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 difficulties. (March 15, 2004)

Introduction

Thank you for purchasing a StarTech.com Digital KVM control over IP switch. The SV1110IPEXT and SV1110IPPCI will open a new world of easy remote KVM console management for you.

This document will guide you through the setting up and using the many features of the digital KVM control over IP switch.

Before You Begin

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

Contents

This package should contain:

SV1110IPEXT

- 1 x SV1110IPEXT unit
- 1 x Power supply

Required Cables

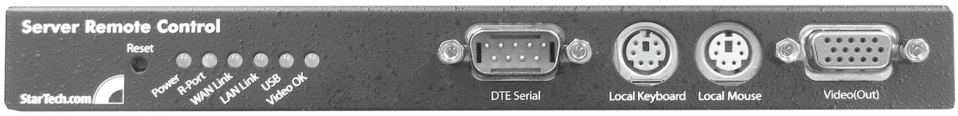
- 1 x RS-232 cable (9-pin RS-232 (straight pin-out))
- 1 x USB cable (Five-pin mini-B to standard type-A)
- 1 x VGA cable (Standard HD15)
- 1 x Ethernet cable (10/100 Mbits/sec Ethernet cable)

SV1110IPPCI

- 1 x SV1110IPPCI card
- 1 x Breakout cable
- 1 x ATX power supply cable
- 1 x Front panel control cable
- 1 x Power supply (The power supply attaches to the breakout cable and can be used to power the SV1110IPPCI when main system power is turned off. The SV1110IPPCI does not use the standby voltages available on the PCI connector.)

Device Connections

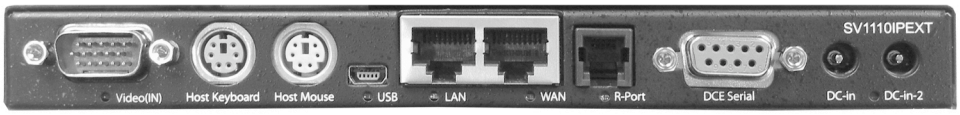
Front View of SV1110IPEXT



Reset *LEDs DTE Serial Local K Local M Video (Out)

**LEDs are, from left to right: Power Good, R Port, WAN link, LAN link, USB, Video OK*

Rear View of SV1110IPEXT



Video (IN) Host K Host M USB LAN WAN R-Port RS-232 (DCE) DC-in DC-in-2

Front View of SV1110IPPCI

*LEDs WAN LAN Breakout

**LEDs are WAN link, LAN link, USB*

SV1110IPEXT Installation

This section will guide you through the installation of your SV1110IPEXT KVM. Please read this section carefully and complete each step in the order listed.

Connecting Your Device

1. Install the system in a convenient location. You may use the optional bracket and two machine screws to secure the hub to the rear of a rack. Choose an orientation that allows easy access to the connectors. The SV1110IPEXT is convection cooled and has no fans, but its cooling vents should not be blocked.
2. Connect your network to the leftmost (LAN) Ethernet port. The first time the unit is booted, it will perform DHCP lease request to get an IP address (and other network settings). Therefore, it is best if it is connected to the network ***before*** being turned on.
3. Connect the VGA video from the video card on the server to the connector on the rear of the SV1110IPEXT.
4. Connect PS/2 mouse and keyboard. These connections are not “hot-pluggable”, so you should power down the host computer to make these connections. If that isn't acceptable, use the USB connection instead.
5. Connect the rear-panel RS-232 serial port to a computer that can be used temporarily for setup and control. This serial port connection is not required once the unit is initially setup and configured. It is an 115,200 BPS (8N1) connection. A straight-through, 9-pin RS-232 cable is used, **not** a null-modem cable.
6. (Optional) Connect USB between the mini-B connector on the rear of the SV1110IPEXT and any USB host port. A USB hub may be used in between. When the USB is connected and recognized by the host, the PS/2 keyboard and mouse connections are not used. However, if your system's BIOS does not support USB keyboards, then you should leave both PS/2 and USB connected to allow BIOS access. Where possible, use USB since it is more reliable than PS/2. Most modern BIOSes will support USB keyboards correctly.
7. Connect the AC/DC power supply to either one of the redundant DC inputs. The front panel power light should illuminate, and the other applicable lights should turn on in about 10 seconds.

