External KVM control over IP

Server Remote Control External KVM control over IP

SV1115IPEXT

Instruction Manual

Actual product may vary from photo

StarTech.com
Making hard-to-find easy!

FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

• Reorient or relocate the receiving antenna.

• Increase the separation between the equipment and receiver.

• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult the dealer or an experienced radio/TV technician for help.

Use of Trademarks, Registered Trademarks, and other Protected Names and Symbols

This manual may make reference to trademarks, registered trademarks, and other protected names and/or symbols of third-party companies not related in any way to StarTech.com. Where they occur these references are for illustrative purposes only and do not represent an endorsement of a product or service by StarTech.com, or an endorsement of the product(s) to which this manual applies by the third-party company in question. Regardless of any direct acknowledgement elsewhere in the body of this document, StarTech.com hereby acknowledges that all trademarks, registered trademarks, service marks, and other protected names and/or symbols contained in this manual and related documents are the property of their respective holders.

Table of Contents

i

iii

Introduction

Thank you for purchasing a StarTech.com SV1115IPEXT Server Remote Control. 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 (i.e.TCP/IP and SNMP)

- Offers secure management options including SSL encryption, SSH tunneling, and RADIUS authentication

- Allows for disk emulation and file transfers, including completely remote application and operating system installations

- Transfers data at speeds up to 920 Kbits/sec

- Platform independent: can be managed using any Java-enabled Web browser and connected to virtually any host server or computer that supports PS/2 or USB input devices

- On Screen Display offers convenient control and configuration options

Contents

This package should contain:

- 1 x SV1115IPEXT unit

- 1 x Power adapter

- 1 x Power cord

- 1 x Integrated PS/2 and VGA Switchbox cable

- 1 x Instruction Manual

Required Cables and Hardware

The included integrated KVM cable will allow you to connect the SV1115IPEXT to most IBM compatible computers. Depending on your requirements and how you wish to handle the initial configuration of the unit, you may wish to use the following additional cables and hardware.

All applications

- 1 x Straight-through Ethernet patch cable (to connect the unit to your LAN)

StarTech.com part number: M45PATCHxxxx

1

To use the optional dedicated WAN port

- An additional straight-through Ethernet patch cable to connect the unit directly to a dedicated WAN/Internet connection

StarTech.com part number: M45PATCHxxxx

Configuration via serial port

- 1 x Straight-through RS-232 serial cable with 9-pin DB9 male/female connectors

StarTech.com part number: MXT100

–or–

- 1 x Null modem RS-232 serial cable with 9-pin DB-9 female/female connectors

StarTech.com part number: SCNM9FF

To use USB connections on host and/or virtual disk emulation

- 1 x USB Type A to B cable

StarTech.com part number: USBFAB_3

To install the SV1115IPEXT into a rack or cabinet

- 1 x Rack kit (supports up to two units)

StarTech.com part number: 1110EXTRACK

To add a redundant power supply

- StarTech.com part number: xxxxxxxxxxxxxxxx

2

Installing the SV1115IPEXT

Connecting the Unit to the Host Computer and Network

Please note: It is important that multiple users not be connected to the same physical network.

| Video (IN) | Host Keyboard | Host Mouse | USB | WAN | LAN | DCE Serial | DC (IN) | DC (IN) (2) |

Local Keyboard, Mouse, Monitor
(Native PS/2 or optional USB)

USB Hub (Optional)

Remote User

USBFAB_3
(Optional)

