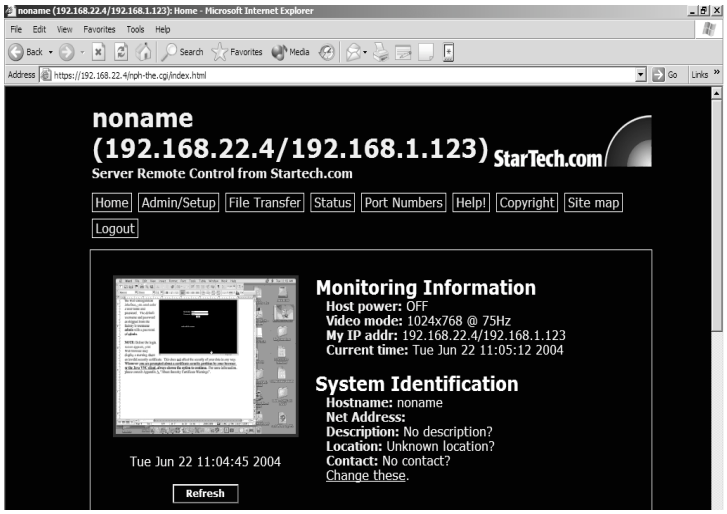
Before you can access the Web configuration interface, you must enter a user name and password. The default username and password as shipped from the factory is username **admin** with a password of **admin**.



NOTE: Before the login screen appears, your Web browser may display a warning about an invalid security certificate. This does not affect the security of your data in any way. **Whenever you are prompted about a certificate security problem by your browser or the Java VNC client, always choose the option to continue.** For more information, please consult Appendix A, "About Security Certificate Warnings".

The Home Screen

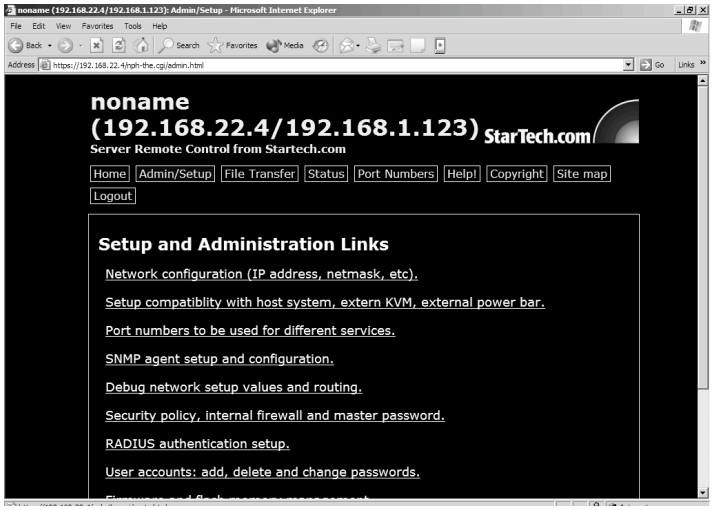
The Home screen serves two functions. First, it is a place to check the status of the SV1110IPEXT, view essential system information, and capture screen shots from the host computer. Second, it is where you can start the integrated Java VNC client to interact with the host computer by clicking on the large screen shot or choosing one of the VNC client links.



The Admin/Setup Screen

This is the menu that will allow you to access all the features you will need to perform an initial configuration of the SV1110IPEXT. Each of the options is explained in detail here.

Network Configuration (IP address. Netmask, etc).



Dynamic Host Configuration Protocol (DHCP)

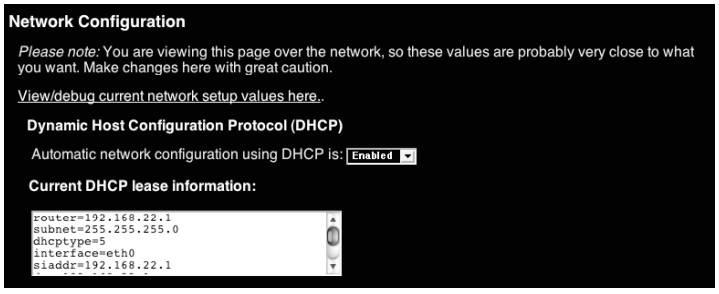
Automatic network configuration using DHCP is: **Enabled/Disabled.** This feature applies only to the **LAN** port on the rear panel, and is enabled by default. When enabled, the unit will automatically configure itself with an IP address when a DHCP server is present. When disabled, the **LAN** port will use the values assigned to it on the **IP Addresses and Routing** table below.

Current DHCP Lease Information

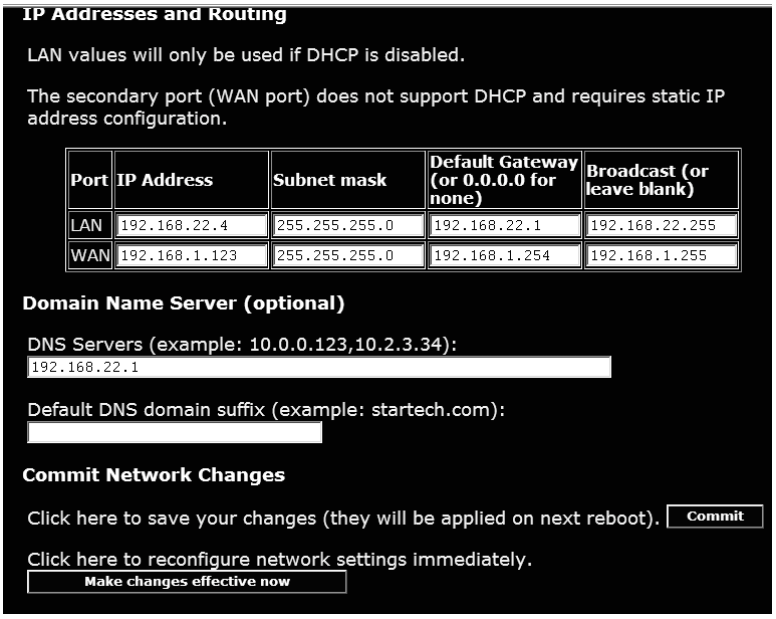
This box provides detailed information about the IP lease that the unit has obtained from the DHCP server.

IP Addresses and Routing

This table allows you to assign IP information for the **LAN** and **WAN** ports separately. If you are using DHCP, the values for the **LAN** port will be filled in automatically and any changes made will not affect the setup. If **Ethernet Bridging** is enabled (see below) the **WAN** port



will use the same settings as the **LAN** port, and any changes will not affect the setup for that port. Adjusting the setting for the **WAN** port allows you greater control over how the SV1110IPEXT is configured for access from outside the local network, particularly if a firewall or proxy is in use.



Domain Name Server (optional)

This section allows you to specify DNS servers and the default DNS domain suffix in use on the network. If DHCP is enabled, some of these values may be supplied automatically.

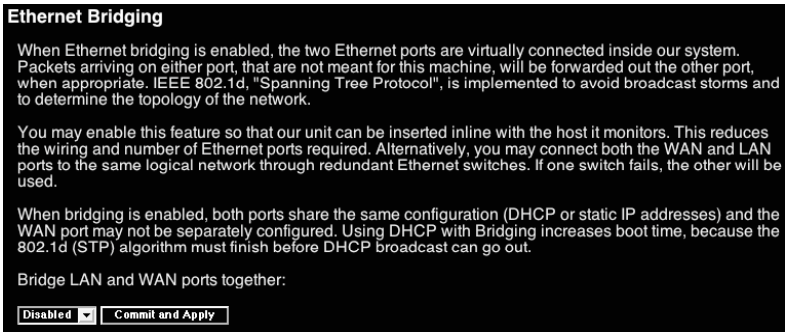
Commit Network Changes

Clicking the **Commit** button applies any changes made on the page to the configuration, but leaves the old settings active until the next time the unit restarts. Clicking **Make changes effective now** applies the changes and restarts the SV1110IPEXT so the new settings take effect immediately.

Ethernet Bridging

When Ethernet bridging is enabled, the two Ethernet ports are virtually connected inside the SV1110IPEXT. Packets arriving on either port that are not meant for it will be forwarded out to the other port, when appropriate. IEEE-802.1d ("Spanning Tree Protocol") is implemented to avoid broadcast storms and to determine the topology of the network.

You may enable this feature so that the module can be inserted inline with the host it monitors. This reduces the wiring and number of Ethernet ports required. Alternatively, you may connect both the WAN and LAN ports to the same logical network through redundant Ethernet switches. If one switch fails, the other will be used. When bridging is enabled, both ports share the same configuration (DHCP or static IP addresses) and the WAN port may not be separately configured. Using DHCP with Bridging increases boot time, because the 802.1d (STP) algorithm must finish before the DHCP broadcast can go out. To change this setting, select either **Enabled** or **Disabled** from the drop-down menu and click **Commit and Apply.**



Setup compatibility with host system, external KVM, external power bar.

This menu offers features that may offer enhanced functionality with certain KVM and power products. These can be left at their default values in many situations.

Port numbers to be used for different services.

Takes you to the **Ports** menu (see below).

SNMP agent setup and configuration.

This menu allows you to configure the SV1110IPEXT so it can be recognized and managed using industry-standard Simple Network Management Protocol software.

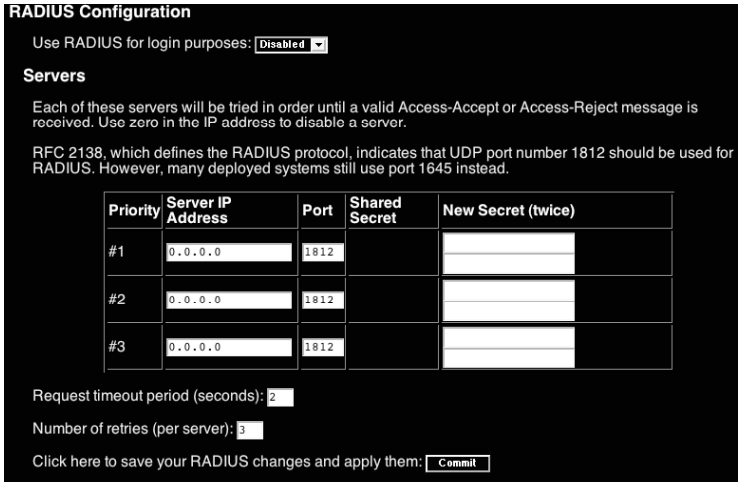
Debug network setup values and routing.