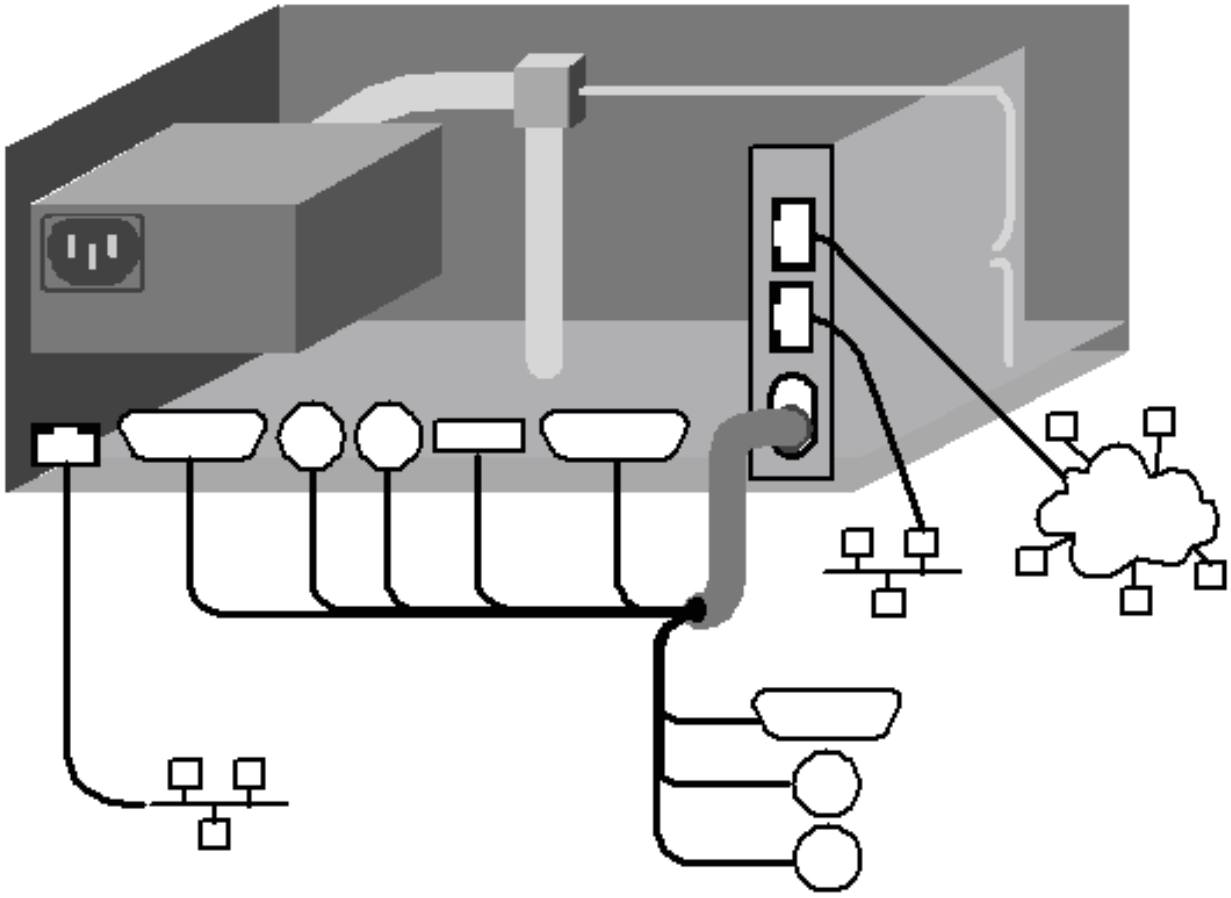
Optional WAN Installation

1. Install optional secondary Ethernet, to the WAN port (rightmost RJ-45 connector). This is a separate network, which can have a different security configuration and is well suited to use on a DMZ or outside your corporate firewall.
2. Install optional secondary AC/DC power supply. The load is shared between the two power supplies and either source will be used if the other source fails.
3. Install local video, keyboard and mouse using the front-panel connections.