Internet/
Intranet

Integrated
KVM Cable   Host Computer

Ethernet Patch Cable(s) for
LAN/WAN   Network Infrastructure
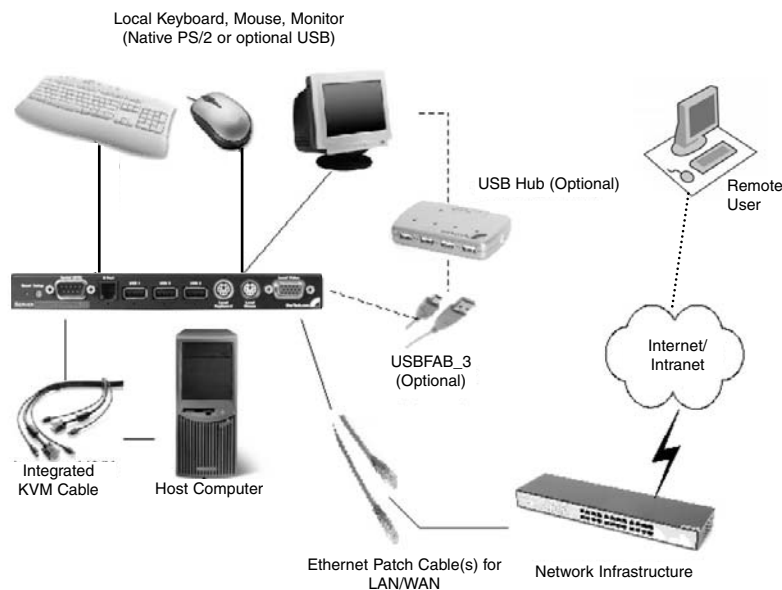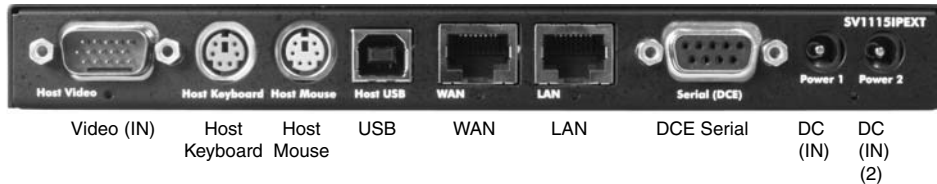
Follow these instructions if the host computer uses a PS/2 keyboard and mouse:

1. Power down the computer to which the SV1115IPEXT will be connected (***host computer***). If purchased, install the unit in your rack or cabinet following the instructions that came with the 1110EXTRACK (optional, not included).

2. If present, disconnect the existing monitor and PS/2 keyboard/mouse from the host computer.

3. Using the provided integrated KVM cable, locate the end with the male VGA (monitor) connector and connect it to the VGA-out connector on the back of the host computer.

4. Connect the PS/2 keyboard and mouse connectors on the same end of the integrated

3

KVM cable as the male VGA connection you completed in the previous step.

5. Insert the connectors on the opposite end of the integrated KVM cable (female VGA monitor connector, keyboard, mouse) to the **Video (IN)**, **Host Keyboard**, **Host Mouse** ports on the rear panel of the SV1115IPEXT as appropriate.

6. Using a Category 5 Ethernet patch cable, connect the LAN connector on the rear panel of the SV1115IPEXT to a network data jack (usually on a hub, switch, router, or pre-wired wall jack).

7. *Optional*: If needed, connect the WAN connector on the rear panel of the SV1115IPEXT to a network data jack (usually a hub, switch, router, or pre-wired wall jack). For more information on the WAN port, please refer to the section **Configuring SV1115IPEXT** (page 7) for important information.

8. **Important**: If you want to continue to use the host computer locally, skip step 10 and go directly to "Connecting a Local Keyboard, Mouse, and Monitor" after completing step 9. Otherwise, complete steps 9 and 10 now and continue to **Configuring SV1115IPEXT** (page 7).

9. Connect the power cord (provided) to an appropriate electrical outlet, plug the opposite end of the power cord into the AC/DC adapter, and insert the power connector into either the DC-in or DC-in-2 port on the rear panel of the unit. The LED underneath the power connectors will be solid green when the unit is powered.

IMPORTANT: If you wish to add power redundancy to the unit, simply connect the optional second AC/DC adapter to the unit following the instructions in step 9 above. This provides a load-balancing feature between the two power sources and allows the unit to function if one adapter fails. ***Please note: The additional power supply used with SV1110IPEXT can NOT be used with SV1115IPEXT.**

10. Power on the host computer.

Follow these instructions if the host computer uses a USB keyboard and mouse:

IMPORTANT: Not all computers fully support USB mice and keyboards and recognize them on startup. It is strongly recommended that you test the USB devices you will use with the host computer before configuring the SV1115IPEXT. If the computer does not work properly with USB devices, you can attempt to update the computer's BIOS to the most recent version to see if it adds USB input device functionality. Consult your computer manufacturer for details.