Takes you to the **Status** menu (see below).

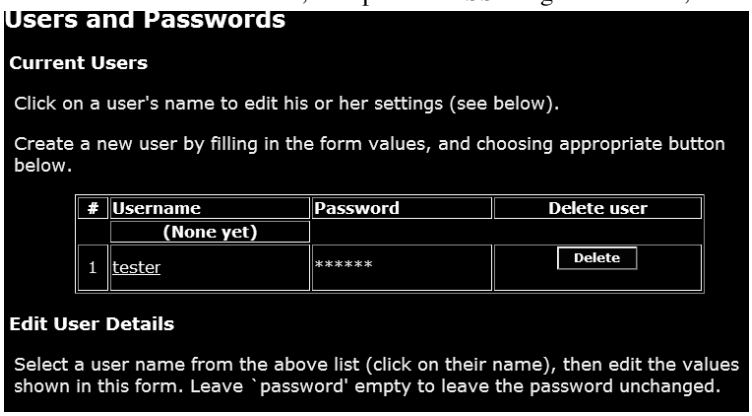
Security policy, internal firewall and master password.

This menu allows you to configure a number of settings, including changing the default password for **admin** (recommended). Read and consider the comments and instructions on this menu before making any changes, as changing these features could make the unit inaccessible through Web configuration (i.e. due to firewall filtering). Note that any password changes you make will have to be entered in duplicate to reduce the chance of error.

RADIUS authentication setup.



The RADIUS server requires the IP address, the UDP port number (1812 - *default* or 1645) and the shared secret. The shared secret is used to encrypt communications and corresponds to a shared password for the RADIUS server and the client machine. Two additional servers may be defined for backup purposes. Each server will be tried in order, using the indicated number of retries and timeout period, which are configurable on the same page. *Remember to enable RADIUS after configuring it*. While RADIUS authentication is enabled, the locally defined accounts on the KVM control over IP module will not be used, except for the SSH login. However, if a user name of the form "name.local" is given at the RADIUS prompt, the system will use "name"; check the password locally, and skip RADIUS authentication. Delete all local accounts to avoid this behavior. When connecting via VNC, a login screen is generated that asks for a RADIUS username and password.



User accounts: add, delete and change passwords.

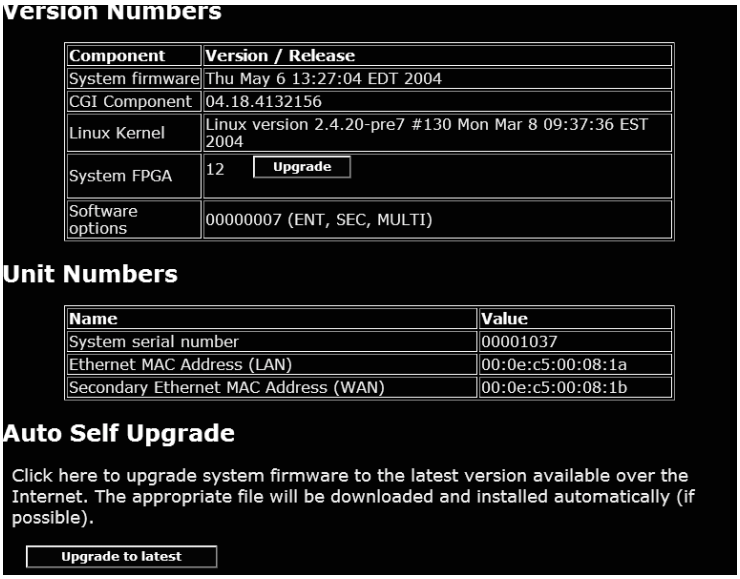
This menu will allow you to add accounts other than **admin** to the system. These accounts will not have the authority to change settings, but can access the Web interface and log in the VNC console. Selecting **Delete** permanently removes the user from the system. If you enter values for a user that does not already exist under **Edit User Details**, the system will create that user for you when you click **Record changes**. If the user already exists, you will change the password for that user.

Firmware and flash memory management.

The firmware on the KVM control over IP is field upgradeable. To upgrade to another version, login as **admin**.

Auto Self Upgrade

The KVM control over IP module includes an innovative feature allowing the unit to upgrade itself over the Internet. Simply click on the button labeled Upgrade to Latest and the module will go out to the Internet and download the latest version of the system firmware and then install it. If the module cannot access the Internet directly (perhaps due to a web proxy or other firewalls), then a page will be shown that causes your browser to download the required file. Save this file to disk and then upload it as described in the next section, Manual Upload. The main FPGA is upgraded separately, and has its own Get latest button. This file is unique for each unit, so it must be done in this manner.



If you have multiple units to upgrade, you may choose the Get latest version button that will not attempt to upgrade the unit directly, but will instead fetch the required file. This file can be uploaded to multiple units manually.

Manual Upload

Enter the name of the firmware file that you received from StarTech.com into the field provided (or use the Browse... button). Press Start Upload and wait until a successful upload message is shown.

NOTE: Remember the following during the firmware upgrade…

- Do NOT turn off power to unit before this operation completes successfully. It may take several minutes to write to flash memory.
- The unit will sometimes reboot as part of the upgrade procedure, depending on which system component is upgraded. You will have to reconnect and re-login in those cases.
- Wait at least two minutes after pressing Start. Do not assume the upload did not work. There is no status indicator bar to show the progress of the upload. The upload could simply be slow.
- Each file that is distributed upgrades a different component of the system. Therefore, be sure to apply all files you are given as part of an upgrade. The system knows what to do with each file you give it, and they are checked for validity before being applied.

Software Options Upgrade

Certain firmware features may be offered separately from the base unit, in order to reduce the initial cost for the KVM control over IP module.
NOTE: If you wish to upgrade after the system is in operation, go to the Manage Firmware page and scroll down to the section entitled Purchase Options.
Look for a unique code, like the following one:

4-C80C-B960-1-0

If you provide this code to the technical support department, they can give you an unlock code that will open any feature you request. Types in the code provided, exactly, into the area provided and click "Submit". The new features opened by the code will be enabled immediately, but you may need to reboot the unit to begin using certain features.

Set date and time.

Allows you to set the unit to local or Universal Coordinated Time (GMT).

Change system identification.

Provides details about this SV1110IPEXT that will be available to DHCP servers, SNMP agents, and VNC clients. While these values do not affect the operation of the unit, they make it easier to manage on the network.

The File Transfer Screen

The SV1110IPEXT is able to emulate a disk driver attached to the host via USB. Depending on configuration, it will appear to the host as a floppy drive (1.44MB), an 8MB RAM disk or a CD-ROM. The host computer does not require any special drivers or other configuration. It just looks like a new USB drive. You can transfer files onto the virtual disk while it is "ejected" and then "insert" the disk so the host can see the files. Any files the host writes to the disk can be retrieved once the disk is "ejected".
Access to the files is performed through the web interface. The disk may be inserted from either the web interface, or the Disk Control menu available via VNC. Most operating systems can "Eject" the disk once it is inserted, but it can also be ejected from the Web or VNC.

When emulating a floppy disk or RAM disk, the data is stored in RAM on the SV1110IPEXT itself. In order to emulate a CD-ROM disk drive, a web server is required to provide the CD-ROM image data. The web server must be accessible to the module, which communicates with it constantly as data is needed.

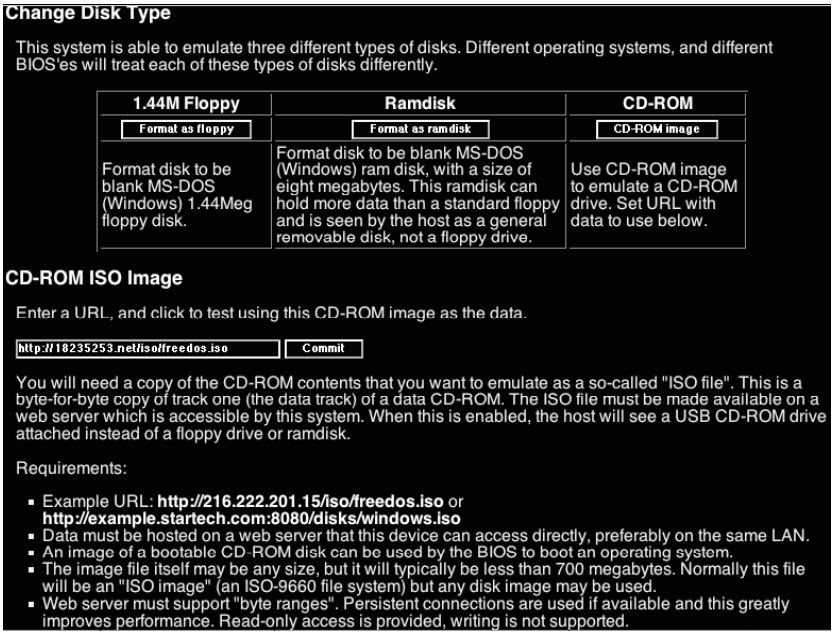
Floppy mode

Choose the **Format as floppy** button to switch to floppy mode. Under Windows, the drive will be identified as a "high density floppy" and will typically be assigned a drive letter of "B:". The capacity is limited to 1.44 megabytes in this mode. The purpose of supporting floppy mode is to permit the use of floppy-disk images generated by other systems. For example, the flash BIOS upgrade process is performed

with a special floppy and is bootable. You can transfer bits from that floppy to the SV1110IPEXT (use the upload disk image form). Now, you can boot from the special floppy. In addition, emergency repair disks are often restricted to floppies.

