

SERVER REMOTE CONTROL

Secure Server Remote Control with Web Interface
and Integrated Digital KVM Switch

SV441HDI
SV841HDI
SV1641HDI

Instruction Guide



* Actual product may vary from photo

StarTech.com



Table of Contents

INTRODUCTION	1
FEATURES	1
BEFORE YOU BEGIN	1
Required Cables and Hardware	1
INSTALLING THE SERVER REMOTE CONTROL	2
Disabling Mouse Acceleration on the Managed Computers	3
NETWORK CONFIGURATION METHODS EXPLAINED	3
Web Configuration Using DHCP	4
Terminal Configuration Using a Serial Cable	4
CONFIGURING THE KVM FOR YOUR NETWORK	6
Using the Web Interface	6
Using the Terminal Interface via Serial Port	12
ACCESSING THE VNC INTERFACE	13
Web Interface	13
Native VNC Client	14
SSH Tunnel (with Native VNC client)	15
USING THE VNC MENU	15
Welcome Window	16
Bribar Feature	16
Main Menu	18
VirtKeys Menu	19
Video Tuning Menu	19

ACCESSING KVM FEATURES	22
Cascade Configuration	22
OSD Operations	23
Hot Key Commands	27
Changing Your Configuration	28
TROUBLESHOOTING	29
SPECIFICATIONS	31
SUPPORTED PROTOCOLS	32
SUPPORT AND WARRANTY INFORMATION	33
REGULATORY COMPLIANCE STATEMENTS	33
APPENDIX A: ABOUT SECURITY CERTIFICATE WARNINGS	34
APPENDIX B: USING THE ADVANCED VIDEO TUNING FEATURE	35
APPENDIX C: GETTING PEAK PERFORMANCE	37
APPENDIX D: THE IPMI UPGRADE OPTION	38
APPENDIX E: THE MODEM OPTION UPGRADE	45
APPENDIX F: USING OPTIONAL R-PORT DEVICES	51

NOTE: Since firmware for our Server Remote Control Products is constantly evolving to offer more functionality and improvements, some of the options and instructions presented in this manual may differ from your unit. To obtain the latest documentation and support information for this product, please visit www.startech.com.

4 August 2004 (Rev. A)

Introduction

Thank you for purchasing a StarTech.com SVx41HDI series Server Remote Control with integrated KVM. Using the Internet or your TCP/IP enabled network, you can now remotely monitor and control critical PC servers and workstations using an industry-standard Web browser or VNC client.

Features

- Supports industry-standard networking and management protocols such as TCP/IP and SNMP
- Offers secure management options including SSL encryption, SSH tunneling, and RADIUS authentication
- Platform independent: can be managed using any Java-enabled Web browser
- One remote management point for multiple computers

Before You Begin

This section describes the cables and other hardware that you may wish to use when setting up and configuring your new Server Remote Control. We suggest you review this section carefully before beginning the installation process.

Contents

Your package should contain the following:

- 1 x SVx41HDI Server Remote Control unit
- 1 x Power adapter
- 1 x Instruction Guide
- 1 x Rack Mount screw kit
- 1 x DB9 RS-232 null modem serial cable

Required Cables and Hardware

Depending on your needs, you may need one or more of the following cables:

All applications

- 1 x Straight-through Ethernet patch cable (connects unit to your LAN)
StarTech.com part number: M45PATCHxxxx
- StarTech.com PS/2 3-in-1 KVM Cables (1 for each managed computer connected via PS/2)
StarTech.com part number: SVECONxx
- StarTech.com USB 3-in-1 KVM Cables (1 for each managed computer connected via USB)
StarTech.com part number: SVECONUSxx

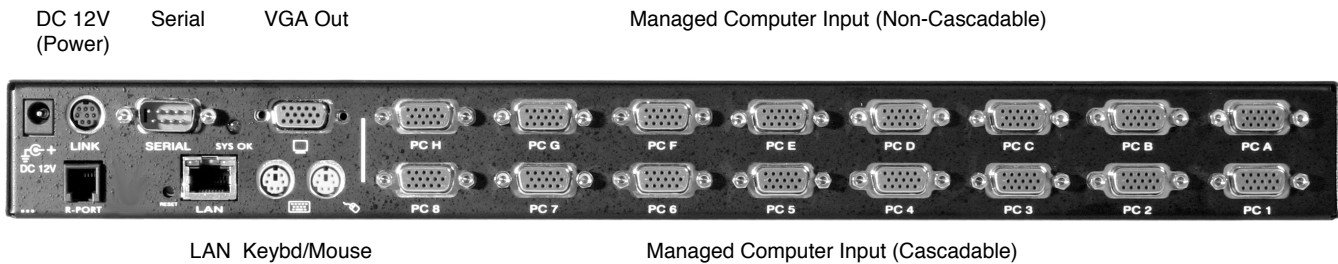


SVECONxx



SVECONUSxx

Installing the Server Remote Control



NOTE: The instructions here and elsewhere in the manual refer to port designations of the SV1641HDI, the 16-port version of the Server Remote Control. For other versions, note the following:

SV841HDI: Ports **PC A~H** = Ports **PC A~D** and Ports **PC 1~8** = **PC 1~4** on your product

SV441HDI: Ports **PC A~H** = Ports **PC A~B** and Ports **PC 1~8** = **PC 1~2** on your product

The restrictions on functions such as cascading and the assignment of master and slave units also apply to all versions of the product.

1. Ensure that the Server Remote Control unit and the computers to be managed are powered off.
2. If desired, mount the unit in a standardized rack or cabinet.
3. Connect a standard straight-through Ethernet patch cable to the **LAN** port on the rear panel of the unit.
4. Connect the opposite end to your network hub, switch, or terminated wall outlet.
5. If you wish to use the product as a local console, connect a standard keyboard (purple connector) and mouse (green connector) to the PS/2 ports, as marked on the rear panel.
6. Connect a VGA monitor to the video-out port on the rear panel of the unit.
7. (a) **If you are using PS/2 connections to your managed computers**, connect the end of the SVECONxx cable that has three connectors (keyboard, video, mouse) to the keyboard, mouse, and VGA Out ports on a computer (often a server or other critical system). Connect the opposite end (with a single VGA-style connector) to one of the **PC A~H** or **PC 1~8** ports on the rear panel of the Server Remote Control. Repeat this procedure for each PS/2-enabled managed computer. You will be able to add additional managed computers later with the Server Remote Control powered on.
 (b) **If you are using USB connections to your managed computers**, connect the end of the SVECONUSxx cable that has two connectors (USB, video) to an available USB port and VGA Out port on the computer (often a server or other critical system). Connect the opposite end (with a single VGA-style connector) to one of the **PC A~H** or **PC 1~8** ports on the rear panel of the Server Remote Control. Repeat this procedure for each USB-enabled managed computer. You will be able to add additional managed computers later with the KVM powered on.

8. Power on the Server Remote Control by connecting the AC adapter to a suitable power source and connecting the opposite end to the **DC 12V** port on the rear panel of the unit.
9. Power on each of the managed computers, observing normal startup procedures.

NOTE: You can choose to mix managed computers connected via PS/2 and USB connections as necessary with no impact on features or functionality.

NOTE: Steps 5 and 6 are necessary only if you wish to have the ability to manage the KVM and its computers locally (i.e. not over the Internet or LAN). While not required, adding these devices is highly recommended for ease of administration.

NOTE: The KVM also has the ability to “cascade” multiple KVMs to increase the total number of possible managed computers. If you wish to take advantage of this feature, refer to the section “Cascade Configuration” in this manual.

Disabling Mouse Acceleration on the Managed Computers

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 unit and should be disabled on the managed computers before a remote session is attempted. Follow the instructions below to disable mouse acceleration for the operating system installed on each managed 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

Network Configuration Methods Explained

The Server Remote Control offers two 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.

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 **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:

DHCP Client Log ?		
DHCP Client Log View your LAN client's information that are currently linked to the Broadband router's DHCP server.		
Numbers of DHCP Clients: 3		
ip=192.168.22.3	mac=00-03-93-D1-D7-18	name=stpcpm18
ip=192.168.22.4	mac=00-0E-C5-00-08-1A	
ip=192.168.22.5	mac=00-00-39-03-56-D6	name=STPCMOBILE01

The information displayed for your own network may vary significantly from the data displayed in the 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 unit 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 Server Remote Control 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 unit. **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 unit switch and wish to proceed with the Web configuration, do not power off the unit or your DHCP server, since it might lease a different IP address. Should this happen, re-examine the DHCP log to verify the IP address again.

Terminal Configuration Using a Serial Cable

Configuring the unit 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. or are not using DHCP on your network. 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 Server

Remote Control, you can use any typical communication software package (**UNIX:** tip, cu, kermi, minicom; **Windows:** HyperTerminal, kermi).