1. Power down the computer to which the SV1115IPEXT will be connected (*host computer*). If purchased, install the unit in your rack or cabinet following the instructions that came with the 1110EXTRACK (optional, not included).

2. If present, disconnect the existing monitor and USB keyboard/mouse from the host computer.

3. Using the provided integrated KVM cable, locate the end with the male VGA (monitor) connector and connect it to the VGA-out connector on the back of the host computer.

4

4. Insert the female VGA connector on the opposite end of the integrated KVM cable to the Video (IN) port on the rear panel of the SV1115IPEXT.

5. Connect a USB Type A to B cable to the USB port on the rear panel of the KVM.

6. Connect the opposite end of the USB Type A to B cable to an available USB port on the managed computer.

7. Using a Category 5 Ethernet patch cable, connect the LAN connector on the rear panel of the SV1115IPEXT to a network data jack (usually on a hub, switch, router, or pre-wired wall jack).

8. *Optional*: If needed, connect the WAN connector on the rear panel of the SV1115IPEXT to a network data jack (usually a hub, switch, router, or pre-wired wall jack).

9. **Important**: If you want to continue to use the host computer locally, skip step 11 and go directly to **Connecting a Local Keyboard, Mouse, and Monitor** (next page) after completing step 10. Otherwise, complete step 11 now and continue to the section entitled **Configuring SV1115IPEXT** (page 7).

10. Connect the power cord (provided) to an appropriate electrical outlet, plug the opposite end of the power cord into the AC/DC adapter, and plug the power connector into either the DC-in or DC-in-2 ports on the rear panel of the unit. The LED underneath the power connectors will be solid green when the unit is powered.

11. Power on the host computer.

NOTE: If you are using cables other than those provided in the SV1115IPEXT package or branded by StarTech.com, ensure that the cables are of high quality and use the minimum possible distance necessary. Low quality or excessively long (particularly video) cables between the host computer and the SV1115IPEXT could degrade performance.

NOTE: In the event that you do not have enough integrated USB ports available on the managed computer to directly connect the keyboard, mouse, and SV1115IPEXT, you may use a high-quality USB hub on one of the computer's USB ports to make all of the connections.

IMPORTANT: The SV1115IPEXT is convection-cooled. As such, please ensure the vents on both sides are unobstructed.

Connecting a Local Keyboard, Mouse, and Monitor

| Reset Button | DTE Serial | R Port | USB 1, 2, 3 | Local Keyboard | Local Mouse | Local Video |

SV1115IPEXT has the capability to connect a local keyboard, mouse, and monitor to the host computer for maintenance and monitoring, allowing users to physically use the host computer as though SV1115IPEXT were transparent. If needed, the unit can be run through a typical KVM switch like any other computer. Using a KVM cable, you can connect the Server Remote Control's host computer inputs to the "console" connectors on a KVM switch allowing you to control more than one computer remotely using a single Server Remote Control. If you want to use SV1115IPEXT through a KVM switch, consult the documentation that came with the switch for more details on how to make the necessary connections. See the section entitled Configuring the SV1115IPEXT for more information on using a KVM switch with the SV1115IPEXT.

To connect console devices:

1. Connect a standard PS/2 keyboard to the **Local Keyboard** port on the front panel of the SV1115IPEXT.

2. Connect a standard PS/2 mouse to the **Local Mouse** port on the front panel of the SV1115IPEXT.

3. Connect a SVGA-compliant monitor to the **Video (Out)** port on the front panel of SV1115IPEXT.

4. Power on the host computer.

Disabling Mouse Acceleration on the Host Computer

Please note: If you are using USB to connect SV1115IPEXT to the host computer, you will not be required to adjust the mouse settings on the host computer, as this device uses "Absolute" mode, which eliminates any problems you may otherwise experience with mouse synchronization or host mouse acceleration.