RAM disk mode

Choose the **Format as ramdisk** button to switch to RAM disk mode. This mode is intended to facilitate simple data transfer between the remote user and the host computer. It will be recognized by Windows as an eight megabyte removable disk and assigned a drive letter. You can easily drag and drop files up to 8MB in size to this device. In Windows explorer, you can choose the "Eject" option to make the data available to the remote users.



Reading files from disk

On the **File Transfer** menu, make sure the disk is "ejected," then choose the **Browse files** link. A web page will be generated that shows the root directory on the disk. You can download files to your browser by clicking on the file name. It is also possible to delete files and create directories using the buttons provided on that page.

Disk Formats

When you choose the **Format as...** button, the disk image stored in RAM is formatted to be an empty MS-DOS disk, with a single file called "Put files here...TXT". The SV1110IPEXT is able to read most MS-DOS/Windows formatted disks and presents the files via the web interface. However, disk emulation occurs at the lowest level so that other disk formats can be used, if you have the tools needed to create and read the disk images. At the bottom of the page are the upload and download options for the entire disk image. Any image that is exactly 1,474,560 bytes long will be treated as a floppy. Images of other sizes are supported up to 8MB.

CD-ROM Mode

The SV1110IPEXT does not store any data in this mode. Instead, it emulates a USB CD-ROM drive with a disk inserted. The data from that disk must be provided by an external web server. You will need a copy of the CD-ROM contents that you want to emulate as an ISO file. This is a byte-for-byte copy of track one (the data track) of a data CD-ROM. The ISO file must be made available on a web server which is accessible by the SV1110IPEXT. To switch to this mode, type in a URL pointing to the ISO image, and click on **Commit**. The system will connect to the web server and test the file for access. If successful, you will be shown a short report on the file contents, and the disk will be ready to use. Currently there is no other way to preview or browse the contents of the CD-ROM image, except from the host.

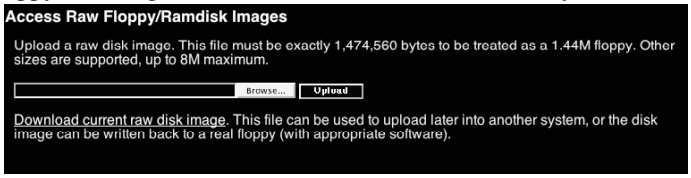
CD-ROM Web Server Requirements:

- Data must be hosted on a web server that the SV1110IPEXT can access directly, preferably on the same LAN.
- An image of a bootable CD-ROM disk can be used by the BIOS to boot an operating system.
- The image file itself may be any size, but it will typically be less than 700 megabytes. Normally this file will be an ISO image (an ISO-9660 file system) but any disk image may be used.
- Web server must support "byte ranges". Persistent connections are used, if available, as this greatly improves performance. Read-only access is provided; writing is not supported.

Booting from USB Disk

If the host machine's BIOS supports USB boot devices, it is possible to boot from the emulated CD-ROM or floppy. This allows complete operating system replacement without touching the computer.

The first step is getting a bootable disk image onto the emulated floppy or CD-ROM. For CD-ROM images, you will need an ISO image from a disk that contains special bits to enable boot ("El Torito" standard). Nothing special is needed when reading the ISO from a working, bootable CD-ROM. To create a bootable floppy, you can format the emulated floppy from the target system, or read the data from a working boot floppy. This can be done from Windows using "Disk Copy" (right click on the drive letter in the Windows Explorer) or by using a program like "RAWRITE".
Once you have a bootable image (CD-ROM or floppy) working on the KVM control over IP module, you must adjust your BIOS settings to tell it to boot from a USB device.
NOTE: You must select "USB CD-ROM" as the boot device for the BIOS, if using a CD-ROM image and "USB Floppy" if using a floppy image.



BIOS and OS Vendor Support

NOTE: Up-to-date information about OS and BIOS support is listed in the on-line help page of the internal web server.

Windows 95 or earlier: No USB support.
Windows 98: Keyboard and mouse are supported. Floppy/CD-ROM disk emulation is not supported.
Windows 2000 SP3+: Keyboard and mouse are supported. A bug in versions before Sevice Pack 2 prevents floppy/CD-ROM support from working correctly. (In particular, it appears to work, until you attempt to transfer files bigger than 4096 bytes). Upgrade to SP3 or later for full disk emulation support.
Windows XP, Windows Server 2003: Keyboard, mouse and disk emulation are supported.
FreeBSD 4.5: Keyboard, CD-ROM tested and working; other features untested.
AMIBIOS (from American Megatends Inc): Keyboard, floppy and CD-ROM emulation work well. It is possible to boot from virtual CD-ROM or Floppy. You must enable either the USB floppy or CD-ROM as a boot device (under Advanced Setup) and enable "USB Function for DOS" (under Features Setup).
Award BIOS (from Phoenix Technologies): USB Keyboard works. USB booting is not implemented by this BIOS, although it is listed in the menus.

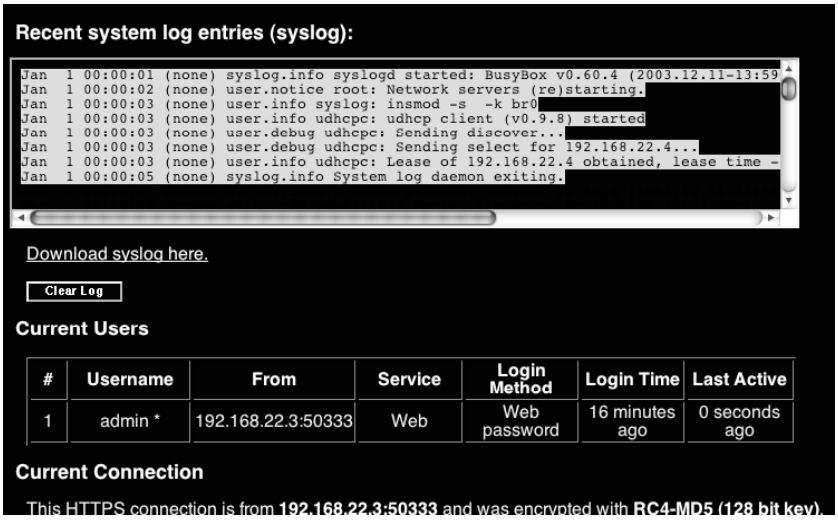
NOTE: BIOS firmware is constantly evolving. Contact your computer or BIOS manufacturer for the latest release of your computer's BIOS for maximum functionality.

Status Screen

This screen displays a system security log, various system settings, and the ability to generate a copy of the system configuration in plain text format.

Port Numbers

This table allows you to change TCP port values for services available on the SV1110IPEXT. By default, they are factory-set to common Internet values. You may wish to enhance security by disabling services that you will not use with the unit. To disable a service, change its port number to **0**. For flexibility, both the **LAN** and **WAN** ports can be configured separately. When you have made any necessary changes, click **Commit Changes** to use the settings the next time the SV1110IPEXT restarts. To force the unit to restart immediately, click **Restart Servers**.



Help! Menu

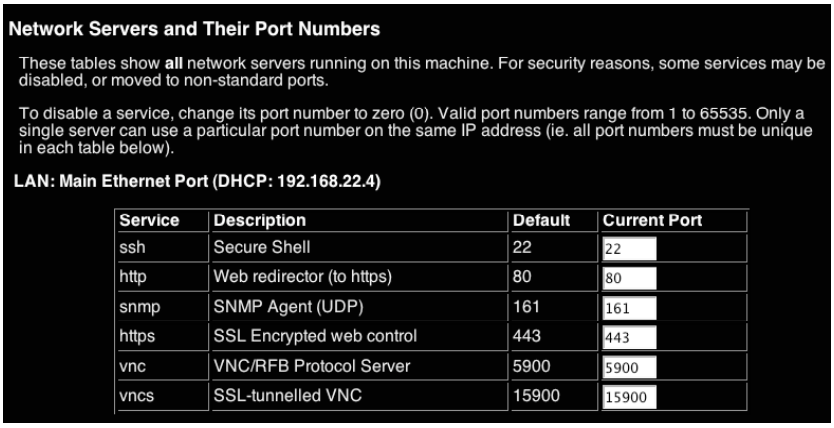
Provides a FAQ (Frequently Asked Questions) listing to assist you with the features and operation of the SV1110IPEXT.

Copyright Menu

Provides the Terms of Use and other information related to the firmware and software on the SV1110IPEXT.

Site map Menu

This menu provides a hyperlinked directory of each setting available on the Web configurator.



Logout

Securely logs you out from your Web session on the SV1110IPEXT.