SV1110IPPCI Installation

Step 1: Hardware Installation

1. Install the card into any convenient PCI slot. Be sure to secure the metal card bracket securely to the server's chassis.
2. Connect your network to the bottom (LAN) Ethernet port. The first time the unit is booted, it will performs a DHCP lease request to get an IP address (and other network settings). Therefore, it is best if it is connected to the network before being turned on.
3. Install the breakout cable. See the diagram below for reference in later steps. Please note the "long" wires are intended to loop-back to the host, and the "short" wires are for local connections.



4. Connect the VGA video from the video card on the server to the SV1110IPPCI.
5. Connect PS/2 mouse and keyboard. These connections are not "hot-pluggable", so you should power down the host computer to make these connections. If that isn't acceptable, use only the USB connection instead.
6. Connect the rear-panel RS-232 serial port to a computer that can be used, at least temporarily for setup and control. This serial port connection is not required once the unit is initially setup and configured. It is a 115,200 bps (8N1) connection.
7. (Optional) Connect USB to any USB host port. A USB hub may be used in between. When the USB is connected and recognized by the host, the PS/2 keyboard and mouse connections are not used. However, if your system's BIOS does not support USB keyboards, you should leave both PS/2 and USB connected to allow BIOS access. We recommend using USB if possible, since it is more reliable than PS/2. Most modern BIOSes will support USB keyboards correctly.

Step 2: Choosing a Power Supply Method for Your SV1110IPPCI

You can choose between two control methods: ATX or front-panel. You should use the front-panel method if:

- Your server does not have an ATX power supply. Most contemporary computers use a standard power supply connector with twenty pins. If the power supply connector on your motherboard does not mate with the supplied ATX power harness, then your system does not have an ATX power supply.
- You have multiple power supplies or redundant supplies.
- There is a need to frequently remove the SV1110IPCI card. The front panel connector cables can be left inside without connecting them to the card, while the ATX method requires the cable and card to be installed for the server to function.

Front-panel method

- Carefully note which cable goes to the front-panel power switch. You should also be able to determine the correct cable by consulting the documentation that came with your motherboard.
- Unplug the existing cable, and plug our cable into the existing cable. Then plug both our cable, and the existing cable, into the motherboard. The long end of the SV1110IPPCI cable (small connector) can now be connected to the card at the location marked POWER (P5). Be careful to connect to the correct connector on the board.
- Repeat the above procedure for the front-panel reset cable (attaches to P7).
- The IPMB and ATX/EPS connectors should be left unused.

ATX method

- Unplug the main DC power cable between the power supply and the motherboard. There is a small catch on one of the long sides that may need to be depressed before the cable can be removed. Install the ATX power adapter into the motherboard, and connect the power supply to that connector.
- Connect the small 4-pin plug to the SV1110IPPCI card. It connects to the spot labeled ATX/EPS (P8) near the top right of the card.
- The remaining connectors on the card are unused (Power, Reset and IPMB).

Step 3. Power Supply

Connect the AC/DC power supply to either DC input connector on the breakout cable. The card will immediately power up (even if host is off) and the LAN led may flash. The system is ready to run in about 10 seconds. Boot server and return it to service.

Step 4. Optional Local connections

The short leads may be used to connect a local video output (monitor) and PS/2 keyboard and mouse. These may also be connected to a conventional KVM.

Setup of the Server PC

Mouse Acceleration

The server PC to which the KVM control over IP is connected must be configured to disable mouse acceleration. This means that when the KVM control over IP module sends a mouse movement command, the server should not do any arithmetic calculations on the received value. This applies to both PS/2 and USB mouse connections.

NOTE: Throughout this manual "managed host" or "host computer" refers to the computer connected to the KVM control over IP module. "Remote client" or "client computer" refers to the PCs used to access the host computer.

Each operating system has a different way to control the mouse acceleration:

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 and Windows XP

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 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

Initial Setups

DHCP Server Setup

If you have a DHCP server on your network already, the KVM control over IP module should automatically be assigned a dynamic IP address as soon as it is turned on. You can determine if an IP address has been assigned by consulting your DHCP server and looking up the lease information based on the MAC (Ethernet link-layer) address of the KVM control over IP module. The factory-assigned MAC address is printed on a sticker attached to the product.