Using the DB9 female-to-female null-modem serial cable (provided) connect one end of the cable to the **SERIAL** port on the rear panel of the SVx41HDI. Connect the opposite end 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

Flow Control: None

Configuring the KVM for Your Network

NOTE: As firmware for this product evolves, some of the menu options may change and therefore these screenshots and instructions may differ slightly from the options displayed on your screen.

Using the Web Interface

The Web interface is the most intuitive way to configure the Server Remote Control. It also offers a Java-based VNC client that you can use to control the managed computers from a remote location. The unit 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 unit 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) the address you configure through the terminal via a serial cable (see the section “Using the Terminal Interface via Serial Port” for more information).

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**.



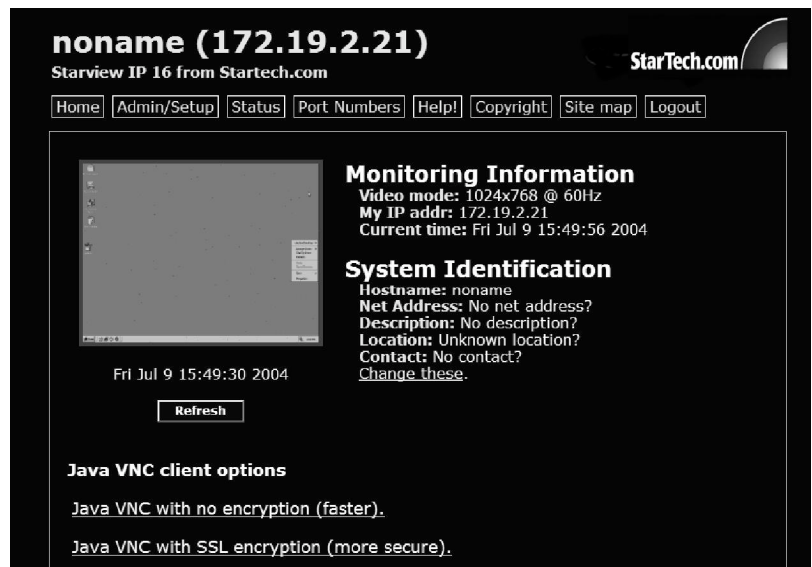
NOTE: Before the login screen appears, your Web browser may display a warning about an invalid security certificate. This does not affect the security of your data in any way. **Whenever you are prompted about a certificate security problem by your browser or the Java VNC client, always choose the option 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 unit, view essential system information, and capture screen shots from the managed computers. Second, it is where you can start the integrated Java VNC client to interact with the managed computers 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 Server Remote Control. Each of the options is explained in detail here.



Network Configuration (IP address, netmask, gateway)**Dynamic Host Configuration Protocol (DHCP)**

Automatic network configuration using DHCP is: **Enabled/Disabled**.

This feature applies 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.

Network Configuration

Please note: You are viewing this page over the network, so these values are probably very close to what you want. Make changes here with great caution.

[View/debug current network setup values here..](#)

Dynamic Host Configuration Protocol (DHCP)

Automatic network configuration using DHCP is: **Disabled**

IP Addresses and Routing

These values will only be used if DHCP is disabled.

Port	IP Address	Subnet mask	Default Gateway (or 0.0.0.0 for none)	Broadcast (or leave blank)
LAN	172.19.2.21	255.255.0.0	172.19.1.7	172.19.255.255

Domain Name Server (optional)**IP Addresses and Routing**

This table allows you to assign IP information for the **LAN** port. 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.

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 unit so the new settings take effect immediately.

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

Users and Passwords**Current Users**

Click on a user's name to edit his or her settings (see below).

Create a new user by filling in the form values, and choosing appropriate button below.

#	Username	Password	Delete user
	(None yet)		
1	tester	*****	Delete

Edit User Details

Select a user name from the above list (click on their name), then edit the values shown in this form. Leave 'password' empty to leave the password unchanged.

Username:
 Password:

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.

Change system identification

Provides details about this unit 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.

Security policy, internal firewall and admin 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 prevent the chance for error.

Security Profile

Administrator Password

This is the administrator (or root, superuser) password. You must have used it to get here.

The administrator's password can be changed here. However, the user name for this account cannot be changed: The system will accept either 'root', 'admin', or 'administrator' as the name of this account. [Add or change other user accounts here.](#)

Admin password:

Setup compatibility with host system, external power bar.

This menu allows you to configure the unit for use with products such as the StarTech.com Serial Control Power Switch and locale-specific items such as a non-English keyboard. When the StarTech.com 8-outlet Serial Power Console Switch is selected as the external power bar, additional menu choices will appear on the main page of the Web interface. See the documentation for the StarTech.com Serial Control Power Switch for more details on how to access and configure this feature.

Keyboard Mapping (for localization)

In many parts of the world, the keyboard has extra keys and/or different layout to better suit the local language than the default US/English layout. If your host O/S is expecting a keyboard of a special type, choose it here.

If the wrong value is used here, special language keys will not work, and some basic symbols (such as ") may not even work correctly. The key layout of the "remote" keyboard must match the key layout of the "local" keyboard defined here.

Select keyboard layout:

External Power Bar

Connect a remote power control device to the serial port, and choose the model from the list below.

You will typically require a null-modem cable to connect between this device and the power bar (DCE to DCE).

Once enabled, a status and control area will appear on the [main web page](#). Individual ports can then be controlled and monitored.

Select model:

Port numbers to be used for different services.

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

Debug network setup values and routing.

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

SNMP agent setup and configuration.

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

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. Additional RADIUS challenges may be demanded depending on the RADIUS server in use. This allows operation with hardware tokens and other advanced authentication devices.

External Serial consoles setup and control.

The StarTech.com Server Remote Control product line offers a

RADIUS Configuration

Use RADIUS for login purposes:

Servers

Each of these servers will be tried in order until a valid Access-Accept or Access-Reject message is received. Use zero in the IP address to disable a server.

RFC 2138, which defines the RADIUS protocol, indicates that UDP port number 1812 should be used for RADIUS. However, many deployed systems still use port 1645 instead.

Priority	Server IP Address	Port	Shared Secret	New Secret (twice)
#1	0.0.0.0	1812		
#2	0.0.0.0	1812		
#3	0.0.0.0	1812		

Request timeout period (seconds):

Number of retries (per server):

Click here to save your RADIUS changes and apply them:

Serial Consoles Attached

#	Name / Description	Baud (bps)	Mode	Force DCD	Console Log	Connect...
	No units are attached. Plug them in now.					

Notes

- All common baud rates between 300 and 115,200 bps are supported.
- Hardware handshaking (CTS/RTS) is required at speeds over 9600bps. It is always enabled here, but your serial device may require setup to enable handshaking on the other end of the connection.
- The following character modes are supported:
 - 8N1 - Eight bits, no parity, one stop bit (default and most common).
 - 7N1, 7O1, 7E1, 7M1, 7S1 - Seven bits, (none, odd, even, mark, space) parity, one stop bit.
 - 8N1, 8O1, 8E1, 8M1, 8S1 - Eight bits, (none, odd, even, mark, space) parity, one stop bit.
 - 8N2 - 8 bits, no parity, two stop bits.
- "Force DCD" means to keep Carrier Detect signal active at all times. Normally DCD is asserted when a new user connects, and dropped when the last user disconnects.

number of additional accessories that enhance the flexibility of this product, called R-Port Devices. This screen allows you to view and manage these devices. For more information on accessories available for the Server Remote Control see Appendix F, contact your local dealer or visit **www.startech.com** for more information.

Set date and time.

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

Firmware and flash memory management.

The firmware on the Serial Remote Control is field upgradeable. To upgrade to another version, login as **admin**.

Auto Self Upgrade

The unit 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 **Upgrade** 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. You may also choose **Reboot Myself** at the bottom of the screen to restart the unit without powering on and off.

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.

CGI Component	04.27.4172125
Linux Kernel	Linux version 2.4.20-pre7 #130 Mon Mar 8 09:37:36 EST 2004
System FPGA	3 Upgrade
Software options	00000007 (ENT, SEC, MULTI)

Unit Numbers

Name	Value
System serial number	00001226
Ethernet MAC Address (LAN)	00:0e:c5:00:09:94

Auto Self Upgrade

Click here to upgrade system firmware to the latest version available over the Internet. The appropriate file will be downloaded and installed automatically (if possible).

Click here to just download the appropriate file. You must then upload the same file to this unit (see next section).

- 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 Server Remote Control.

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.

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 unit. 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**. When you have made any necessary changes, click **Commit Changes** to use the settings the next time the unit restarts. To force the unit to restart immediately, click **Restart Servers**.

Network Servers and Their Port Numbers

These tables show **all** network servers running on this machine. For security reasons, some services may be disabled, or moved to non-standard ports.

To disable a service, change its port number to zero (0). Valid port numbers range from 1 to 65535. Only a single server can use a particular port number on the same IP address (ie. all port numbers must be unique in each table below).