Using the Terminal Interface via Serial Port

The terminal interface you can access via the serial port permits the configuration of the basic settings of the SV1110IPEXT. While not intended to be a substitute for the Web interface, it does allow you to configure some of the same functions. The menu list below describes the options that can be modified through the terminal interface:

Note that you must use the **W** option to confirm any changes you make before restarting the unit or the changes will not take effect. There is no restart option available from the command line; power the unit off and on again manually to restart the unit in the new configuration.

```
-----------------------------------

Server Remote Control Network Setup

-----------------------------------


NOTE: This interface is used to set network parameters and perform
certain recovery procedures, but the majority of setup and
configuration can only be done using the web interface.

Primary Ethernet Port (LAN)     (00:0e:c5:00:08:1a)

  DHCP is enabled. Current lease information:

  IP Address: 192.168.22.4
     Netmask: 255.255.255.0
     Gateway: 192.168.22.1
   Broadcast: 192.168.22.255

Secondary Ethernet Port (WAN)   (00:0e:c5:00:08:1b)

  IP Address: 192.168.1.123
     Netmask: 255.255.255.0
     Gateway: 192.168.1.254
   Broadcast: 192.168.1.255

Ethernet bridge: Disabled

Machine name: noname

Commands (press one key, then Enter):

    D - Disable DHCP, and use fixed IP address.
 *  I - Set IP address.
 *  N - Set netmask.
 *  G - Set default gateway.
 *  B - Set broadcast address (optional).
    I2 - Set IP address (WAN).
    N2 - Set netmask (WAN).
    G2 - Set default gateway (WAN).
    B2 - Set broadcast address (WAN, optional).
    E - Ethernet bridging (enable or disable).
    M - Change machine name (DHCP client name).
    H - Reset/disable firewall, TCP ports, SNMP, RADIUS.
    F - Reset everything to factory defaults.
    S - Change system admin password.
    P - Send ICMP ping packets (testing purposes).
    ? - Show TCP/IP ports and servers enabled.
    R - Revert to current settings (undo changes).
    W - Commit changes to configuration.

 *  -> These values ignored due to DHCP.


Choice:
```

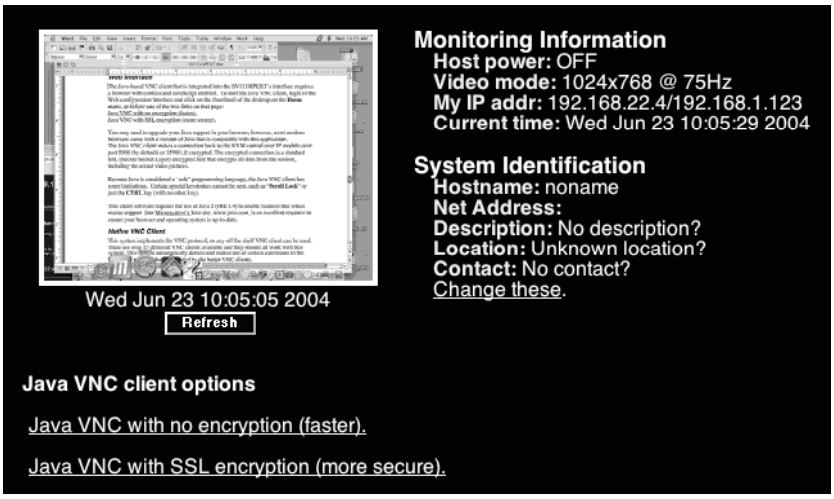
Accessing the VNC Interface

There are three ways to communicate with the KVM control over IP module in order to control the host computer.

- **Web interface:** The integrated Web server includes a Java-based VNC client. This allows easy browser-based remote control.
- **Native VNC client:** There are several third-party software programs that use the standard VNC protocol, available in open source and commercial VNC clients.
- **SSH access:** By default, there is a standard SSH server running on port 22 (the standard SSH port). Once connected via SSH, the VNC traffic is tunneled through the SSH connection and encrypts the VNC session. Each method will be discussed briefly in the following section. The type of encryption method or client used is not critical.

Web Interface

The Java-based VNC client that is integrated into the SV1110IPEXT's interface requires a browser with cookies and JavaScript enabled. To start the Java VNC client, login to the Web configuration interface and click on the thumbnail of the desktop on the **Home** menu, or follow one of the two links on that page:
Java VNC with no encryption (faster).
Java VNC with SSL encryption (more secure).



You may need to upgrade your Java support in your browser; however, most modern browsers come with a version of Java that is compatible with this application.
The Java VNC client makes a connection back to the KVM control over IP module over port 5900 (by default) or 15900, if encrypted. The encrypted connection is a standard SSL (Secure Socket Layer) encrypted link that encrypts all data from the session, including the actual video pictures.

Because Java is considered a "safe" programming language, the Java VNC client has some limitations. Certain special keystrokes cannot be sent, such as "**Scroll Lock**" or just the **CTRL** key (with no other key).

This client software requires the use of Java 2 (JRE 1.4) to enable features like wheel mouse support. Sun Microsystem's Java site, www.java.com, is an excellent resource to ensure your browser and operating system is up-to-date.

Native VNC Client

This system implements the VNC protocol, so any off the shelf VNC client can be used. There are over 17 different VNC clients available and they should all work with this system. This system automatically detects and makes use of certain extensions to the basic RFB protocol that is provided by the better VNC clients.
The best client currently is TightVNC (www.tightvnc.com). Binaries are available for Windows, Linux, MacOS and many versions of Unix. Source code for all clients is available there too. This version of VNC is being actively developed. The authoritative version of VNC is available from RealVNC (www.realvnc.com). This source base is the original version of VNC, maintained by the original developers of the standard. For a commercial, supported version of VNC, you should consider TridiaVNC (www.tridiavnc.com). Their version of VNC is a superset of TightVNC and contains a number of enhancements for use in a larger corporate environment.

NOTE: Some native VNC clients may require a flag or setting indicating they should use BGR233 encoding by default. If this flag is not set, you may see a garbled picture and the client will fail. The Unix versions of VNC require the flag **-bgr233**. For examples on using this flag, review the commands in the following section.

SSH Tunnel (with Native VNC client)

If you are using openssh, here is the appropriate Unix command to use, based on the default settings on a machine at 10.0.0.34:

ssh -f -l admin -L 15900:127.0.0.1:5900 10.0.0.34 sleep 60
vncviewer **-bgr233** 127.0.0.1::15900

Same command, but using the WAN port:

ssh -f -l admin -L 15900:127.0.0.1:5900 10.0.0.98 sleep 60
vncviewer **-bgr233** 127.0.0.1::15900

Notes:

A copy of these commands, with appropriate values filled in for your current system setting, is provided in the *on-line help* page. This allows you to "cut-and-paste" the required commands accordingly.

You have 60 seconds to type the second command before the SSH connection will be terminated.

The port number "15900" is arbitrary in the above example and can be any number (1025...65535). It is the port number used on your client machine to connect your local SSH instance with the VNC client. If you want to tunnel two or more systems, you will need to use a unique number for each instance on the same SSH client machine.

Some Unix versions of the VNC client have integrated SSH tunneling support. Some clients require your local user id to be the same as the userid on the system.

Use a command like this:

vncviewer **-bgr233** -tunnel 10.0.0.34:22

Using the VNC Menu

One of the unique features of this product is the VNC menu system. Whenever you see a window with a dark blue background and grey edges, this window has been inserted into the VNC datastream so that it is effectively laid over the existing video. These menus allow you to control the many features of the SV1110IPEXT without resorting to the web interface or a custom client.

Welcome Window

When you initially connect to the system, a window similar to the one above will be shown.
This tells you which system you are controlling, what encryption algorithm was used and what key strength is currently in effect. Click anywhere inside the window to clear it, or wait ten seconds.

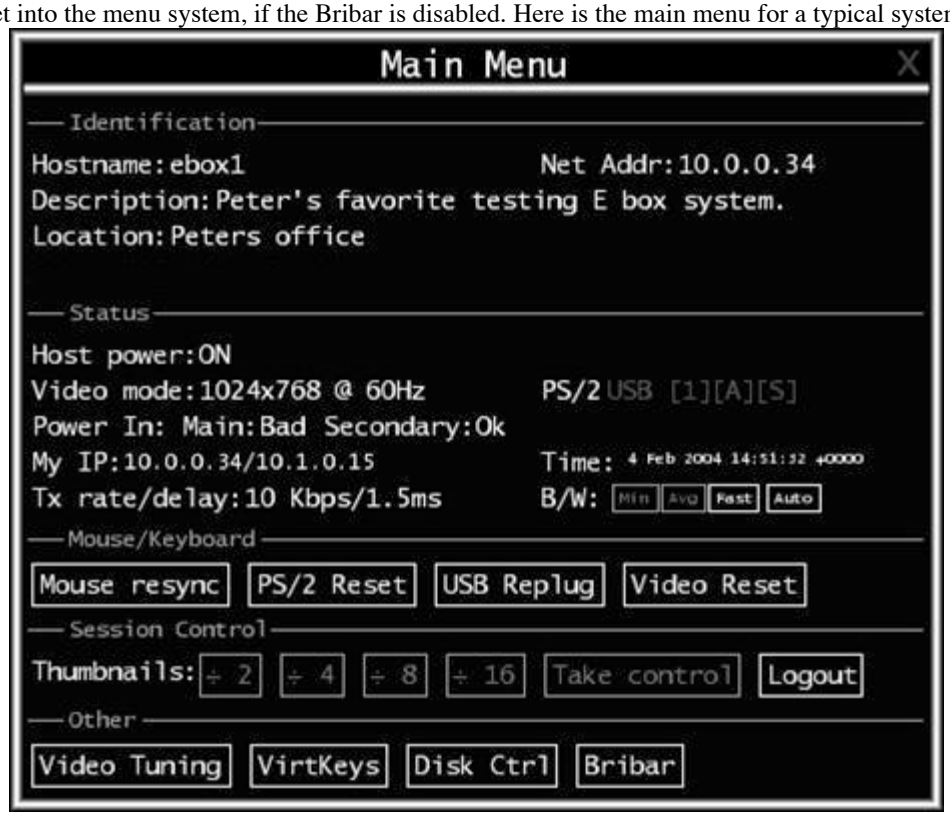
Bribar Feature

Along the bottom of the VNC screen is a dark blue bar with various buttons. We call this feature “the bribar”. Its purpose is to show a number of critical status values and to provide shortcuts to commonly used features. Here is a snapshot of what it may look like. There will be slight differences based on optional features and system configuration. Starting from the left side of the Bribar, each feature and its function is outlined below.