NOTE: If DHCP setup has been used, there is no need to connect via the serial port.

Connect via Serial Port

Connect a serial cable to a computer (straight-through connection; no null-modem cable required) to change the IP address, or set a static IP address. The serial port is fixed at 115,200 baud (8N1) and cannot be changed. You should be able to use any standard serial terminal program.

Here are some typical terminal programs for different operating systems.

UNIX: tip, cu, kermit, minicom. **Windows:** hyperterm, kermit.

Set the baud rate to 115,200bps 8N1(8-bits, no parity, 1 stop bit).

Once you've connected a serial cable, press Enter to see the **Setup** menu, as shown here:

```
-----------------------------------
External KVM-over-IP 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     (00:04:ac:e3:00:05)
  DHCP is enabled. Current lease information:
  IP Address: 10.0.0.34
     Netmask: 255.255.255.0
     Gateway: 10.0.0.254
   Broadcast: 10.0.0.255

Secondary Ethernet Port   (00:04:ac:e2:00:05)
  IP Address: 10.1.0.2
     Netmask: 255.255.255.0
     Gateway: 10.1.0.1
   Broadcast: 10.1.0.255

Ethernet bridge: Disabled

Machine name: demo.dmtz.com

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 (secondary).
    N2 - Set netmask (secondary).
    G2 - Set default gateway (secondary).
    B2 - Set broadcast address (optional, secondary).
    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:
```

This program has a simple menu-based interface. Type the one or two letter command and press Enter. You will be prompted for the required values.

NOTE:

- Using DHCP is mutually exclusive to using static IP addresses and routing.
- You must save your changes using the "**W**" command. This applies the new values and saves them permanently.
- The master administration password may be changed from this interface (press "**S"**). The default password is "**admin**".

Web Browser Interface

Once the system is configured with your network, login to a web browser interface to finalize your initial setup.

Go to this address, using any web browser:

http://**ipaddr/**

*Where "**ipaddr**" is the numeric IP address that was either assigned by your DHCP server or the fixed IP address you assigned using the serial port method.*

For the system in the example above, the correct address would be:

http://10.0.0.34/

The first screen displayed is the login screen. Use "admin" for the username and enter the password of "admin" to login for the first time. Regular operation and host system control is available on the home page.

To configure and change the setup of the unit, follow the link at the bottom of the page labeled "**Admin/Setup"**. That will take you to a page with various links to different pages that control the administration functions of the system.

Consult the on-line help page or FAQ if you encounter any difficulties.

Your KVM control over IP system is now operational, but we recommend you perform these additional operations:

- Set the time and date (under **Set date and tim**e).
- Select a system hostname (under **Network Setup**).
- Change the master password (under Master Password).
- Create one or more user accounts for day-to-day operation (under Users and Passwords). Only the master account can change the configuration of the system. Regular users can perform all KVM-type operations, including file transfer.
- Disable any unnecessary features under "Port Numbers" to enhance security.
- Define the names and other host identification details under "Change system identification".

LEDs

SV1110IPEXT

There are a number of lights (LEDs) on the front and rear panels of the SV1110IPEXT. This section provides a brief description of each LED.

- **Power Good** - Indicates one or both of the DC power inputs is providing your system with power.
- **R-Port -** [Optional feature]
- **LAN/WAN link** - This is the standard “link light” which is typical for Ethernet equipment. It means the network cable is connected to a working Ethernet hub or switch. It lights up with a link connection and blinks with network activity. The LEDs under the Ethernet connectors respond in a similar manner.
- **USB** - This lights up when the USB port is connected to a host and that host has configured the USB port for use. It will blink when USB data is transmitted.
- **Video Good** - This light is lit when a valid VGA signal is received from the host. It is off while in power save mode, if no video is connected or if the host is off.