LAN: Main Ethernet Port (DHCP: 192.168.22.4)

Service	Description	Default	Current Port
ssh	Secure Shell	22	22
http	Web redirector (to https)	80	80
snmp	SNMP Agent (UDP)	161	161
https	SSL Encrypted web control	443	443
vnc	VNC/RFB Protocol Server	5900	5900
vnscs	SSL-tunnelled VNC	15900	15900

Help! Menu

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

Copyright Menu

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

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 Server Remote Control.

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 unit. While not intended to be a substitute for the Web interface, it does allow you to configure some of the same functions. The following menu list describes the options that can be modified through the terminal interface. Note that you must use the **W** option to confirm and apply any changes you make before exiting the terminal session.

```

-----
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:c5:00:09:94)
D.H.C.P.: Disabled
IP Address: 172.19.2.21
Netmask: 255.255.0.0
Gateway: 172.19.1.7
Broadcast: 172.19.255.255

Machine name: noname

Commands (press one key, then Enter):
D - Enable DHCP for dynamic IP address.
I - Set IP address.
N - Set netmask.
G - Set default gateway.
B - Set broadcast address (optional).
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.

Choice:

```

Accessing the VNC Interface

There are three ways to communicate with the Server Remote Control in order to control the managed computers:

- **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.

NOTE: The first time the Server Remote Control is accessed, it defaults to the **PC 1** port on the master switch as the default managed client to display. If there is no computer/slave KVM connected to that port, you will see a blank screen until you switch to a port with an active managed computer. For future sessions, the unit will default to the last port accessed when beginning a VNC session, assuming the unit has not been upgraded or reset.

Web Interface

The Java-based VNC client that is integrated into the unit'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 unit 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** on the keyboard.

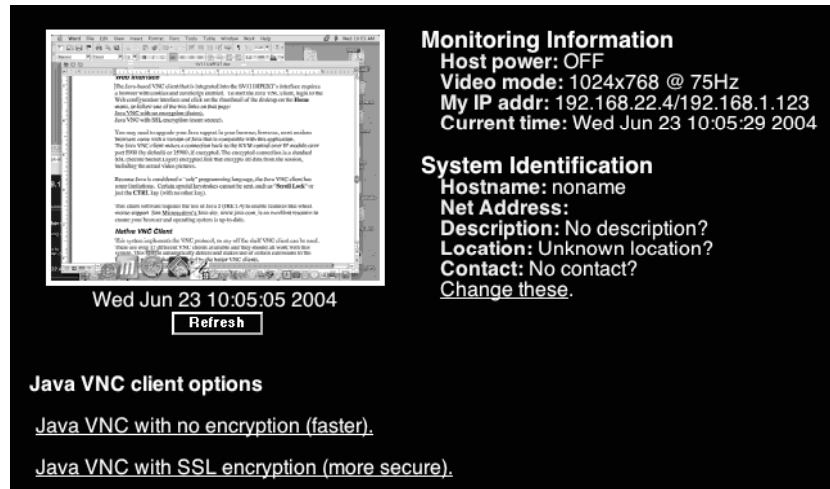
This client software requires the use of Java 2 (JRE 1.4) to enable features like wheel mouse support. Sun Microsystems’s Java site, www.java.com, is an excellent resource to ensure your browser and operating system is up-to-date.

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.



Monitoring Information
 Host power: OFF
 Video mode: 1024x768 @ 75Hz
 My IP addr: 192.168.22.4/192.168.1.123
 Current time: Wed Jun 23 10:05:29 2004

System Identification
 Hostname: noname
 Net Address:
 Description: No description?
 Location: Unknown location?
 Contact: No contact?
[Change these.](#)

Java VNC client options
[Java VNC with no encryption \(faster\).](#)
[Java VNC with SSL encryption \(more secure\).](#)