Bandwidth: Indicates current average bandwidth coming out of the KVM control over IP module. The second number measures round trip time (RTT) of the connection when it was first established.
Resync: Re-aligns the remote and local mouse points so they are on top of each other.
Redraw: Redraws the entire screen contents; occurs immediately.
PS/2: Resets the PS/2 keyboard and mouse emulation. Useful to recover failed mouse and/or keyboard connections in PS/2 mode.
USB: Resets the USB connection by simulating an unplug and replug. Forces operating system to notice the USB keyboard, mouse and emulated disk drive.
÷4, ÷8: Switches to thumbnail mode, at indicated size.
Ctrl-Alt-Del: Sends this key sequence to the host. Works immediately.
Alt-F4: Sends the key sequence to host (closes windows).
KVM: Sends the KVM “hotkey” sequence. This function is only enabled when you have configured the unit to expect a particular brand of KVM downstream. It sends the key sequence to pull-up the KVM's on-screen display (OSD) menu.
Menu: Shows the main menu.
Video: Shows the video-tuning menu where the picture quality can be tuned.
Keys: Shows the VirtKeys menu, which allows you to simulate pressing special keys such as the Windows key or complex multi-key sequences.
Disk: Shows the USB emulated disk menu.
In/Ej: Insert or eject the emulated USB disk. Enabled only if the host is recognizing the USB disk.
R/W: Shows if the disk image is readable and/or writeable. If the disk is readable, the R letter will be white. Whenever the host reads from the disk, the R letter will glow green for a few seconds. Whenever the host is writing to the disk, the W letter will glow for a few seconds.
8M: The type of USB disk selected is indicated here. In this example, it is an eight-megabyte Ramdisk. The letters Flpy indicate floppy disk and CD indicate emulated CD-ROM.
PS/2: This area will show either PS/2 (as in this example) or USB to indicate if keyboard and mouse are being emulated via USB connection or PS/2 signals.
[1][A][S]: These flags show the state of the keyboard lights, NumLock, ShiftLock and ScrollLock respectively.
X: Click this button to close the Bribar and hide it. This can be very useful on a client machine whose screen-size is the same as the remote machine. No vertical screen space is wasted with the Bribar. Use double-F7 to start the main menu, then click on Bribar to restore the feature.
Other items. If the server's screen is larger than 1024x768, additional buttons will be shown to the right of the above listed items. These are all keyboard shortcuts and are duplicated in the Keys menu.

Main Menu

To access the main menu, press F7 twice quickly. You must press the key twice within one second. If you press it once or too slowly, then the F7 key(s) are sent to the host, just like any other key. This is the only way to get into the menu system, if the Bribar is disabled. Here is the main menu for a typical system:



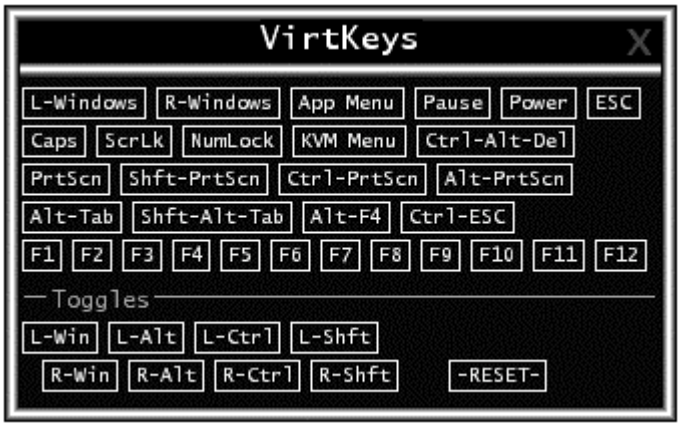
The main menu window may be moved by clicking and dragging on the title bar. It can be closed by pressing Escape, or by clicking on the red X in the top right corner.
Here is a guide outlining various fields from the Main Menu. Most of the functions operate immediately. Other functions require a response to a confirmation prompt first before performing the requested function.
Identification - Fixed text data that is defined by the user from the web interface. Intended as an organizational aid.

Status: Current status of the attached system and the status of the module.
B/W Min/Avg/Max/Auto: Bandwidth control. The white button is the mode the system is currently operating. If you choose **Min/Avg/Max** then you will override the default, **Auto**. As the automatic mode measures actual network performance, you may see the current mode switch from **Min** up to **Avg** or **Max**. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.
Mouse Resync: Resynchronizes the mouse pointer so that the local and remote mouse pointers are on top of each other.
PS/2 Reset: Resets the PS/2 emulation going to the host and to the attached PS/2 devices. This can be used if the mouse stops responding or the PS/2 keyboard isn't working.
USB Replug: Simulates unplugging the USB connector and then plugging it back in. If the host is confused or having trouble with USB, this button may be used to restore it.
Take Control: When multiple users are connected to the same system, use this button to take control away from another user. Only one user may control the keyboard and mouse at any time. All users see the same picture.
Thumbnails: Switch to smaller thumbnail size screen images (click anywhere on thumbnail to restore it). Each button corresponds to a different sized image, from half size to one-sixteenth.

Logout: End the VNC login session and disconnect.
Video Tuning: Sub-menu with video adjustments, to be used when automatic picture adjust does not provide a good quality picture. (See section below.)
VirtKeys: Virtual keyboard provides a menu with special keys that are often hard to generate but needed by the remote system. The most common key sequence is the "Control - Alt - Delete". (See section below.)
Disk Ctrl: Emulated USB disk control submenu. Shows status of floppy/Ramdisk or CD-ROM and permits easy "insertion" or "eject". (See section below.)
KVM Menu: Simply generates the key sequence Scroll Lock and Scroll Lock-Space. This sequence is used to startup the on-screen menu for a number of enterprise-class KVM switches. When these conventional KVM switches are combined with the KVM control over IP module, this key makes accessing their built-in menu easier, especially from the Java client, which does not support the Scroll Lock key. This button will only be shown when an external KVM has been enabled via the web interface.
Bribar: Closes or reopens the Bribar window along the bottom of the screen.

VirtKeys Menu

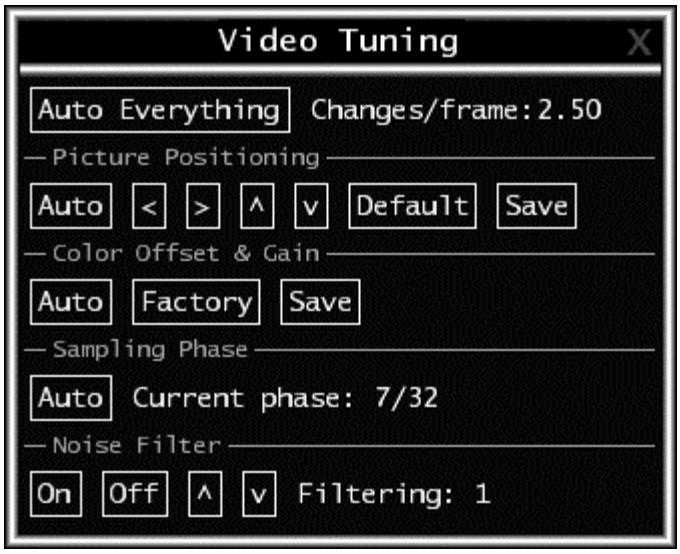
Here is a snapshot of the Virtual Keys window.



Clicking any button in the top half of the window simulates pressing and releasing the indicated key. In the bottom area of the screen, clicking will simulate the indicated Meta key being pressed. You may then click in the top part to send another key and release the Meta key at the same time. Alternatively, you may move the mouse outside this window, press the regular key, and then choose -RESET- to release all depressed keys.
The VirtKeys menu can be left open while using the host system. You can then click the required button at the suitable time, and still interact with the host in a normal fashion.

Examples:

- **Ctrl-Alt-F4:** Use **L-Ctrl** then **L-Alt** in the Toggles area. Then click **F4**.
- To bring up the **Start** menu under Windows: Click the **L-Windows** button at the top left of the above window.



Video Tuning Menu

This menu is used to fine-tune the video picture.

Use the **Auto Everything** button to automatically fine-tune all three adjustments. If the test pattern for Color Offset calibration is not present on the screen, then the Color Offset adjustment is skipped.

Changes/frame indicates the number of 16x16 blocks of video that are being sent, on average, for every frame of video. With a static image being displayed by the server, this number should be zero (shown as -nil-). Moving the mouse, for example, will cause the number to jump to about 2 or 3. You may use this number to judge the picture quality as you adjust the controls on this menu.

Picture Positioning affects the image position on your screen. If you see a black line on either side of your screen, or at the top or bottom, you can use the arrow buttons to shift the image in that direction. Pressing Auto does the same thing for you automatically. Use Save to save the changes you have made manually. Since this adjustment depends on the video mode, separate values are stored for each video mode.

Color Offset is a fine tuning adjustment that requires the use of a test pattern. There is a copy of the test pattern available on the Help! menu of the integrated web server. You must arrange for that image to be shown on the host computer. Do not allow scaling, cropping or any other changes to that image. Press the Auto button and the system will calibrate color for the best possible picture in approximately one minute. If the system cannot find the test pattern on the screen, it will say so. Check that the pattern isn't scaled or covered up. It's important to do this operation in 24-bit or 32-bit color video mode (i.e. truecolor). Although the algorithm may work in 16-bit or 8-bit color video modes, the results will not be optimum and usually it won't be able to find the test pattern.

Sampling Phase does not normally need to be used since our system tunes the sampling phase whenever the video mode changes. This button does not require a test pattern, but will perform optimally when used with our standard test pattern. For your reference, the sampling phase number is shown to the right of the Filtering button.

Noise Filter controls the advanced video filtering of our system. Unlike other filtering algorithms, our noise filter will only remove noise. It does not degrade the signal quality or readability of small text. You may turn it on and off using the indicated button, or set it to other values using the arrows. Higher numbers cause more filtering and may cause artifacts when moving windows. *The most common visual artifact is a*

vertical line dropping when moving windows horizontally. You may use the Redraw button to correct these, or use a lower filter number. At minimum, these values must be greater than two.

Disk Control Menu

Here is a picture of the Disk Control Menu, while using a CD-ROM image:

Aside from status information, there are only three buttons in this window. **Insert** and **Eject** will simulate that action, and only one option is enabled at any time, based on the current state of the emulated disk. **USB Replug** can be used to force the host to recognize the disk. It is not needed unless the host OS or hardware is does not recognize it automatically.