SV1110IPPCI

- **LAN/WAN link** - This is the standard “link light” which is typical for Ethernet equipment. It means the network cable is connected to a working Ethernet hub or switch. It lights up with a link connection and blinks with network activity. The LEDs under the Ethernet connectors respond in a similar manner.
- **USB** - This lights up when the USB port is connected to a host and that host has configured the USB port for use. It will blink when USB data is transmitted.

Accessing the Module for KVM Control

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

- **Web interface -** There is an embedded web server running on ports 80 and 443. You may use either HTTP or HTTPS (encrypted HTTP, using SSL/TLS). This interface provides an easy-to-use GUI interface appropriate for setup and control tasks. It can also serve a Java applet, which implements the VNC protocol. This allows easy browser-based remote control.
- **Native VNC client -** The module uses the standard VNC protocol which is available with publicly 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 / Java VNC Client

Use a standard Java-enabled web browser. Cookies and JavaScript must be enabled.

To start the Java VNC client, click on the thumbnail of the desktop on the home page, 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, this link encrypts everything, including the actual video pictures.

Because Java is considered a “safe” programming language, there are some limitations of the Java VNC client. 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 such features as wheel mouse support. This link, www.java.com, provides you with the latest version of your web browser for downloading.

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 VNC Menu System

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 this one 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 make it go away, 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.

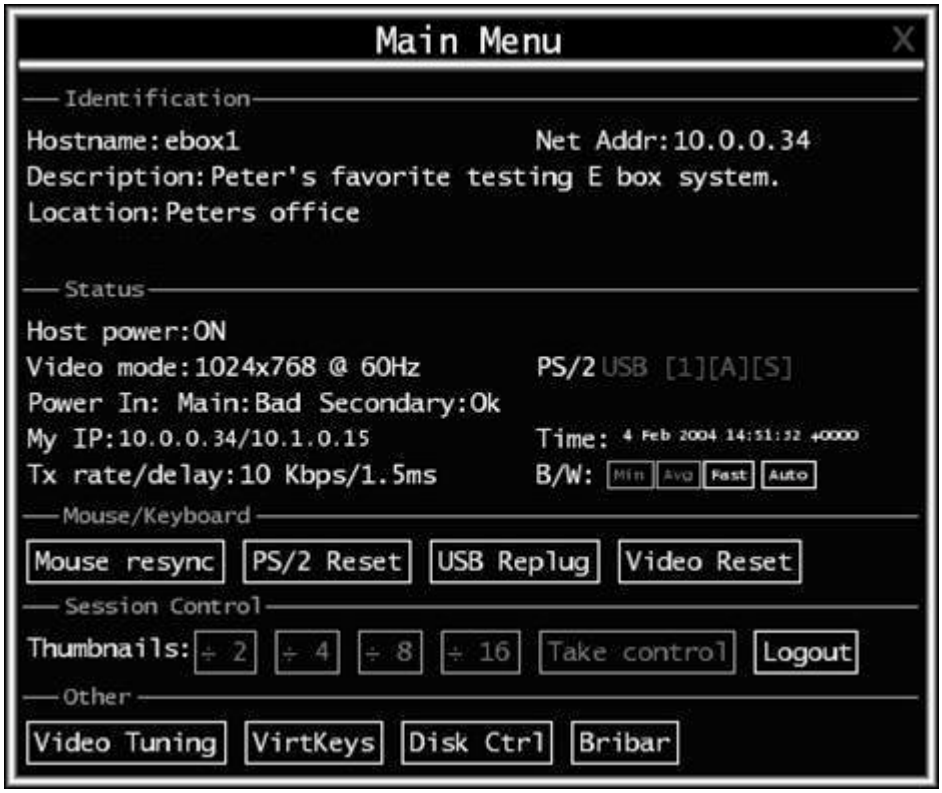
[1][A][S] - These flags show the state of the keyboard lights, NumLock, ShiftLock and ScrollLock respectively.

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 pull up 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.