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
```

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 KVM without using the Web interface or a custom client.

The commands you send through this interface (i.e. restart) will be sent to the managed computer currently active on the Server Remote Control. It is advisable to verify which managed computer is active before making any changes. We strongly recommend you thoroughly familiarize yourself with the information here and in the next section (“Accessing KVM Features”) before undertaking any critical tasks through the VNC interface.

Welcome Window



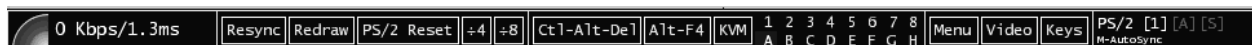
When you initially connect to the system, a window similar to this one will be shown.

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 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 Reset: Resets the PS/2 keyboard and mouse emulation. Useful to recover failed mouse and/or keyboard connections.

÷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).

1~8, A~H: Switches the current view to the specified KVM port. This function works for the master unit only. Use the **KVM** menu (see below) to access KVM functions on a slaved unit.

KVM: Sends the KVM “hotkey” sequence. This function is equivalent to pressing the left control key on the keyboard three times to access the KVM on-screen display.

Menu: Shows the main menu.

Video: Shows the video-tuning menu where the picture quality can be adjusted.

Keys: Shows the **VirtKeys** menu, which allows you to simulate pressing special keys such as the Windows key or complex multi-key sequences.

PS/2: This area will show either **PS/2** (as in the example) or **USB** to indicate if keyboard and mouse are being emulated via USB connection or PS/2 signals.

M-Autosync: Shows when the mouse autosync feature is enabled. When active, the unit will automatically attempt to match the positions of the remote mouse pointer and the VNC session’s (local) mouse pointer on the screen (recommended).

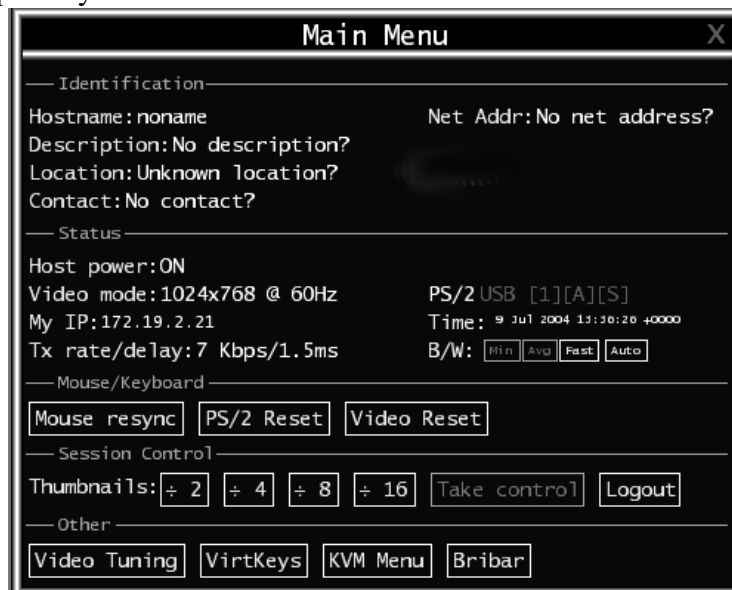
[1][A][S]: These flags show the state of the keyboard lights, **NumLock**, **ShiftLock** and **ScrollLock** respectively.

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:

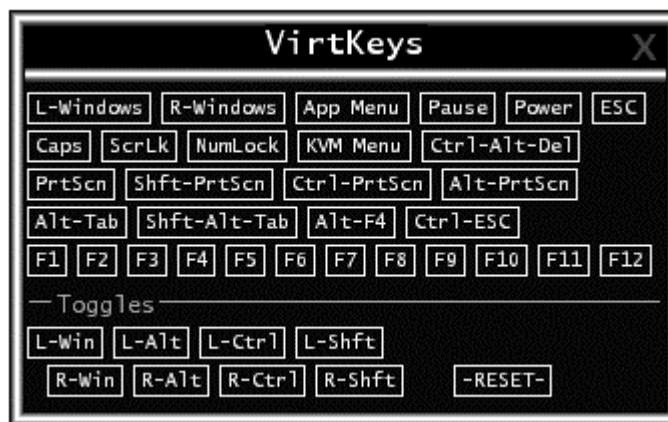


The main menu window may be moved by clicking and dragging on the title bar. It can be closed by pressing **Escape**, or by clicking on the red **X** in the top right corner.

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 label that is defined by the user in the Web interface. This does not affect the operation of the system and is intended to assist with administration.
- **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.
- **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 (see below).
- **KVM Menu:** Allows access to the menus on a slave KVM unit.
- **Bribar:** Closes or reopens the Bribar window along the bottom of the screen.



VirtKeys Menu

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.

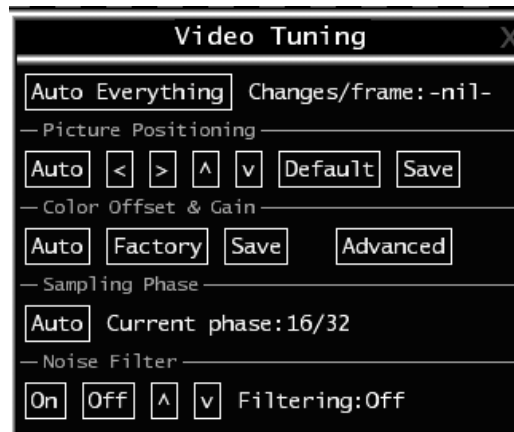
The VirtKeys menu can be left open while using the host system. You can then click the required button at the suitable time, and still interact with the host in a normal fashion.

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 will 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 managed 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. true color). 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 recognize the test pattern.

Pressing the **Advanced** button will open the **Advanced Video Tuning** menu. While the vast majority of users will not need to adjust these settings, it offers a high-degree of control of the video settings of your VNC sessions. See Appendix B for more information on this feature.

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.

Accessing KVM Features

Once you can access and configure the networking component of the Server Remote Control, you can use it to select and control the managed computers connected to it. This section describes how to add additional KVM switches to the master unit for greater flexibility, and how to use the on-screen display (OSD) system to manage your computers. Once you have established a VNC session with the SVx41HDI, you can access the KVM features as though you were at a local console.

Cascade Configuration

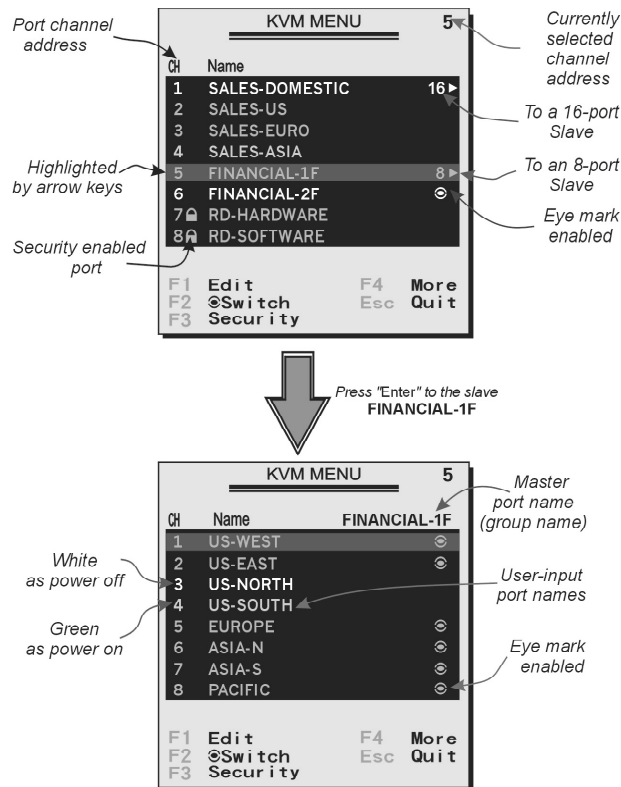
You can connect a second level of KVMs to one or more of your Master Server Remote Control's **PC x** ports. The KVM switches connected to the Server Remote Control (the "Master switch") are known as Slaves. Once connected, the units will automatically configure themselves as either Masters or Slaves. You can only connect an equal or "smaller" KVM to the Master: a 16-port master Server Remote Control switch can have both 16-port and 8-port KVM slaves, an 8 port Master Sever Remote Control switch can have 8-port and 4-port Slaves, and so on.

For example, the 16-port unit can support 136 computers, with 8 16-port Slave KVMs, each connected to 16 computers. The Slave KVMs must be connected to the **PC 1~8** ports, not the **PC A~H** ports.

To cascade your KVMs, use a 3-in-1 PS/2 KVM cable to connect one of your Master switch's PC ports to the Slave switch's **PC 1~8** ports. When turning on your cascaded switches, turn on the Master switch before turning on any of the others.

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 (below) showing a list of the computers with corresponding channel addresses, names and status.



- The port number (or channel address) of the currently selected computer is displayed in red in the top right of the screen.
- The device name is green if the device has power and is ready for selection or white if it has no power. The OSD menu automatically 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.
- Press <ESCAPE> to exit the OSD menu and remove the OSD menu from the screen.
- A triangle mark on the right side of the screen indicates the port is cascaded to a Slave KVM; the number at the left of the triangle mark shows the number of ports the Slave has. With that port highlighted, press <ENTER> to bring up a screen listing the computers connected to that Slave. The name of the Slave KVM will be shown at the upper right corner of the OSD menu.
- An eye mark on the right side of the screen indicates that the computer has been selected to be monitored in Scan mode. You can switch this mark on and off using function key <F2>.

- Press <ESCAPE> to exit the OSD and to return to using the selected computer. The computer name is shown on the screen.

OSD Function Keys

You can use the function keys when the OSD menu is active.

Function key <F1>

Edits the name of a managed computer or a Slave KVM. First, use the <UP> and <DOWN> arrow keys to highlight a channel then press <F1> followed by name entry. Your name can be up to 14 characters long. Valid characters are A to Z, 0 to 9, and the dash character. Lowercase letters are converted to uppercase. 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>

Marks a computer to be scanned by switching the eye mark on or off. First, use the <UP> and <DOWN> arrow keys to highlight the device, then press <F2> to switch its eye mark on or off. If Scan Type is Ready PC + Eye (see Function key <F4>), only the powered and eye-marked computers will be displayed in Scan mode.

Function key <F3>

Locks a device (a computer or a Slave) from unauthorized access. 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 beside 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>. Enter the password and you can access the device. The device is automatically re-locked once you switch to another device. During Scan mode, OSD skips the security-enabled device.

Function key <F4>

More functions are available by hitting <F4>. A new screen pops up displaying the functions 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 function and press <ENTER>. Available options will be shown in the middle of the screen. To select an option, use the <UP> and <DOWN> arrow keys then press <ENTER> to select the options. You can press <ESCAPE> to exit at any time.

Auto Scan

In this mode, the KVM automatically switches from one powered 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 Auto Scan mode, press the left <CTRL> twice. 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. Scan Rate (<F4>: More\Scan Rate) sets the display interval when a computer is selected before selecting the next one.

Manual Scan

Scans through powered computers using 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

A multimedia module can be LINKed to the back of each KVM 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. Off mode 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.

(Note: This is an **optional** feature requiring a separate device to be connected to the master switch.)

Scan Type

Ready PC + Eye: In Scan mode, scans through only powered computers that are eye-marked selected.

Ready PC: In Scan mode, scans through all powered 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

The KVM offers a keyboard typematic setting that overrides the typematic settings in the BIOS and Windows operating system. 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

You can choose where the selected computer name and/or OSD status is displayed on your screen during operation. The actual display position shifts due to different VGA resolutions: 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.

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.

Left Ctrl refers to the <CTRL> key located at the left side of the keyboard.

1~8/A~H refer to the number keys 1 to 8 at the upper row of the keyboard (Do not use the keypad at the right of the keyboard) and character keys A to H (case insensitive).

Selecting a Computer

To select a computer by hot-key command you need to know the device's channel address, which is determined by the KVM connection. For a computer connected to the Master switch, the address is represented by the PC port number (**1~8** or **A~H**). For example, to access the PC plugged into port 7 of the Master KVM switch, type:

left Ctrl + left Ctrl + 7

For a computer connected to a Slave KVM, you need to know the channel address of the Slave unit (**1~8**) and then the channel address of the device (**1~8** or **A~H**). (Please note that only Master's **PC 1** to **PC 8** ports can be connected to a Slave.) For example, to access the computer plugged into port C of a Slave KVM Switch that is plugged into Port 6 of the Master switch, type:

left Ctrl + left Ctrl + 6 + C

Auto Scan

Auto Scan automatically scans through powered computers at a fixed interval:

left Ctrl + left Ctrl + F1

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. The length of the Auto Scan interval (Scan Rate) is adjustable (see **Scan Rate** on the following page). To abort the Auto Scan mode, press the left Ctrl key twice.

NOTE: The **Scan Type** setting will determine whether computers must be eye-marked to be included in the scan. See page 25 for details.

Manual Scan

Manual Scan enables you to manually switch back and forth between powered computers:

left Ctrl + left Ctrl + F2

Press the up or down arrow to select the previous or next computer in sequence. Press any other key to abort the Manual Scan.

NOTE: The **Scan Type** setting will determine whether computers must be eye-marked to be included in the scan. See page 25 for details.

Scan Rate

Scan Rate sets the duration between switching to the next computer in Auto Scan mode:

left Ctrl + left Ctrl + F3

The unit switches between scan intervals of 3, 8, 15 and 30 seconds.

Keyboard Typematic Rate

You can adjust the keyboard typematic rate (given in characters/sec). This setting over-rides the keyboard typematic rate of your BIOS and any operating system.

left Ctrl + left Ctrl + F4

The unit switches between rates of 10, 15, 20 and 30 characters/sec.

Audio Stick

A multimedia module can be LINKed to the back of the master KVM 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

(Note: This is an **optional** feature requiring a separate device to be connected to the master switch.)

Changing Your Configuration

After the initial power up, any device (either a KVM or a PC) can be added or removed from any **PC x** port on the KVM without having to power down the Master KVM Switch. Make sure that devices are turned off before connecting them to the Master KVM switch.