Getting Peak Performance

Choose the best video mode

We recommend using 60Hz refresh rate and 1024x768 resolution. Using a smaller resolution like this allows you to fit multiple windows on your remote desktop. Higher refresh rates stress the video card's quality and do not provide any additional information or benefit.

Noisy video cards

- A digital KVM works by converting the analog video signals emitted by your video card into digital data. If there is noise on that signal, then it must be digitized and sent over the network too. The name brand, quality video cards have, in our experience, better performance simply because they don't add analog noise.
- Some external KVM switches generate video noise too. Try to keep cables short to reduce the effect.
- Enable the Noise Filter option (on the Video Tuning menu) to mitigate noise issues.

Network performance

- The SV1110IPEXT will always send as much data as it can, given what's happening on the screen and the actual network performance. When nothing is changing on the video screen, zero bytes are sent over the network. If the whole screen is changing, then the module will send as much data as your network connection and VNC client can handle while not allowing it to fall behind.
- Network latency, which is the total time it takes for a packet to get to the SV1110IPEXT and come back, has the biggest impact on perceived performance and usability. Network bandwidth has a lesser effect, particular when just moving the mouse around. Only a few bytes need to be sent when the mouse is moving (and nothing else is changing on the screen), but the round-trip-time limits the hand-eye coordination of the user if it is too great. Both actual bandwidth and measured network latency are shown in the Main Menu.

USING YOUR KVM SWITCH

SV831D, SV1631D

Cascade Configuration

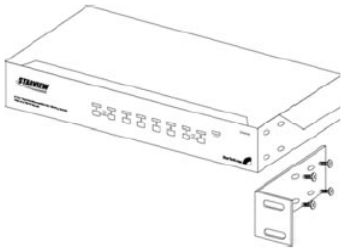
To can connect a second level of KVMs to one or more of your KVM switch's PC ports. There is one **Master** KVM switch, the switch connected to the KVM Control Over IP Console. The KVM switches connected to the Master switch are know as **Slaves**. Once connected, KVM switches configure themselves as either Masters or Slaves. You can only connect an equal or "smaller" KVM to the Master KVM. For example, a 16-port Master KVM switch can have both 16-port and 8-port slaves. An 8-port Master KVM switch can only have 8-port KVM slaves or lower.

The 8-port KVM can support 64 PCs, with 8 8-port Slaves KVMs, each connected to 8 PCs. The 16-port KVM can support 136 computers, with 8 16-port Slave KVMs, each connected to 16 computers.

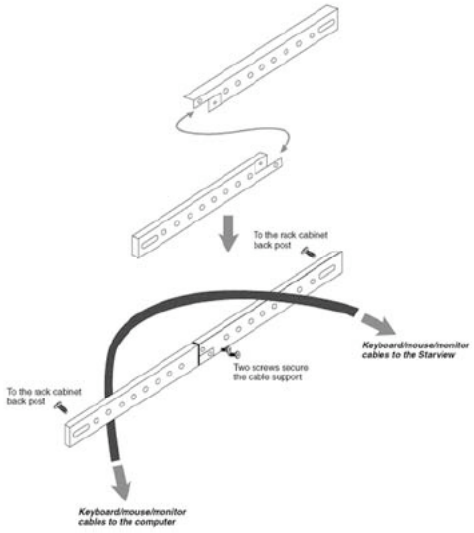
To cascade your KVMs, connect one of your Master switch's **PC** port to the Slave switch's **Console** port. When turning on your cascaded switches, turn on the Master switch before turning on any of the others.

Optional Rack Mount Accessories

Attach the rackmount brackets to the KVM Switch as shown below.



Assemble the rack cable support then screw it to the back and inside the rack cabinet vertical post.



Operating Your KVM Switch

To toggle between computers, you can use the hot-key commands, OSD (On-Screen Display) menu or by using the pushbuttons. If you are operating your PCs remotely, you will likely be using the hot-key commands or the OSD.

Push Buttons

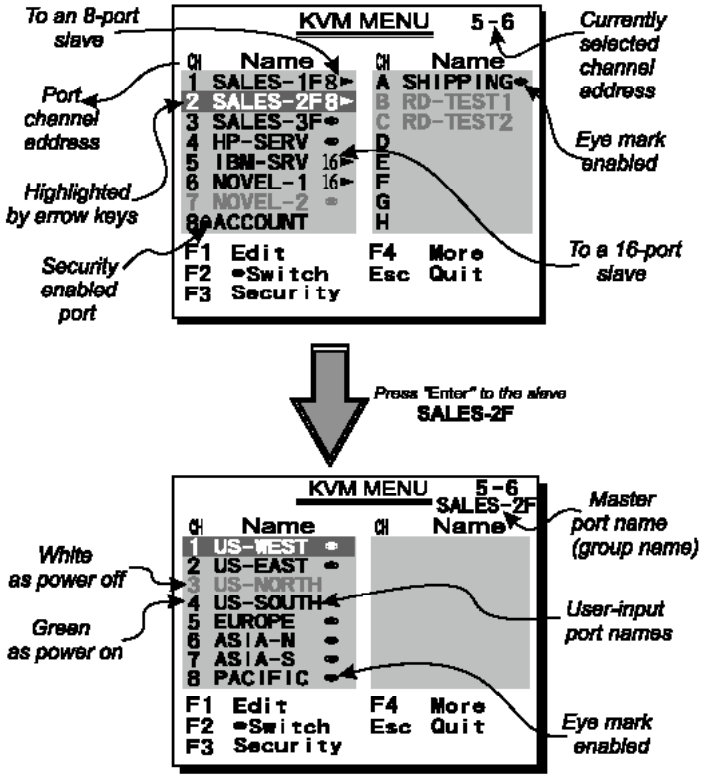
The LEDs on the KVM switch indicate which computers are turned on (green) and which computer is selected (red). The indicator flashes red when in Auto or Manual Scan mode. You can press any of the corresponding pushbuttons to select the active computer.

The **K/M Reset** function reconfigures your system without powering down your computers or your KVM switch. To reset the switch, press the front-panel **1** and **2** buttons simultaneously.

The **Auto-Scan** function automatically scrolls through your connected computers. Press the front-panel **7** and **8** buttons simultaneously to enter Auto Scan mode.

OSD Operations

By hitting the left <CTRL> key twice within two seconds, you may see the 'Hotkey Menu' if it is enabled (an OSD option). Or, by hitting the left <CTRL> key three times within two seconds, you will see a 'KVM MENU' screen showing a list of the computers with corresponding channel addresses, names and status.



The channel address of the currently selected computer is displayed in red, same as the front indicator, to the right of the OSD title 'KVM MENU'. The color of a device name is green if it has power and is ready for selection (its corresponding front panel indicator is green), or the color is white as it has no power. OSD menu updates the color when it is activated. Use the <UP> and <DOWN> arrow keys to highlight a computer and the <ENTER> key to select it. Or, you may press <ESCAPE> to exit OSD and remove the OSD menu from the display; the status window returns to the display and indicates the currently selected computer or operating status.

A triangle mark to the right of a name indicates the port is cascaded to a *Slave*; the number at the left of the triangle mark shows the number of ports the *Slave* has, i.e. **8** for SV831D. <ENTER> key brings you one level down and another screen pops up listing the names of the computers on that *Slave*. The name of the *Slave* will be shown at the upper right corner of the OSD menu. It is useful to group computers and still be able to see the group name.

An eye mark to the right of a name indicating the computer is selected to be monitored in Scan mode. In OSD, this mark can be switched on or off by function key <F2>.

Press <ESCAPE> key to exit OSD and to return to the selected computer; the computer name is also shown on the screen.

Function key <F1>
To edit name entry of a computer or a *Slave*. First, use the <UP> and <DOWN> arrow keys to highlight a channel then press <F1> followed by name entry. Valid characters are **A** to **Z**, **0** to **9**, and the dash character. Lowercase letters are converted to uppercase ones. Press <BACKSPACE> to delete a letter one at a time. Non-volatile memory stores all name entries until you change, even if the unit is powered down.

Function key <F2>
To switch the eye mark of a computer on or off. First, use the <UP> and <DOWN> arrow keys to highlight it, then press <F2> to switch its eye mark on or off. If *Scan Type* is **Ready PC + Eye**, only the power-on and eye mark selected computers will be displayed sequentially in Scan mode.

Function key <F3>
To lock a device (a computer or a *Slave*) from unauthorized access, use *Security*. *Security* is effective for only one device (a computer or a *Slave*). To lock a device, use the <UP> and <DOWN> arrow keys to highlight it, then press <F3>. Now, enter up to 4 characters (**A** to **Z**, **0** to **9**, dash) followed by <ENTER> as new password. A Security-enabled device is marked with a lock following its channel number. To permanently disable the *security* function from a locked device, highlight it, press <F3> then enter the password.

If you want to access the locked device temporarily, simply highlight it and press <ENTER>, the OSD will ask you for the password. After entering correct password, you are allowed to use the device. This device is automatically re-locked once you switch to another one. During Scan mode, OSD skips the security-enabled device.

NOTE: Only one device (a computer or a *Slave*) can be locked by this function at a time.

If you forget the password, the only way to permanently disable the security function is to remove all possible power sources from the master StarView. You need to turn off all computers and unplug all power adapters, then restart everything

Function key <F4>
More functions are available by hitting <F4>. A new screen pops up displaying more functions as described below. Most of them are marked with a triangle indicating there are options to choose from. Using the <UP> and <DOWN> arrow keys, select the functions and press <ENTER>. Available options will be shown in the middle of the screen. Again, using the <UP> and <DOWN> arrow keys to view options then press <ENTER> to select it. You can press <ESCAPE> to exit at any time.

Auto Scan
In this mode, the StarView automatically switches from one power-on computer to the next sequentially in a fixed interval. During *Auto Scan* mode, the OSD displays the name of the selected computer. When *Auto Scan* detects any keyboard or mouse activity, it suspends the scanning until activity stops; it then resumes with the next computer in sequence. To abort the *Auto Scan* mode, press the left <CTRL> twice, or, press any front button. *Scan Type* and *Scan Rate* set the scan pattern. *Scan Type* (<F4>: More\Scan Type) determines if scanned computers must also be eye mark selected. S*can Rate* (<F4>: More\Scan Rate) sets the display interval when a computer is selected before selecting the next one.