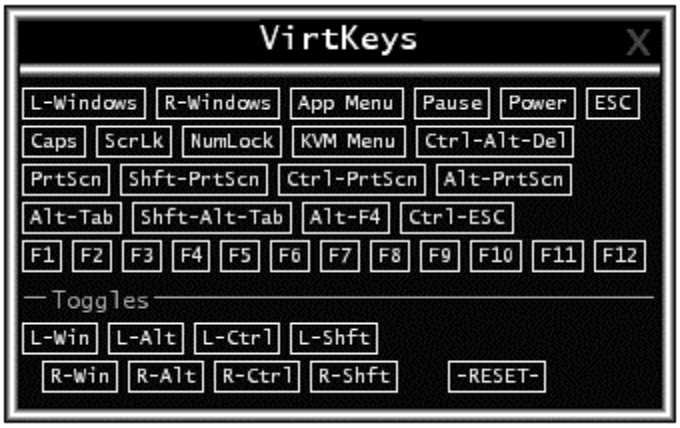
Here is a guide outlining various fields from the Main Menu. Most of the functions operate immediately. Other functions require a response to a confirmation prompt first before performing the requested function.

- **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** - Resync 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 adjusts fail. ***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.

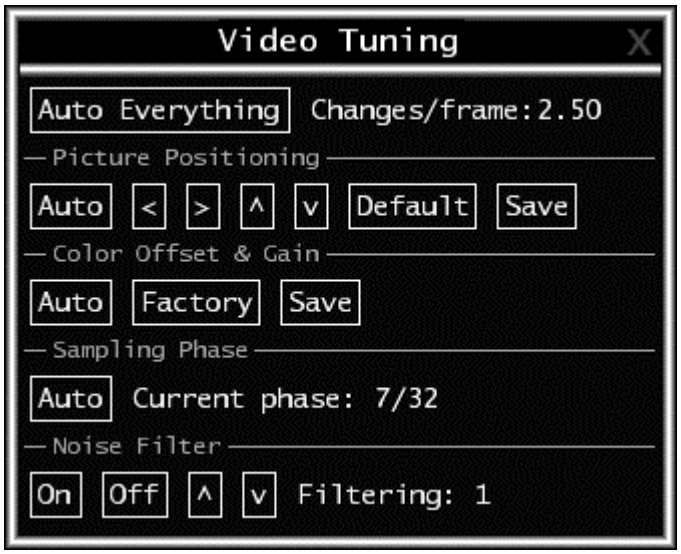
The VirtKeys menu can be left open while using the host system. You can then click the required button at the suitable time, and still interact with the host in a normal fashion.

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**!" page 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 unreliable.

File Transfer/USB Disk Emulation

The KVM control over IP module 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 (1.44M), an 8M 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 KVM control over IP module 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.

Select the "**File Transfer** " page from the home page to setup and control the virtual disk.

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.

Ramdisk mode

Choose the "**Format as Ramdisk** " button to switch to Ramdisk 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 of "**E:**". You can easily ***drag and drop*** files up to 8M 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 page, 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 8M.

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.

RADIUS Authentication

RADIUS may be used to provide the usernames and passwords for accessing the KVM control over IP module. It is configured on the RADIUS page, listed under the “Admin/Setup “ page.

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.

Using the SNMP Interface

The SNMP control/management interface is enabled for read access by default. The initial community string is public. You can define a “read-write” community string from the web interface. Follow the directions given on that page.

The MIB (Management Information Base) you will need is available via a link on the SNMP page. Since the MIB is subject to constant improvement, you may want to check on our company web site for the latest version.

It is possible to change any configuration value, manage user accounts and passwords, configure or disable servers at different port numbers, all via the SNMP agent. Special commands have been provided to reboot and warm restart the system as well.