Note: After changing your configuration, the OSD will automatically update to reflect the new configuration.

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.

Mouse does not work.

Make sure there is only one mouse driver installed in each computer.

Monitor works, but keyboard and mouse do not.

Make sure you haven't swapped the keyboard and mouse cables

VGA image is not clear.

You may be using poor quality VGA cables. Make sure you are using UL-2919 rated, double-shielded VGA cables.

No OSD screen or screen image.

You may have selected a power-off computer. Use the pushbuttons or to select a computer that is turned on.

There is a keyboard error on boot.

You may have a loose keyboard connection. Make sure your keyboard cables are well-seated.

The letters on the TFT LCD display are blurry or have shadows.

You may have improper resolution settings. Under the Control Panel, set the VGA output of your computers to match the highest resolution of the LCD monitor with Large Font selected.

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. Make sure that you have removed all power sources from the Slave unit before connecting it to the Master switch.

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

Make sure more than one computer is turned on. Manual Scan only works with powered computers. Check the Scan Type (from the OSD menu) and make sure you have selected the proper computers.

Auto Scan does not work.

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 or press any front pushbutton 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 **PC 1 to PC 8** can be connected to Slaves, even if the Master switch has 16 PC ports.

Keyboard strokes are shifted.

Press both Shift keys.

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” option, 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. For more details, refer to Appendix A, “About Security Certificate Warnings.”

Specifications

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	18 watts (13.5 VDC, 1.8A)
Input Connectors	Video In (for local console) PS/2 Keyboard (for local console) PS/2 Mouse (for local console) LAN RJ-45 R-Port (RJ11) DB9 RS-232 Male (DTE) DC in SV441HDI: 4 x HD15 (female) Integrated KVM Cable Input SV841HDI: 8 x HD15 (female) Integrated KVM Cable Input SV1641HDI: 16 x HD15 (female) Integrated KVM Cable Input
Regulatory Certifications	FCC Class A, CE

Supported Protocols

<i>Service</i>	<i>Description</i>	<i>Benefits</i>
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	Converts text name into IP Address Only used in the URL specification needed to emulate a CD-ROM. Use is optional.

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>

Regulatory Compliance Statements

This device complies with part 15 of the FCC Rules for a class A digital device 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.

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 SVx41HDI?

As it redirects you 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 SVx41HDI. 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 Server Remote Control any more vulnerable to outside attacks.

Can I prevent the warning from occurring?

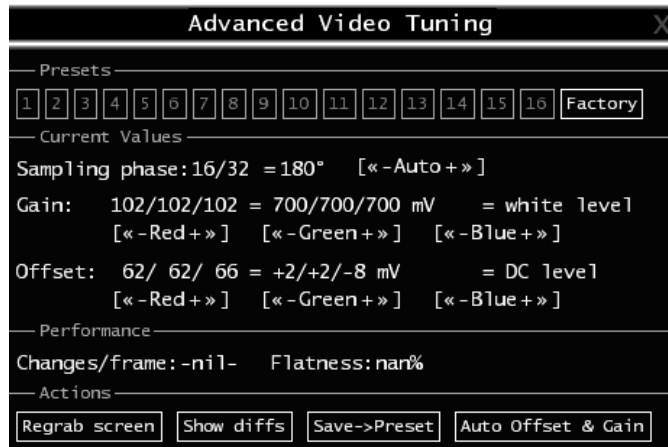
Yes. You have two options that may prevent the warning from occurring. First, if the Web browser you are using offers the option to ignore the warning for future visits, the browser will no longer generate a warning if that option is selected. Second, if you install the certificate from the KVM onto the remote 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 instructions detail how to install the certificate from the SVx41HDI onto your local computer (in this case, running Windows XP and Internet Explorer).

1. Open your Web browser and go to the KVM 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.

Appendix B: Using the Advanced Video Tuning Feature



The **Advanced Video Tuning** menu allows you to adjust the qualities of the video in your VNC sessions, and can be accessed by clicking the **Advanced** button on the **Video Tuning** VNC menu. While many users will probably allow the SVx41HDI to automatically configure the video properties, you can use this menu to exercise a great deal of control over the settings if you wish.

The **Presets** section contains up to sixteen different settings plus the factory setting. If a number is highlighted, as in the example shown, then that preset has been programmed with valid settings and may be used. Note that the **Factory** preset is always available. Simply click on the appropriate button and those settings will be restored.

To save settings to a preset, click on the **Save->Preset** button in the **Actions** pane. The preset buttons will highlight. Click the desired preset button to save the values. Note that any previous settings assigned to that button will be lost. If you do not wish to save the presets after clicking the **Save->Preset** button, click the **Save->Preset** button a second time and the save function will be canceled.

The section of the screen marked **Current Values** indicates the various video parameters that can be adjusted. For each parameter, there are a series of buttons: [, <<, -, **Auto**, +, >,]. The '[' and ']' buttons set the parameter to its smallest value or largest value, respectively. The '<<' and '>>' buttons decrement or increment the parameter by a large amount. In the case of phase, this is 4 units. For all the others, this is 10 units. The '-' and '+' buttons decrease or increase the parameter by one unit. The middle button sets the parameter to the middle value. The text of the middle button also indicates which parameter is being controlled. Note that in the case of phase, the middle button invokes the auto-phase algorithm.

The **Performance** section of the screen gives an indication of the quality of the video. **Changes/frame** is the average number of tiles that change for each frame sampled by the hardware. **Flatness** is an indication of what percentage of the screen contains tiles that are comprised of only one color.

The **Regrab Screen** button in the **Actions** section causes the screen to be re-captured. When making small changes to the video parameters, sometimes these changes are not reflected in the

displayed screen immediately, particularly if the noise filter is enabled. Press this button to see the immediate effect of the changes.

Use the **Show Diffs** button to learn which parts of the screen are being sent over the Internet. When you click this button, the screen is cleared to a medium grey color. All blocks that are sent from that point on will show up on the screen as they are sent. Click the button again to reset the screen to grey. To return to normal operation, click the **Regrab** button. It is very easy to visually identify the effect of noise on the signal processing using this feature.

The **Auto Offset & Gain** button in the **Actions** section invokes the automatic algorithm for setting the video parameters. The algorithm requires the factory calibration test pattern to be correctly displayed on the screen.

Appendix C: 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 Server Remote Control 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 KVM 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**.

Appendix D: The IPMI Upgrade Option

Background

To offer a more complete remote server control solution, the SVx41HDI offers an optional power management feature that allows remote hardware restarts and the ability to power the a managed computer on and off. You may be able to take advantage of this feature if the computer you are managing supports IPMI (Intelligent Platform Management Interface). Note that only one managed computer can use this feature at any one time.

Managed Computer Requirements

The managed computer must support the IPMI standard version 1.5 to use this option. Most popular server motherboards now support the IPMI standard. To determine if your computer supports this IPMI, consult its documentation for more information.

IPMI is used to configure and control a device on the motherboard called the BMC (Baseboard Management Controller) using a dedicated serial port. Once the computer is configured for IPMI management, the serial port on the managed computer is normally reserved by the BIOS solely for that purpose and cannot be accessed or recognized by the operating system. It is therefore unlikely that a serial port provided by an add-in card will be able to act as an IPMI port, so you must use a serial port integrated on the motherboard of the managed computer. If the computer you are managing only has a single serial port, you must add an additional port (or ports) via an add-in card if you need a serial port for other purposes (i.e. modem). Enabling IPMI support usually requires enabling options in the managed computer's BIOS setup software, and the instructions will vary considerably from make to make and model to model. Normally, a password will be created by the BIOS that allows the IPMI feature to be accessed; this password is exclusive to the IPMI feature and does not correspond to a password or account in the managed computer's operating system.

If the Managed Computer Does Not Support IPMI

If the managed computer you wish to monitor with the SVx41HDI does not support IPMI, StarTech.com offers a non-IPMI solution that also works via serial port and acts as a power concentrator and a power management device: the 8 Outlet Serial Power Console and Switch (PM815NAS). For more information about this product, visit www.startech.com or contact your local StarTech.com dealer.

Activating the IPMI Option

Version Numbers

Component	Version / Release
System firmware	Thu Jul 8 17:28:01 EDT 2004
CGI Component	04.27.4172125
Linux Kernel	Linux version 2.4.20-pre7 #130 Mon Mar 8 09:37:36 EST 2004
System FPGA	3 Upgrade
Software options	00000007 (ENT, SEC, MULTI)

A system without the IPMI option enabled

The SVx41HDI contains the necessary software to use IPMI. To enable this capability, you must purchase the software option from StarTech.com unless you have purchased a model with the feature pre-enabled. To verify whether the IPMI feature is enabled on your unit, login to the Web interface as **Admin**, click the **Setup/Admin** button at the top of the page, and click **Firmware and flash memory management**. If **IPMI** is not listed beside **Software Options** (see above) then the IPMI option is not present and you will have to purchase the software option to use the feature.

To purchase the IPMI option, contact StarTech.com Technical Support:

USA/Canada: 1-800-265-1844

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

Rest of the World: +1-519-455-9675

Purchase Options

If you wish to add additional optional features to this unit, please call technical support and provide them with this special code:

4-E680-074A-1-7

They will provide you with an unlock code. Please enter that code, exactly, here:

Unlock code:

Have your model and serial number on hand. When asked, supply the technician with the code listed under **Purchase Options** at the bottom of the **Firmware and flash memory management** page. Once the order is processed, the technician will provide you with an Unlock code. Enter that code in the space provided, and click **Submit**. The system will update itself to allow IPMI configuration.

Connecting the SVx41HDI for IPMI Control

The **SERIAL** port on the rear panel requires the use of a null modem serial cable. Connect one end of the serial cable to the serial port that is configured for IPMI access on the managed computer. Connect the opposite end to the **SERIAL** port on the SVx41HDI.

Configuring IPMI on the SVx41HDI

Once you have connected the IPMI-configured serial port to the SVx41HDI and enabled the software option, you can begin to configure IPMI settings through the Web interface.

IPMI/IPMB setup (Intelligent Platform Management)

Log in to the Web interface as **admin**. Click the **Admin/Setup** link at the top of the page and choose **IPMI/IPMB setup (Intelligent Platform Management)**.

IPMI Status

IPMI is **not** currently working. Check configuration here and verify host is configured correctly.

IPMI via Serial Port

Enable IPMI (Intelligent Platform Management Interface) via serial port: **Disabled** ▼