Manual Scan
Scan through power-on computers one by one by keyboard control. *Scan Type* (<F4>: More\Scan Type) determines if scanned computers must also be eye mark selected. Press the up arrow key to select the previous computer and the down arrow key to select the next computer. Press any other key to abort the *Manual Scan* mode.

Audio Stick
An optional multimedia module can be LINKed to the back of each StarView for selecting microphone and stereo speaker signals. There are two options for *Audio Stick*: **ON** and **Off**. When set to **On**, audio selection follows computer selection. When set to **Off**, audio selection stops following computer selection. It is useful if you want to listen to a particular computer's audio signal while operating other computers. The non-volatile memory stores the *Audio Stick* setting.

Scan Type
Ready PC + Eye: In Scan mode, scan through power-on and eye mark selected computers.
Ready PC: In Scan mode, scan through power-on computers.
The non-volatile memory stores the *Scan Type* setting

Scan Rate
Sets the duration of a computer displayed in *Auto Scan* mode. The options are **3 seconds, 8 seconds, 15 seconds and 30 seconds**. The non-volatile memory stores the *Scan Rate* setting.

Keyboard Speed
StarView offers keyboard typematic setting that overrides the similar settings in BIOS and in Windows. Available speed options are **Low**, **Middle**, **Fast** and **Faster** as 10, 15, 20 and 30 characters/sec respectively. The non-volatile memory stores the Keyboard Speed setting.

Hotkey Menu
When you hit the left <CTRL> key twice within two seconds, the Hotkey Menu appears displaying a list of hot-key commands if the option is **On**. The Hotkey Menu can be turned **Off** if you prefer not to see it when the left <CTRL> key is hit twice. The non-volatile memory stores the Hotkey Menu setting.

CH Display
Auto Off: After you select a computer, the channel address and name of the computer will appear on the screen for 3 seconds then disappear automatically. **Always On**: The channel address and name of a selected computer and/or OSD status displayed on the screen all the time. The non-volatile memory stores the CH Display setting.

Position
The position of the selected computer name and/or OSD status displayed on screen during operation. The actual display position shifts due to different VGA resolution, the higher the resolution the higher the display position. The non-volatile memory stores the Position setting.
UL as Upper Left **UR** as Upper Right
LL as Lower Left **LR** as Lower Right
MI as Middle

ESC: To exit the OSD, press the <ESCAPE> key

Hot Key Commands

A hot key command is a short keyboard sequence to select a computer, activate a computer scan, etc. A hot-key sequence starts with two **Left Control** keystrokes followed by one or two more keystrokes. A built-in buzzer generates a high-pitched beep for correct hot-key sequences and a low-pitched beep for errors or bad key combinations that will not be carried out.

The short form hot-key menu can be turned on as an OSD function (<F4>: more\Hotkey Menu) every time the left <CTRL> key is pressed twice.
L-CTRL: is the <CTRL> key located at the left side of the keyboard.
1~8/A~H: are the number keys 1 ~ 8 at the upper row of the keyboard and character keys A ~ H case insensitive.

Do not use the keypad at the right of the keyboard.

Selecting a Computer
To select a computer by hot-key command, you must know its channel address, which is determined by the StarView connection. For a computer connected to a *Master*, its address is represented by the PC port label (1~8 or A~H). For a computer connected to a *Slave*, two characters represent its address. The first character is the channel address of the *Master* unit (1~8) and the second one is the channel address of the *Slave* (1~8 or A~H). Please note that only *Master's* 'PC 1' ~'PC 8' ports can be connected to a *Slave*.

left ***Ctrl*** + left ***Ctrl*** + ***7*** selects a computer connected to port 7 of the *Master*.
left ***Ctrl*** + left ***Ctrl*** + ***6*** + ***C*** selects a computer connected to port C of a *Slave* connected to port 6 of the *Master*.

Auto Scan
To start *Auto Scan*, automatically scan power-on computers one by one at a fixed interval:
left ***Ctrl*** + left ***Ctrl*** + ***F1***

When *Auto Scan* detects any keyboard or mouse activity, it suspends the scanning till activity stops; it then resumes with the next computer in sequence. The length of the *Auto Scan* interval (*Scan Rate)* is adjustable. To abort the *Auto Scan* mode, press the left ***Ctrl*** key twice.

Note: *Scan Type* determines whether eye mark is necessary during *Auto Scan*.

Manual Scan enables you to manually switch back and forth between power-on computers.
left ***Ctrl*** + left ***Ctrl*** + ***F2***

Press the up or down arrow to select the previous or the next computer in sequence. And, press any other key to abort the *Manual Scan.*
Note: *Scan Type* determines whether eye mark is necessary during *Manual Scan*.
To adjust *Scan Rate* which sets the duration before switching to the next computer in *Auto Scan*:

left ***Ctrl*** + left ***Ctrl*** + ***F3***

The StarView sends one to four beeps indicating scan interval of ***3***, ***8***, ***15*** and ***30*** seconds respectively.

To adjust keyboard typematic rate (characters/sec), this setting over-rides that of BIOS and any operating system:

left ***Ctrl*** + left ***Ctrl*** + ***F4***

The StarView generates 1 to 4 beeps corresponding to ***10***, ***15***, ***20*** and ***30*** characters/sec respectively.

Audio Stick

An optional multimedia module can be LINKed to the back of each StarView for selecting microphone and stereo speaker signals. There are two options for *Audio Stick*: **On** and **Off**. When set to **On**, audio selection follows computer selection. When set to **Off**, audio selection stops following computer selection. It is useful if you want to listen to a particular computer's audio signal while operating other computers.

left ***Ctrl*** + left ***Ctrl*** + ***F5***

The StarView generates 1 or 2 beeps corresponding to ***On*** and ***Off*** respectively.

Troubleshooting

If you are experiencing trouble with your devices, first make sure that all cables are connected to their proper ports and are firmly seated. You may also want to try resetting the devices by removing and reconnecting the AC Adapter (SV1110IPEXT) or the **KVM Reset** button (SV831D, SV1631D). If problems persist, you can do a full reset of the SV1110IPEXT by using the rest to factory setting from the serial terminal interface menu. Using the factory restore button will **delete all your configurations and restore the device back to the factory defaults**. You will have to go through the initial setup procedure again.

Video response is slow to respond or erratic.

- Verify that the managed host computer video configuration is set to a supported resolution and refresh rate. Optimum video resolution is 1024 x 768 @ 75Hz. For a list of supported video resolutions and refresh rates, see the Technical Specifications.

Video displays pink screen.

- Verify that the managed host computer is turned on.
- Verify that the video refresh rate on the managed host is set to 85Hz or lower.
- Re-establish video communication using power-on reset.
- Reboot the managed host computer as needed.

Mouse pointer or mouse buttons slow to respond or erratic.

- Re-sync the mouse using the left-click or moving it across the screen several times (for at least five seconds).

Mouse pointer is out of sync with local mouse "dot."

- Verify that the managed host computer mouse acceleration is turned off. See "Mouse Acceleration."

Can't communicate with the SV1110IPEXT after power-on reset or new installation.

- Wait 10 seconds after resetting before attempting to access the device.
- Ensure that the correct IP address has been entered in the browser.
- If you have performed a "factory default restore," the IP address has been reset to 192.168.1.254.
- If you are operating behind a firewall, make sure that all the appropriate ports have been opened.

No OSD screen.

- Make sure monitor cables are firmly connected.
- Make sure you are using a Multisync monitor.

Master/Slave does not work or there is a double OSD.

- Make sure that the slave's Console port is connected to one of the Master's PC ports.
- Perform a KVM Reset.

The Up and Down arrows don't work in manual scan mode.

- Check the Scan Type (from the OSD menu) and make sure you have selected the proper computers.

Auto Scan does not work, the StarView beeps and the indicators flash red

- Make sure more than one computer is turned on. Auto Scan only works with powered on computers.
- Check the Scan Type (from the OSD menu) and make sure you have selected the proper computers.
- Press the Left Control key twice to abort the Auto Scan.

OSD menu is not in the proper position.

- The OSD menu has a fixed resolution and its size varies depending on the monitor. Use <F4> More/ Position (from the OSD menu) to move the OSD menu to a different location.

Cannot select a computer connected to a Slave.

- Make sure that the Slave's Console port is connected to one of the Master's PC ports.
- Only ports PC1 to PC8 can be connected to Slaves, even if the Master KVM has 16 PC ports.
- Only one level of Slave KVMs is allowed.

Forgotten master password. (SV1110IPEXT)
You can reset the master password using the serial interface on the module. Use the `S' command, and type a new password. The old password is not required for this procedure.

Remote mouse and local mouse don't line up. (SV1110IPEXT)
Use the "mouse resync" command in the main menu or press the "Resync " button on the Bribar. If the mouse pointers still don't line up, verify that mouse acceleration has been disabled.
NOTE: The Windows login screen does not accept the "mouse acceleration" configuration, and always has the mouse accelerated regardless of your configuration. Therefore, on this screen it is best to avoid using the mouse.

After resync, mouse is still a little bit off. (SV1110IPEXT)
Use the video adjust menu to position your video image exactly where it should be. Normally a slight video positioning error is perceived as a mouse sync issue. A video positioning error is visible as a black line along the top or bottom (and right or left) edges of the remote screen. *Remember to save your position changes!*

Cannot login via SSH. (SV1110IPEXT)
Remember to use either "admin" or a username created in the system as the user name you give your SSH client. If you see a warning about "identity of host cannot be verified", and a question about saving the host's fingerprint, this is normal for the first time you connect to any machine running SSH. You should answer "yes" so that your SSH client saves the public key of this host and doesn't re-issue this warning.