SNMP Tree Diagram

Here is a tree diagram of the SNMP values that can be queried and controlled. Values that can be changed via SNMP are marked with “RW”. For more information, please consult the MIB.

```
+--dkvm(2)
   |
   +--dkvmConfig(1)
   | |
   | +--dkvmCfgTable(1)
   |    |
   |    +--cfgEntry(1)
   |       | Index: cfgIndex
   |       |
   |       +-- ---- Integer32 cfgIndex(1)
   |       +-- -R-- String    cfgItemName(2)
   |       |        Textual Convention: DisplayString
   |       |        Size: 0..255
   |       +-- -RW- String    cfgItemValue(3)
   |                Textual Convention: DisplayString
   |                Size: 0..255
   |
   +--dkvmStatus(2)
   | |
   | +-- --W- Integer32 dkvmReboot(1)
   | +-- --W- Integer32 dkvmWarmRestart(2)
   | +-- -R-- EnumVal   dkvmHostPower(3)
   | |        Values: Off(1), On(2)
   | +-- -R-- EnumVal   dkvmVideoState(4)
   | |        Values: Okay(1), NoSignal(2), BadMode(3), DPMSStandby(4),
   | |                DPMSPowerdown(5), NoPower(6), Unstable(7)
   | +-- -R-- String    dkvmVideoSummary(5)
   | |        Textual Convention: DisplayString
   | |        Size: 0..255
   | +-- -R-- Integer32 dkvmTemperature(6)
   | +-- -R-- String    dkvmVoltages(7)
   |          Textual Convention: DisplayString
   |          Size: 0..255
   |
   +--dkvmUsers(3)
   | |
   | +--UserTable(1)
   |    |
   |    +--UserEntry(1)
   |       | Index: UserIndex
   |       |
   |       +-- ---- Integer32 UserIndex(1)
   |       +-- -RW- EnumVal   UserStatus(2)
   |       |        Values: existing(1), create(2), delete(3),
   |       |                unused(4), special(5)
   |       +-- -RW- String    UserName(3)
   |       |        Textual Convention: DisplayString
   |       |        Size: 0..255
   |       +-- -RW- String    UserPassword(4)
   |       |        Textual Convention: DisplayString
   |       |        Size: 0..255
   |       +-- -R-- EnumVal   UserIsAdmin(5)
   |       |        Values: RegularUser(1), Administrator(2)
   |       +-- -RW- EnumVal   UserClass(6)
   |                Values: FullAccess(1), ViewOnly(2)
   |
   +--dkvmFactory(4)
   | |
   | +-- -R-- String    firmwareDate(1)
   | |        Textual Convention: DisplayString
   | |        Size: 0..255
   | +-- -R-- String    serialNumber(2)
   | |        Textual Convention: DisplayString
   | |        Size: 0..255
   | +-- -R-- String    MACAddr(3)
   | |        Textual Convention: MacAddress
   | |        Size: 6
   | +-- -R-- String    productName(4)
   | |        Textual Convention: DisplayString
   | |        Size: 0..255
   | +-- -R-- String    productFrom(5)
   | |        Textual Convention: DisplayString
   | |        Size: 0..255
   | +-- -R-- String    productURL(6)
   | |        Textual Convention: DisplayString
   | |        Size: 0..255
   | +-- -R-- String    versionOther(7)
   | |        Textual Convention: DisplayString
   | |        Size: 0..255
```

```
|  +-- -R-- String    versionKernel(8)
|           Textual Convention: DisplayString
|           Size: 0..255
|
+--dkvmPorts(5)
   |
   +--PortTable(1)
      |
      +--PortEntry(1)
         |  Index: PortIndex
         |
         +-- ---- Integer32 PortIndex(1)
         +-- -R-- EnumVal   PortInterface(2)
         |        Values: LAN(1), WAN (2), localhost(3)
         +-- -R-- EnumVal   PortType(3)
         |        Values: TCP(1), UDP(2)
         +-- -R-- String    ServiceName(4)
         |        Textual Convention: DisplayString
         |        Size: 0..255
         +-- -R-- String    ServiceDesc(5)
         |        Textual Convention: DisplayString
         |        Size: 0..255
         +-- -RW- Integer32 CurrentPort(6)
         |        Range: 0..65535
         +-- -R-- Integer32 DefaultPort(7)
                  Range: 0..65535
```

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 KVM control over IP module 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 the KVM control over IP module 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.