Many operating systems offer a feature called mouse acceleration, allowing the user to adjust the responsiveness of the cursor on the screen in relation to physical movements of the mouse. While this is usually a beneficial interface enhancement, it can interfere with the operation of the SV1115IPEXT and should be disabled on the host computer before a remote session is attempted. Follow the instructions below to disable mouse acceleration for the operating system installed on the host computer.

Windows 98

1. From the Control Panel, click on **Mouse**.

6

2. From Mouse Properties, click on the **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 the **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** and ensure 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   (For more information, please refer to **Troubleshooting**)

Configuring SV1115IPEXT

SV1115IPEXT offers four distinct methods for configuring the unit for your network. Which method will work best will depend on your level of experience and your specific network configuration.

Web Configuration Using the On-Screen Display

Upon boot-up, including following a reset, SV1115IPEXT will display a window on the local video output (front VGA connector), that will appear as follows:


```
Network Settings SV1115IPEXT

Enter this web URL:
     https://192.168.2.12
     https://192.168.1.123

      DHCP: No
  LAN addr: 192.168.2.12
   Netmask: 255.255.255.0
   Gateway: n/a
  Ethernet: 00:0E:C5:00:51:50
  WAN addr: 192.168.1.123
W Netmask: 255.255.255.0
W Gateway: 192.168.1.254
ESC→Close              Enter→Menu
```
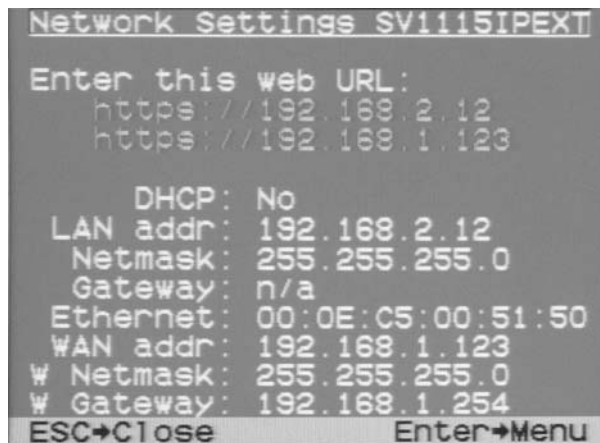
The initial screen will display the IP address assigned by your existing DHCP server (if present on your network). If no DHCP server is detected, a factory assigned IP address

7

will be displayed in its place (10.0.0.15 by default). Please make note of the assigned IP address, as you will need to enter it into your web browser to access the Web Interface.

If static IP addresses are assigned, you will likely need to change the **Net Mask**, **IP Address** and other details, prior to connecting via your Web browser. If this is the case, connect a local keyboard (USB or PS/2) and press the **Enter** key. In order to proceed, you will require an administrative username and password. By default, the username and password are **admin.** You will be given the opportunity to change the password (recommended) once the configuration is complete.

Alternatively, you may press the **Setup** button on the front panel, and you will not be asked to enter the admin password if you just press **Enter**.

At the main OSD menu (pictured below), you will be given several basic setup options. To configure SV1115IPEXT to your required network settings, use the Network Setup Wizard. To select from the menus provided, use the arrow keys on your keyboard. At any time, you can return to the previous menu by pressing the **Page Up** key.
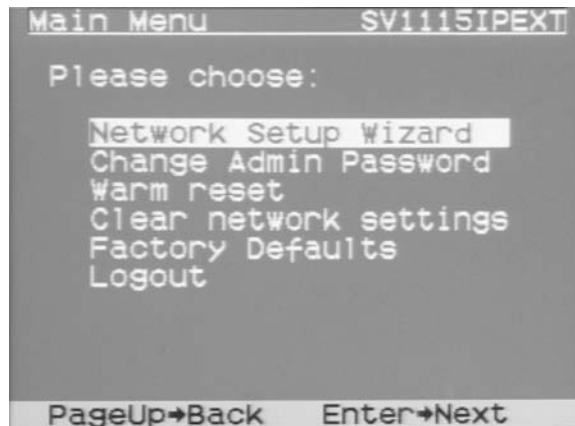
Web Configuration Using DHCP

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:

8

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 SV1115IPEXT 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 SV1115IPEXT 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 using the OSD setup screen. 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 SV1115IPEXT and wish to proceed with the Web configuration, do not power off the unit or your DHCP server, since the Server Remote Control might lease a different IP address. Should this happen, re-examine the DHCP log to verify the IP address again.