Certificate warning shown when connecting via HTTPS. (SV1110IPEXT)
It is normal for a warning dialog to be shown when connecting via HTTPS. The SSL certificate we use is created when the unit is first produced. It does not contain the correct hostname (subject name) because you can change the hostname as required. Also, it is not signed by a recognized certificate authority (CA) but is signed by our own signing authority. For more details, refer to Appendix A, "About Security Certificate Warnings".

Don't set LAN and WAN to the same IP Address. (SV1110IPEXT)
It doesn't work. If you want to use both ports in redundant mode, enable the Ethernet bridging option and plug both into the same network. The WAN IP address is not used in that configuration.

Appendix A: About Security Certificate Warnings

What is a security certificate?
Sites that employ secure TCP/IP (Internet) connections include a certificate that confirms that users are connecting to a legitimate site and are not being redirected without their knowledge. Certificates are issued by trusted third parties called Certificate Authorities (CAs) and contain essential details about a site that must match the information supplied to your Web browser.

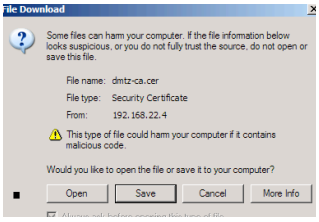
Why do I receive a warning when I access the login screen on the SV1110IPEXT?
As it redirects to a secure (SSL) session by default, the login screen may generate a warning from your Web browser or the VNC Java client for two different reasons. First, the CA that has issued the certificate on StarTech.com's behalf may not yet be recognized as a trusted source by the computer you are using to access the SV1100IPEXT. Second, since the unit could be configured in a number different ways, it is impossible to supply a generic certificate that will match your exact network settings.

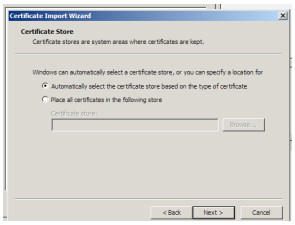
Is my data safe?
Yes. The security certificate does not affect encryption effectiveness in any way, nor does it make the SV1110IPEXT any more vulnerable to outside attacks.

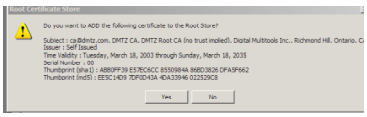
Can I prevent the warning from occurring?
Yes. You have two options that may prevent the warning from occurring. First, if the Web browser you are using offers the option to ignore the warning for future visits, the browser will no longer generate a warning if that option is selected. Second, if you install the certificate from the SV1110IPEXT onto the host computer (see below) and if the unit is configured with a domain name ending in .com, .net, .org, .gov, .edu, .us, .ca, .uk, .jp, or .tw (i.e. **remotecontrol.mydomain.net**) then the warning should no longer occur.

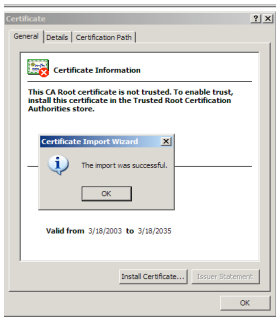
Installing the new certificate…
The following is a demonstration of how to install the certificate from the SV1110IPEXT onto your local computer.

1. Open your Web browser and go to the SV1110IPEXT login screen. Click the update security certificate link.
2. When prompted, choose **Open**.
3. A Window will appear that offers information about the certificate. Click **Install Certificate**.
4. The **Certificate Import Wizard** will appear. Select **Automatically select the certificate store…** (default) and click **Next**. When the next window appears, click **Finish**.
5. A confirmation dialog will appear asking you if you wish to install the certificate. Click **Yes**.
6. A message should appear saying the import was successful. Click OK.









Technical Specifications

KVM-over-IP (SV1110IPEXT):

Maximum supported video mode	1600x1200 @ 85Hz
Standard video modes supported	640x400 @ 85Hz 720x400 @ 85Hz 640x480 @ 60Hz 640x480 @ 72Hz 640x480 @ 75Hz 640x480 @ 85Hz 800x600 @ 56Hz 800x600 @ 60Hz 800x600 @ 72Hz 800x600 @ 75Hz 800x600 @ 85Hz 1024x768 @ 60Hz 1024x768 @ 70Hz 1024x768 @ 75Hz 1024x768 @ 85Hz 1152x864 @ 75Hz 1280x960 @ 60Hz 1280x960 @ 85Hz 1280x1024 @ 60Hz 1280x1024 @ 75Hz 1280x1024 @ 85Hz 1600x1200 @ 60Hz 1600x1200 @ 65Hz 1600x1200 @ 70Hz 1600x1200 @ 75Hz 1600x1200 @ 85Hz
Maximum power consumption	15 watts (12 VDC, 1.2A)
Input Connectors	Video In PS/2 Keyboard PS/2 Mouse USB LAN RJ-45 WAN RJ-45 R-Port (RJ11) DB9 RS-232 Female DC in (2, with redundancy)
Regulatory Certifications	FCC Class A, CE

Service	*Description*	*Benefits*
SSH	Secure Shell	May be used to securely “tunnel” VNC and HTTP protocols.
HTTP	Web redirector (to HTTPS)	Convenience server to redirect all web traffic to encrypted port. Clear-text HTTP is not supported.
SNMP	SNMP Agent (UDP)	Allows integration with existing SNMP network management systems.

Service	*Description*	*Benefits*
HTTPS	SSLTLS Encrypted web control	Secure control and management of the device and attached system. Screen snapshots may be downloaded. Integrated Java VNC client (with or without encryption) allows control from any Java-enabled browser. Password protected.
VNC	VNC/RFB Protocol Server	Standardized real-time KVM network protocol. Compatible with existing VNC client software.
VNCS	SSL-tunneled VNC	VNC protocol tunneled via SSLTLS encryption. For secure real-time control of the server over public networks.
DHCP Dynamic IP Setup Config		Eases network setup by fetching IP address and other network settings from a centralized server.
RADIUS Centralized authentication		Allows integration with existing RADIUS servers, so that user management can be centralized. Supports challenge-response authentication using hardware tokens (like SecurID) and conventional passwords.
SYSLOG	System event logging to another system	MIT-LCS UDP protocol. Must be configured via DHCP option.
DNS	Domain Name Service	Converts text name into IP Address Only used in the URL specification needed to emulate a CD-ROM. Use is optional.

KVM Switch (SV431D, SV831D, SV1631D):

	SV431D	**SV831D**	**SV1631D**
User port number	1	1	1
Computer port number	4	8	16
Cascade control PC number	Up to 16	Up to 64	Up to 136
Front panel control	4	8	16
Hot plug and play	Yes	Yes	Yes
Hot key control	Yes	Yes	Yes
Rack mountable	Yes	Yes	Yes
Auto scan interval	3, 8, 15, 30 seconds	3, 8, 15, 30 seconds	3, 8, 15, 30 seconds
Programmable scan pattern	Yes	Yes	Yes
Cable length (max.)	100 ft (30m)	100 ft (30m)	100 ft (30m)
VGA	1600x1220, DDC2B	1600x1220, DDC2B	1600x1220, DDC2B
Computer Keyboard	PS/2	PS/2	PS/2
Mouse	PS/2	PS/2	PS/2
Monitor	HD-DB-15 male	HD-DB-15 male	HD-DB-15 male
Console Keyboard	PS/2	PS/2	PS/2
Mouse	PS/2	PS/2	PS/2
Monitor	HD-DB-15 female	HD-DB-15 female	HD-DB-15 female
Dimensions	8.63 x 5.13 x 1.75” (219 x 129 x 44mm)	17.25 x 7.25 x 1.75" (438 x 184 x 44mm)	17.25 x 8.75 x 3.5” (438 x 222 x 89mm)
Power Supply (min.)	9V DC 600 mA	9V DC 600mA	9V DC 600mA

Technical Support

The following technical resources are available for this StarTech.com product:

On-line help:

We are constantly adding new information to the *Tech Support* section of our web site. To access this page, click the *Tech Support* link on our homepage, **www.startech.com**. In the tech support section there are a number of options that can provide assistance with this product.

Knowledge Base - This tool allows you to search for answers to common issues using key words that describe the product and your issue.

FAQ - This tool provides quick answers to the top questions asked by our customers.

Downloads - This selection takes you to our driver download page where you can find the latest drivers for this product.

Call StarTech.com tech support for help:

USA/Canada: 1-800-265-1844

UK/Ireland/Europe: 00-800-7827-8324

Support hours: Monday to Friday 8:30AM to 6:00PM EST (except holidays)

Warranty Information

This product is backed by a one-year warranty. In addition StarTech.com warrants its products against defects in materials and workmanship for the periods noted, following the initial date of purchase. During this period, the products may be returned for repair, or replacement with equivalent products at our discretion. The warranty covers parts and labor costs only. StarTech.com does not warrant its products from defects or damages arising from misuse, abuse, alteration, or normal wear and tear.

Limitation of Liability

In no event shall the liability to StarTech.com Ltd. (or its officers, directors, employees or agents) for any damages (whether direct or indirect, special, punitive incidental, consequential, or otherwise), loss of profits, loss of business, or any pecuniary loss, arising out of related to the use of the product exceed the actual price paid for the product. Some states do not allow the exclusion or limitation of incidental or consequential damages. If such laws apply, the limitations or exclusions contained in this statement may not apply to you.

NOTE: The associated software contains encryption technology subject to the U.S. Export Administration Regulations and other U.S. law, and may not be exported or re-exported to certain countries or to persons or entities prohibited from receiving U.S. exports (including Denied Parties, entities on the Bureau of Export Administration Entity List, and Specially Designated Nationals). For more information on the U.S. Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774, and the Bureau of Export Administration (BXA), see the BXA homepage at http://www.bxa.doc.gov

FCC Compliance

This device complies with part 15 of the FCC Rules and also with European standards EN55022. Operation is subject to the following conditions: (1) this device may not cause harmful interference; and (2) this device must accept any interference received, including interference that may cause undesired operation.

June 23, 2004