The following two setting must match the configuration of your host's BMC (Baseboard Management Controller). You will probably have to run some sort of special configuration software to change them on your host.

Select baud rate to use: **19,200 bps (default)** ▼

A password is required for authentication with the BMC. This password must have enough authority to control the chassis power and read all sensors. This password applies only to the BMC and has nothing to do with other software you may be running on the host. Password failures will be logged to the system log for debugging.

BMC Password:

Save changes by clicking here: **Commit**

You will be presented with the **IPMI Status** menu (see above). Make the following changes to enable IPMI:

- **Enable IPMI (Intelligent Platform Management Interface via serial port):** select **Enabled**.
- **Select baud rate to use:** select a value from the menu between **9600 bps** and **115,200 bps** based on the configuration on the managed computer's IPMI settings.
- **BMC Password:** Enter the password twice assigned to the BMC in the managed computer's BIOS setup software.

Note that the selected baud rate should match the managed computer's setting. Problems with the BMC password (as well as any other error information) will be recorded in the SVx41HDI's system log on the **Status** page of the Web interface. If the managed computer's BIOS setup

allows for multiple levels of security for the BMC, ensure the password you enter on the menu offers sufficient authority to control chassis power and monitor fan status.

Once you have made the necessary changes on this screen, click **Commit** to activate IPMI with the settings you entered. Note that clicking **Commit** will cause any active VNC sessions to fail and you will need to re-establish them.

Accessing the Status Screen

The SVx41HDI allows you to monitor the status of the managed computer via IPMI using either the Web interface or the VNC client. The information you will be able to view using the status screen will depend on the model of managed computer. Since IPMI implementations vary widely across manufacturers, the information you are able to see on your status screen may differ from the examples. Note that the **Status** screen will not allow you to make any configuration changes and is for monitoring purposes only.

To access the **Status (IPMI Sensor Report)** screen:

From the Web interface: click **View IPMI sensor report** next to the thumbnail image on the **Home** screen

From the VNC interface: click **IPMI** from the Bribar at the bottom of the VNC window

Examples:

Current IPMI Sensor Report

Refresh

#	Sensor Name /Description	Value
1	Baseboard 1.2V	1.21 Volts
2	Baseboard 1.25V	1.25 Volts
3	Baseboard 1.8V	1.78 Volts
4	System board (Volts)	1.79 Volts
5	Baseboard 2.5V	2.48 Volts
6	Baseboard 3.3V	3.3 Volts
7	System board (Volts)	3.31 Volts
8	Baseboard 5.0V	5.07 Volts
9	Baseboard 5VSB	4.97 Volts
10	Baseboard 12V	12.1 Volts
11	Baseboard 12VRM	12.2 Volts
12	Baseboard -12V	-12.3 Volts
13	Baseboard VBAT	3.11 Volts
14	Baseboard Temp	36 °C
15	System board (°C)	36 °C
16	Sys Fan 1	2280 RPM
17	Sys Fan 2	2140 RPM
18	Sys Fan 3	2900 RPM
19	Sys Fan 4	2900 RPM
20	Processor (°C)	37 °C
21	Proc 1 FanBoost	37 °C
22	Processor 1 Fan	4100 RPM
23	Processor Vccp	1.46 Volts
24	Power Cage	Power Cycle
25	BMC Watchdog	n/a
26	Scrtty Violation	n/a
27	Physical Scrtty	n/a
28	POST Error	n/a

Web Status Report

IPMI Sensor Report

Refresh Status: BMC okay. 02:52:12 PM

Sensors

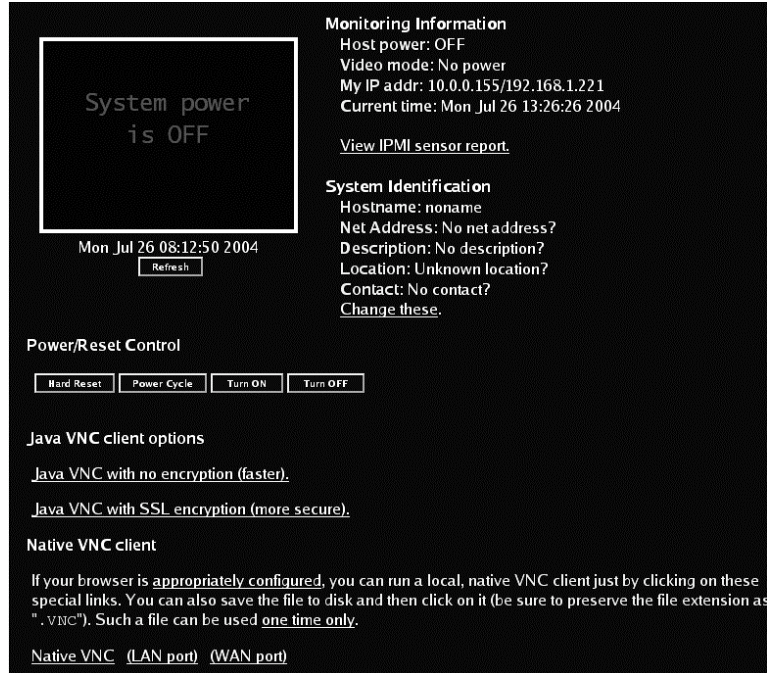
Baseboard 1.2V: 1.21 Volts	Baseboard 1.25V: 1.25 Volts
Baseboard 1.8V: 1.78 Volts	
System board (Volts): 1.8 Volts	
Baseboard 2.5V: 2.48 Volts	Baseboard 3.3V: 3.3 Volts
System board (Volts): 3.31 Volts	
Baseboard 5.0V: 5.07 Volts	Baseboard 5VSB: 4.97 Volts
Baseboard 12V: 12.1 Volts	Baseboard 12VRM: 12.2 Volts
Baseboard -12V: -12.3 Volts	Baseboard VBAT: 3.11 Volts
Baseboard Temp: 36 °C	System board (°C): 36 °C
Sys Fan 1: 2280 RPM	Sys Fan 2: 2140 RPM
Sys Fan 3: 2900 RPM	Sys Fan 4: 2900 RPM
Processor (°C): 37 °C	Proc 1 FanBoost: 37 °C
Processor 1 Fan: 4100 RPM	Processor Vccp: 1.46 Volts
Power Cage: Power Cycle	BMC Watchdog: n/a
Scrtty Violation: n/a	Physical Scrtty: n/a
POST Error: n/a	Critical Int: n/a
Memory: n/a	
System board (Event Logging Disabled): n/a	
Proc Missing: n/a	ACPI State: S5/G2: soft-off
System Event: n/a	Button: n/a
SMI Timeout: n/a	Sensor Failure: [0x00 0x00000]
NMI State: Asserted	SMI State: n/a
FSB Mismatch: n/a	
Processor (Processor/Processor Slot): Processor Presence detected	
Processor #2 (Processor/Processor Slot): n/a	
System board: Deasserted	DIMM 1: Device installed/attached
DIMM 2: Device installed/attached	DIMM 3: n/a
DIMM 4: n/a	

VNC Status Report

Accessing IPMI Controls

There are two ways to access power controls for the managed computer. The first is through the **Home** screen on the Web interface. The second is through the Bribar during an active VNC session.

Web



Controls on the Home Screen (Web)

Once IPMI is enabled and functioning correctly, a set of controls will appear immediately under the thumbnail image of the managed computer on the **Home** screen on the Web interface. Note that you must be logged in as **admin** to use this feature. From here, you have four options:

Hard Reset: Equivalent to pressing the RESET button on the managed computer. (The computer will restart.)

Power Cycle: The computer will power off, pause for a moment, and power on again automatically; equivalent to pressing the POWER button off and on again on the managed computer.

Turn ON: Powers on the managed computer.

Turn OFF: Powers off the managed computer.

VNC



If you are inside an active VNC session and are logged in as **admin** you can use the Bribar to access IPMI features. You have two choices from the Bribar:

Reset: Equivalent to pressing the RESET button on the managed computer. (The computer will restart.)

ON/OFF: Powers the managed computer on or off depending on the current state of the managed computer; equivalent to pressing the POWER button on the managed computer.

NOTE: IPMI may not automatically close the managed computer software safely when you issue a reset or power off command. Since these features are equivalent to pressing hardware buttons on the computer itself, the computer will respond in exactly the same way. Always shut down your operating system and application software normally before issuing an IPMI command to avoid data loss or corruption.

Appendix E: The Modem Option Upgrade

Background

The modem option allows the SVx41HDI to act as an Internet connection server for increased security and flexibility in connecting with the managed computers. Unlike the TCP/IP connection used with the standard Web configuration and VNC clients, the modem creates a one-to-one connection between the SVx41HDI and the computer you are using to manage your network that is essentially private, as it bypasses the public Internet completely. Note this option requires both an external modem (most standard connection protocols are supported) and a dedicated phone line that can be connected to the modem for external access. While it is technically possible to use the modem feature through some PBX systems, this increases the complexity and reduces the performance of the connection. For clarity, the instructions presented here assume that the modem is connected to a typical POTS (plain old telephone system) line that is not routed through a phone management system or shared with other devices. If you wish to use this feature through a PBX system, it may require some experimentation and additional support from your telecom services provider, and is not supported by StarTech.com.

Activating the Modem Option

Version Numbers

Component	Version / Release
System firmware	Thu Jul 8 17:28:01 EDT 2004
CGI Component	04.27.4172125
Linux Kernel	Linux version 2.4.20-pre7 #130 Mon Mar 8 09:37:36 EST 2004
System FPGA	3 Upgrade
Software options	00000007 (ENT, SEC, MULTI)

A system without the modem option enabled

The SVx41HDI contains the necessary hardware to attach a modem. To enable the modem capability, you must purchase the software option from StarTech.com unless you have purchased a model with the feature pre-enabled. To verify whether the modem feature is enabled on your unit, login to the Web interface as **Admin**, click the **Setup/Admin** button at the top of the page, and click **Firmware and flash memory management**. If **MODEM** is not listed beside **Software Options** (see above) then the modem option is not present and you will have to purchase the software option to use the feature.

To purchase the modem option, contact StarTech.com Technical Support:

USA/Canada: 1-800-265-1844
UK/Ireland/Europe: 00-800-7827-8324
Rest of the World: +1-519-455-9675

Purchase Options

If you wish to add additional optional features to this unit, please call technical support and provide them with this special code:

4-E680-074A-1-7

They will provide you with an unlock code. Please enter that code, exactly, here:

Unlock code:

Have your model and serial number on hand. When asked, supply the technician with the code listed under **Purchase Options** at the bottom of the **Firmware and flash memory management** page. Once the order is processed, the technician will provide you with an Unlock code. Enter that code in the space provided, and click **Submit**. The system will update itself to allow modem configuration.

Connecting a Modem

The SVx41HDI will work with virtually any Hayes-compatible modem that recognizes the standard AT command set. Some modem manufacturers offer “enterprise” grade modem products (at a premium price) that include technology to improve the stability of connections; whether this type of product would be beneficial to your application depends on whether you consider the modem connection to be mission-critical, the quality of your telecom infrastructure, and your budget for implementing this solution. The model of modem attached is essentially transparent to the SVx41HDI.

It is important to note that modems that offer “56K” (or 56,000 bps) connections often achieve connection speeds that are far lower than their maximum capabilities. Given the limitations of telecom infrastructure (many locations have yet to implement fully digital switching technology, and still rely on older analog technology for some segments), the maximum “upstream” transfer rate is limited to a maximum of 33,600 bps between two modems; the “downstream” rate is often within a similar range for a typical connection. Therefore, speeds below 56,000 bps do not indicate a problem with the modem or the SVx41HDI but simply reflect the line conditions at the time the connection is made. The **SERIAL** port on the rear panel must be used for the modem connection. It requires the use of a null modem serial cable.

Place the modem near the SVx41HDI and an available telephone jack. Connect the modem to the telephone jack, data cable, and power source according to the instructions in its documentation. The opposite end of the modem’s data cable should be a DB9 female serial connection. Connect that end of the cable to the **SERIAL** connection on the rear panel of the SVx41HDI.

Configuring a Modem Connection on the SVx41HDI

Most connections will work appropriately with the default settings on the SVx41HDI once the feature is enabled. When you entered the Unlock code to enable the feature, the SVx41HDI created a new menu option to enable configuration of this feature.

Modem (PPP) setup

Login to the Web interface as **Admin**. Click **Admin/Setup** from the top of the page and choose **Modem (PPP) setup**.

Modem Option

Enable this to allow the modem to answer the phone and start a PPP connection.

Enable modem connections (PPP) via serial port/modem: **Disabled**

Baud rate to use (affects connection to between us and the modem only): **115200 (default, recommended)**

Modem init string. This should program the modem to answer the phone on whatever ring needed, enable hardware flow control, and force the modem to lock baud rate regardless of connect speed. The default string is `ATE0S0=1&K3` which should work for most modems (answers on first ring).

Init string: `ATE0S0=1&K3`

Save changes by clicking here: **Commit**

You will then be presented with the **Modem Option** menu (see above). Make the following changes to enable and configure the modem connection.

- **Enable modem connections (PPP) via serial port/modem:** select **Enabled**.