NOTE: DHCP functionality is not affected if you also connected the WAN port on the SV1115IPEXT to your network (see below). However, it is not recommended that you connect both the WAN and LAN ports to the same network segment.

Web Configuration Using Static IP

Since some networks rely on static IP addresses (every device has a pre-configured IP address that does not change), the DHCP access method described above is not applicable in those situations. To accommodate this type of installation, the WAN port on the rear panel of the SV1115IPEXT is factory-configured with its own IP address.

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

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

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

To access the Web configuration for this product, you will need to configure the workstation you are using to the same subnet (255.255.255.0) and also assign it a valid IP address (i.e. 192.168.1.100). For details on how to change the IP address of your computer (if necessary), consult your documentation or System Administrator for assistance.

NOTE: It is advisable to verify whether another device on your network is using the

9

same IP address as the SV1115IPEXT before connecting it to the network, to avoid a conflict. Should an IP address conflict occur with another device on the network, power off the conflicting device or assign it another IP address before continuing the installation. If you are configuring more than a single SV1115IPEXT using the factory default settings on the WAN port, they cannot be connected to the network at the same time as they will use the same IP address.

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

Once your computer is configured to the same subnet as the SV1115IPEXT, you can use the IP address 192.168.1.123 to access the Web configuration system.

Terminal Configuration Using a Serial Cable

Configuring the SV1115IPEXT using a serial cable is the best choice if you need to pre-configure the unit before attaching it to a network, i.e. when sending to a branch office, customer site, etc. In general, the Web configuration is preferable because of its intuitive interface and the fact that you do not have to be within close physical proximity to perform the configuration. However, if you wish to use the serial cable method to configure the SV1115IPEXT, you can use any typical communication software package (**UNIX:** tip, cu, kermit, minicom; **Windows:** HyperTerminal, kermit).

You can use either serial port on the SV1115IPEXT to access the terminal configuration tool; your choice will dictate the type of cable you will use to make the connection. The **DTE** Serial port on the front panel requires the use of a null modem serial cable. The **DCE** Serial port on the rear panel requires the use of a straight through serial cable. Connect a female end of a serial cable to the serial port used for serial access on the host computer. Connect the opposite end (male if connecting to the DCE Serial port, female if connecting to the DTE Serial port) to the SV1115IPEXT. Configure the terminal software with "8N1" settings:

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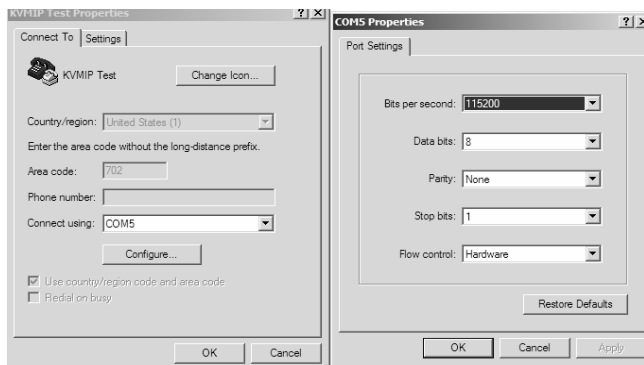
Sample HyperTerminal configuration

10

Using the Web Interface

The Web interface is the most intuitive way to configure the SV1115IPEXT. Offering a Java-based VNC client that can be used to control the host computer from a remote location, as well as support for any industry-standard HTML Web browser. You can access the Web interface by opening your Web browser and entering the IP address of the SV1115IPEXT you wish to access/configure. The IP address will be either **a)** the address assigned by your DHCP server as identified in the previous section, or **b)** 192.168.1.123 if your network uses static IP addressing.