Web Server Interface

Here is the current internal web site map:

- System Status
  - Power/Reset Control
  - Java VNC client options
  - Native VNC client
  - Screen Snapshots
  - Other Functions
- Setup and Administration Links
- Non-encrypted VNC login via Java applet
- SSL encrypted VNC login via Java applet
- Background
- Current Status
- Access Current Disk
- Change Disk Type
- CD-ROM ISO Image
- Access Raw Floppy/Ramdisk Images
- Recent system log entries (syslog
- Current Users
- Current Connection
- Network Config
- System Configuration
- Security Profile
  - Administrator Password
  - Idle Session Timeout
  - Internal Firewall Setup
  - VNC Password Policy
- External KVM Switch Brand
- RADIUS Configuration
- Servers
- Machine Name
- Other identification details
  - Location
  - Contact Name
  - Network Address
  - Description
- Network Configuration
  - Dynamic Host Configuration Protocol (DHCP)
    - Current DHCP lease information
  - IP Addresses and Routing
  - Domain Name Server (optional
  - Commit Network Changes
  - Ethernet Address (MAC Address
- Ethernet Bridging
- RADIUS Enabled
- Users and Passwords
  - Current Users
  - Edit User Details
- Set Date and Time
  - Background
  - Current time
  - Change time/date
- Network Servers and Their Port Numbers
  - Main Ethernet Port (DHCP: 10.0.0.30)
  - Secondary Ethernet Port (10.1.0.2)

Internal Firewall

To enhance security, a simple firewall has been included with this product. It can be configured to reject (ignore) all packets from a list of IP addresses, or to accept packets only from hosts in a list. It must be configured from the web interface.

Ethernet Bridging

When Ethernet bridging is enabled, the two Ethernet ports are virtually connected inside the KVM control over IP module. Packets arriving on either port that are not meant for this machine 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.

Firmware Upgrade

The firmware on the KVM control over IP is field upgradable. To upgrade to another version, login as the administrator, and select `**Manage firmware**' from the admin links page.

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: IMPORTANT WARNINGS regarding the upgrade procedure:

- 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.

General Specifications

- Max video mode: 1600x1200 @ 85Hz.
- All VESA standard graphics modes supported are listed below. Any non-standard (non-interlaced) video mode below 1600x1200 @ 85Hz can also be viewed with some impact on image quality and mouse tracking.

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

- Compatible with most enterprise-class KVM switches with on-screen control.
- Max power consumption: 15 watts. (12 VDC, 1.2A)
- Power supply: external AC/DC power supply.
- Supported Operating Systems: Windows NT, 95, 98, 2000, ME, XP, MS-DOS, CPM, Linux, FreeBSD, UNIX and more
- **SV1110IPEXT Connectors:** Video In, PS/2 Keyboard, PS/2 Mouse, USB, LAN Ethernet: 10/100 Base TX, WAN Ethernet: 10/100 Base TX, R-Port (RJ11), DCE Serial DC in (x2 - dual redundant)
- **SV1110IPPCI Connectors:** WAN, LAN, Multifunction breakout cable port (connects to system Video, USB, Keyboard, Mouse & Video)
- Certifications: FCC, CE

Network Protocols

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.
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	Convert text name into IP Address Only used in the URL specification needed to emulate a CD-ROM. Use is optional.

Troubleshooting

Forgotten master password.

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.

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.

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.

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.

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.

None of these warnings affects the encryption offered and eavesdropping is still impossible. However, they do limit your protection against a so-called `man in the middle' attack. In most situations, there are many other technical reasons why such an attack is not possible anyway.

Don't set LAN and WAN to the same IP Address.

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.

Index

FCC Statements

SV1110IPPCI

FCC Statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference and

(2) This device must accept any in interference received, including interference that may cause undesired operation.

Note: *This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.*

Warning: Changes or modifications not expressly approved by StarTech.Com could void the user's authority to operate the equipment.

SV1110IPEXT

FCC Statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference and

(2) This device must accept any in interference received, including interference that may cause undesired operation.

Note: *This equipment has been tested and found to comply with the limits for a Class B digital devices, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.*

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of more of the following measures:

- *Reorient or relocate the receiving antenna*
- *Increase the separation between the equipment and receiver*
- *Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.*
- *Consult the dealer or an experienced radio/TV technician for help*

Warning: Changes or modifications not expressly approved by StarTech.Com could void the user's authority to operate the equipment.

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 card.

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 9:00AM to 5:00PM 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 below, 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 of StarTech.com Ltd. and StarTech.com USA LLP (or their 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 or 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.