- **Baud rate to use (affects connection between us and the modem only):** select **115200**.
- **Init string:** leave as `ATE0S0=1&K3` (see below).

The baud rate dictates the connection speed between the SVx41HDI's serial port and the modem, and does not affect the connection speed between the local and remote modems, as they will negotiate their own connection speed when a connection is made. It is highly recommended that this setting be left at the default for best performance.

The init string is the command (using the standardized Hayes AT command set) that the SVx41HDI will send to the modem to activate it. The string included should work with the majority of modems and configures the following connection properties: answer incoming calls on the first ring, enable hardware flow control, and lock the connection speed. Your modem's documentation will describe other potential init strings that you can use to alter the connection properties. For instance, you could commit the settings to the modem's non-volatile memory (NVRAM) or allow the modem to adjust the connection speed for greater stability (and so on). You may wish to test the connection with the default init string first before making changes specific to your modem model or situation to simplify the troubleshooting process.

Click the **Commit** button to save your changes and activate the modem feature with the specified settings.

Configuring the Remote Connection

This section describes how to configure a typical Windows dial-up session to access the modem connection on the SVx41HDI. The instructions here relate to a Windows XP configuration; other versions of Windows are similar.

1. Open **My Network Places** from the desktop or the **Start** menu.
2. Click **View network connections**.
3. Click **Create a new connection** under **Network Tasks**.
4. The **New Connection Wizard** window will open. Click **Next**.
5. Select **Connect to the Internet** and click **Next**.
6. Select **Set up my connection manually** and click **Next**.
7. Select **Connect using a dial-up modem** and click **Next**.
8. In the space provided under **ISP Name**, type an appropriate name of your choosing for the connection. Click **Next**.
9. In the space provided under **Phone Number** enter the phone number for the line to which the SVx41HDI's modem is connected. You may need to add the area code, country code, or other digits needed to access the outside line as appropriate. When finished, click **Next**.
10. Make your choice from **Anyone's use** or **My use only** and click **Next**.
11. Beside **User name** enter the user name of any valid user created using the Web interface of the SVx41HDI. Beside **Password** and **Confirm password** enter the password that the user you entered above uses to access the Web interface.
12. This screen also includes 3 checkboxes. **Uncheck all 3 checkboxes**.
13. Click **Next**.
14. You may select to add a shortcut to the desktop for this connection. Click **Finish**.

You can now use this connection to access the SVx41HDI modem. Since you will still login to the unit through the Web interface after establishing a dial-up connection, the user name on the PPP connection and the user name used to access the Web interface do not have to be the same. For security purposes, you may wish to create a separate user name for dial-up access.

The unit will negotiate a PPP connection based on the settings you provided, and no additional scripting or configuration should be required under most circumstances. This is a summary of the settings for use with non-Windows operating systems, or other versions of Windows besides XP:

- PPP (Point-to-Point Protocol) must be used; no other authentication methods are supported.
- TCP/IP must be installed/enabled on the computer making the connection, and must be used for the dial-up connection.
- The connection must be configured to obtain a dynamic IP address.
- The user name/password must match a user currently configured on the SVx41HDI.
- For best performance and to simplify the troubleshooting process, firewall software should not be used with the dial-up connection.

Accessing the Web Interface

Once a dial-up connection has been established, you can access the Web interface or start a VNC session using the following IP address:

https://99.99.99.99

You can now login to the Web interface (and/or VNC session) normally. Note that the remote machine (the one you dialed from) is automatically assigned the IP address 99.99.99.100 for the PPP session. This, and the IP address of the SVx41HDI, cannot be modified. The following TCP/IP port numbers are assigned for a PPP connection, regardless of the settings configured in the Web interface for the **LAN** port:

HTTPS: 443

VNC (clear-text): 5900

VNC (SSL secured): 15900

SSH: 22

Performance Notes

- All images over the PPP connection will be grayscale to conserve bandwidth. If other users are connected while a PPP session is active, their screens will be in grayscale as well. When PPP is inactive, color is automatically re-enabled.
- Some areas of the screen may not be updated as frequently as others, and animations or other auto-updating areas of the screen may appear out-of-focus or “blocky” as a result. Since the area around the mouse pointer is refreshed most frequently, hold the pointer over an area to improve its clarity.
- It may be beneficial to minimize any unnecessary icons, backgrounds, or other clutter on the managed computer’s desktop to make the dial-up connection as efficient as possible.
- You will need to disable the modem feature and re-connect the serial port on the SVx41HDI to the port on a managed computer to use serial configuration.

Troubleshooting Guide

The following messages will appear in the system log on the **Status** screen in the Web interface and may help to diagnose problems with the modem configuration.

Starting PPP (for auth) on port...

Modem is connecting and the PPP login process is starting.

Modem hang up. Resetting

The connection has been closed or terminated unexpectedly.

Timeout during login process. Giving up

The PPP client connecting over the modem has waited too long to complete the authentication process or supplied an invalid user name and/or password.

Modem init chat script failed

The modem did not respond to the initialization string from the SVx41HDI. You may need to change the init string or verify the cabling and modem status.

Modem init okay

The modem has responded appropriately to the init string.

Saw PPP startup from client

A PPP authentication has occurred and a session has started.

Phone line rings!

An incoming call has been detected by the modem.

Modem answers: xxxxxxxxxx

The connection speed and protocol used for a connection, as reported by the modem.

The exact contents of the message will vary depending on the modem make and model.

Appendix F: Using Optional R-Port Devices

Background

The SVx41HDI offers a unique way to expand the functionality of the base product. Using the integrated **R-Port** on the rear panel, you can add up to 16 RS-485 serial devices using a specialized daisy-chain technology. The SVx41HDI includes integrated control functionality that allows you to monitor and configure serial devices using the interactive Web interface. To minimize space and infrastructure requirements, the R-Port serial devices use a single cable to carry both power and the data signal. All configuration settings are stored separately in each attached device in non-volatile memory so that they will not be lost in the event of a power outage or disconnection.

Connecting R-Port Devices to the SVx41HDI

The cable for each serial device is similar to a phone cable and uses an RJ-14 connector. For the first serial device, connect the cable (provided) to the **R-Port** on the rear panel of the SVx41HDI. Connect the opposite end to the **DATA OUT** (or similar) port on the serial device. Note that some devices may use an integrated cable, so you will not need to make a separate connection on the serial device. Once you have added the first serial device to the SVx41HDI, you can connect additional serial devices to the **DATA IN** (or similar) port on the previous device in the chain. Once the cabling is attached, the device becomes active after a 15 second initialization period. For specific information regarding cabling and status indicators for a specific serial console, refer to the instructions that came with the product.

Configuring/Viewing R-Port Devices through the Web Interface

Once you have one or more R-Port serial devices connected, you will be able to configure and manage them through the Web interface. You may need to modify the default settings on the SVx41HDI to match your various R-Port devices' default configuration. Consult the documentation that came with your R-Port device to determine if you need to modify the default settings to complete the installation. To be able to configure your serial devices, you must be logged in as **admin**. Other users will be able to view which devices are active but cannot configure them.

Once you are logged in, choose the **Admin/Setup** option from the menu at the top of the Home screen in the Web interface. Click **External Serial consoles setup and control**. You will be presented with the **Serial Consoles Attached** menu, and a table with the following headings:

#	Name / Description	Baud (bps)	Mode	Force DCD	Console Log	Connect...
---	--------------------	------------	------	-----------	-------------	------------

#: You can assign a value (1 ~ 99) to each attached serial device. This does not affect the configuration or operation of the device in any way, but is simply a means to sort this list for ease of management.

Name/Description: An identifier for the R-Port device. Like the number assignment, it is for ease of administration only.

Baud (bps): This is the communication speed for the device, and the setting here must match the setting on the device itself (see below). All common baud rates between 300 and 115,200 bps are supported.

Mode: Sets the character framing scheme that the SVx41HDI will use with the R-Port device. You can choose from the following selections:

8N1: Eight bits, no parity, one stop bit (default and most common)

7N1/7O1/7E1/7M1/7S1: Seven bits, (none/odd/even/mark/space) parity, one stop bit

8N1/8O1/8E1/8M1/8S1: Eight bits, (none/odd/even/mark/space) parity, one stop bit

8N2: Eight bits, no parity, two stop bits

Force DCD: Forces the Carrier Detect signal to be active at all times. Normally, DCD becomes active when a new user connects and is dropped when the last user disconnects (a response that is similar to many modems). When active, the device will logout and reset itself if the carrier signal is lost, increasing security. Note that this may not work with all devices and could impair proper operation in some circumstances. The default setting is off.

Console Log: Clicking this link will open a separate Web page that will display the last 200 characters committed to that device's console log. Note that existing data is overwritten automatically when the 200 character limit is reached.

(Optional, not shown) **IPMI:** This is an optional feature that requires the purchase of a software upgrade on the SVx41HDI. Refer to Appendix D for more information about purchasing and using the IPMI upgrade. This feature will not appear on the menu if the upgrade is not installed.

You can make as many changes as needed on this menu at one time before applying your changes. Once you are satisfied with the changes you have made, click **Commit changes** to apply the new settings. Click **Refresh** at any time to see an updated list of attached R-Port devices.

Advanced Configuration Using the Integrated SSH Shell

In most cases, configuring the SVx41HDI to the same settings as the R-Port devices you are connecting should allow the devices to work with a minimum amount of configuration. However, you can also change the default settings on each R-Port device to fit your preferences and the needs of your application.

If you click the **Connect...** button next to the device you want to configure, two new windows will appear. The smaller of the two is a login screen; the other is a SSH terminal window. Click the login window and sign in as **admin** (using the same password as the Web interface) to activate the terminal window. You will see a welcome banner similar to the following:

```
Baud rate: 115200 bps, 8N1
Connected to #1: (none)... (Press Ctrl-Shift-_ for menu).
```

You are now connected to the R-Port device. Commands you type will be echoed on the terminal screen. It offers a simple menu system that allows you to change its configuration settings. To access the menu press **[Ctrl] - [Shift] - [_]** (underscore) on the keyboard to access the menu. It will be similar to the following:

```
RS-232 Menu (#1: (none), 115200 bps, 8N1)
Q - Disconnect
# - Send break
H - Hangup line (drop DCD)
E - Send Ctrl-Shift-_
L - Low log entries (line buffer)
l - Show last 10 log entries
other - Return to connection
Press key ->
```

To execute the desired command, simply press the corresponding key on the keyboard. You can also execute the command and avoid the menu by pressing the **[Ctrl] - [Shift] - [_]** key combination quickly and pressing the letter of the command. To quit the menu, press **[Q]** on the keyboard when the menu is active.

Remote Login via SSH

You can also use a standard SSH client to access the R-Port options if you wish to avoid using the Java-based SSH client in the Web interface. Simply use your SSH client (several freeware packages are available for download, along with commercial applications) and connect to the IP address of the SVx41HDI using port 22 (default).

Login in to the SSH session as **admin** using the same password as the Web interface. At the command prompt type **connect x** (where **x** is the number of the R-Port device you wish to manage). Alternatively, you can enter the command **connect -l** to see a list of active devices.

Operating Notes

- Hardware handshaking (CTS/RTS) is required for speeds exceeding 9600 bps. It is enabled by default on the SVx41HDI, but may need to be enabled on the other end of the connection. For Unix systems, the command is:
stty -crtcts < /dev/[serial port]
- R-Port devices use a simple RS-485 multidrop network running at 115,200 bps. It is possible that every R-Port device will not be inputting/outputting data at the same rate at all time. However, since these devices use interactive logins, it is unlikely that all channels would be busy at any one time. Hardware handshaking is used to limit the output rate of individual channels as needed.
- A maximum of four users may simultaneously login to the same device. All users may type commands at any time, and all users will see the same output. Note the following:
 - All users have equal access to all channels.
 - A maximum of 16 R-Port devices may be connected at any one time.

- You plug-in and unplug any R-Port device at any time. When reconnected, it will automatically become available after a 15 second initialization period. Any log entries will be retained by the R-Port device while deactivated, but will not be available to users until it is re-initialized.