The Login Screen

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

NOTE: Before the login screen appears, your Web browser may display a warning about an invalid security certificate. This does not affect the security of your data in any way. Whenever you are prompted about a certificate security problem by your browser or the Java VNC client, always choose the option to continue. For more information, please consult the section entitled **About Security Certificate Warnings** (page 42).

11

Web Interface Introduction

After the inital login screen, the screen will be divided into several sections, four of which will remain on the screen at all times while viewing the Web Interface:
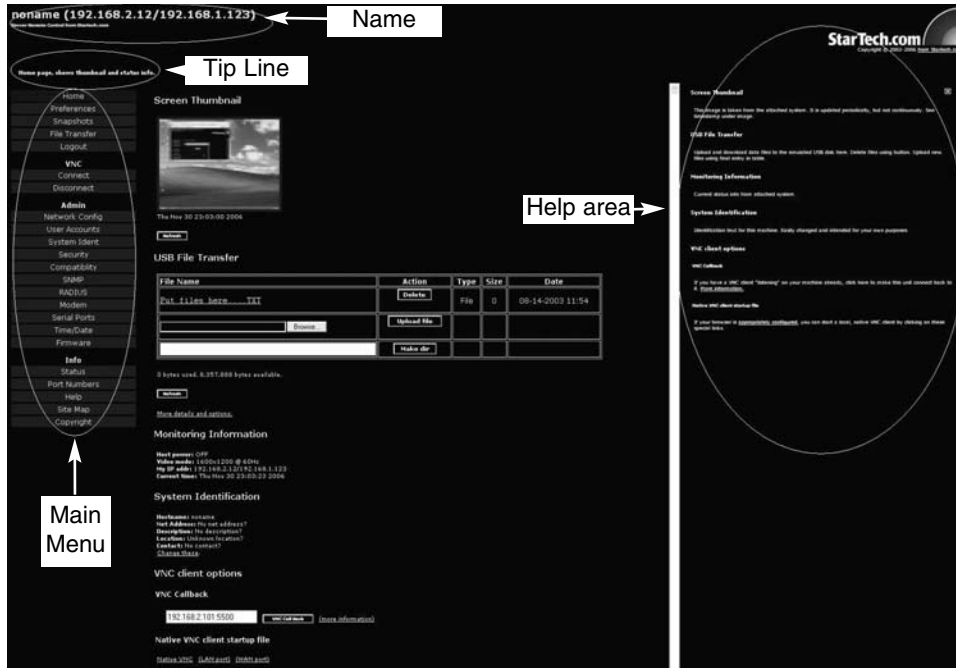
Name: At the top of the screen, the name of the machine being controlled is displayed

Tip line: The area directly below the **Name** indicates what function each selection from the **Main Menu** performs. Hover the mouse pointer over each individual listing in the **Main Menu** to update this message according to the function performed by each listing.

Main Menu: At the left-most side of each page, the **Main Menu** is displayed, allowing users to choose functions offered by the Web Interface.

Help area: The right-most column offers an optional help summary for each page. If you don't wish to use this information, it can be closed by clicking the small **[x]** at the top right (within the Web Interface). If closed, click on the **Help** button near the top right of each page to re-display it.

Please note: While these four sections remain stationary, depending on your selections, the center of the page will display the desired content.

Main Menu selections

Please note: Some of the following items may not be present, based on assigned user privileges (i.e. non-admin users will not see any items under the **Admin** category.)

The **Home** screen offers a **Screen Thumbnail** view of the controlled computer, as well as basic file transfer functions, Monitoring Information, System Identification and VNC Client options.

The **USB File Transfer** function allows you to upload files to a virtual (emulated) USB drive. For more information, please view the **Help** listing for this section.

The **Preferences** screen offers several configuration options, pertaining to the functionality of SV1115IPEXT. Here, you will be able to customize settings to optimize overall performance, (i.e. Encryption options, VNC options, display and bandwidth options etc.), according to each user's individual preferences. Please save your selections by clicking the **Save Changes** button.

The **Snapshots** screen allows you to view and save a screenshot of the controlled computer in its current state. This screenshot will update periodically (automatically). Saved image files are stored in .PNG format.

File Transfer

The SV1115IPEXT is able to emulate a virtual disk drive attached to the host via USB, and must have the optional USB cable connected to the SV1115IPEXT and the host computer to function. Depending on configuration, it will appear to the host as a floppy drive (1.44MB), an 8MB RAMdisk or a CD-ROM. The host computer does not require any special drivers or other configuration. You can transfer files to the virtual disk at any time. SV1115IPEXT will wait until the host is not using the disk, and add or remove the files. When the host computer next looks at the drive, it will notice the changes. You can read files from the virtual disk at any time, as long as the host is not actively writing to the disk. All of this happens in the background, and you may treat the virtual disk as a shared drive without restrictions.

Access to the files is performed through the web interface. The contents of the root directory are shown on the home page. You can download files as you would any file on the web (right-click and **Save target as**). To upload a file, click **Browse**, select a file, and then click **Upload**. Files and directories may be deleted using the **Delete** button situated to their right.

Change Disk Type

1.44M Floppy	Ramdisk	CD-ROM
Format as floppy	Format as ramdisk	CD-ROM image

When emulating a floppy disk or RAMdisk, the data is stored in RAM on the SV1115IPEXT itself. In order to emulate a CD-ROM disk drive, a web server is required to provide the CD-ROM image data. The Web server must be accessible to the unit, which communicates with it constantly as data is needed.

Floppy mode
Choose the **Format as floppy** button to switch to floppy mode. Under Windows, the drive will be identified as a "high density floppy" and will typically be assigned a drive letter of **B**:. The capacity is limited to 1.44 megabytes in this mode. The purpose of supporting floppy mode is to permit the use of floppy-disk images generated by other systems. For example, the flash BIOS upgrade process is performed with a special floppy and is bootable. You can transfer bits from that floppy to the SV1115IPEXT (use the upload disk image form). Now, you can boot from the special floppy. In addition, emergency repair disks are often restricted to floppies.

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

Disk Formats
When you choose the **Format as...** button, the disk image stored in RAM is formatted as an empty MS-DOS disk, with a single file called **Put files here...TXT**. SV1115IPEXT is able to read most MS-DOS/Windows formatted disks and presents the files via the Web interface. However, disk emulation occurs at the lowest level so that other disk formats can be used, if you have the tools needed to create and read the disk images. At the bottom of the page are the upload and download options for the entire disk image. Any image that is exactly 1,474,560 bytes long will be treated as a floppy. Images of other sizes are supported up to 8MB.

CD-ROM Mode
The SV1115IPEXT does not store any data in this mode. Instead, it emulates a USB CD-ROM drive with a disk inserted. The data from that disk must be provided by an external web server. You will need a copy of the CD-ROM contents that you want to emulate as an ISO file. This is a byte-for-byte copy of track one (the data track) of a data CD-ROM. The ISO file must be made available on a web server that can be accessed by SV1115IPEXT. To switch to this mode, type in a URL pointing to the ISO image, and click on **Commit**. The system will connect to the web server and test the file for access. If successful, you will be shown a short report on the file contents, and the disk will be ready to use. Currently there is no other way to preview or browse the contents of the CD-ROM image,

14

except from the host.

CD-ROM Web Server Requirements:
• Data must be hosted on a web server that the SV1115IPEXT can access directly.
• An image of a bootable CD-ROM disk can be used by the BIOS to boot an operating system.
• The image file itself may be any size, but it will typically be less than 700 megabytes. Normally this file will be an ISO image (an ISO-9660 file system) but any disk image may be used.
• Web server must support "byte ranges". Persistent connections are used, if available, as this greatly improves performance. "Read-only" access is provided; writing is not supported.
• CD-Rom block size must be 2048 bytes. Unfortunately, XA-Data type tracks are not supported.

Booting from USB Disk
If the host computer's BIOS supports USB boot devices, it is possible to boot from the emulated CD-ROM or floppy. This allows complete operating system replacement without any on-site intervention.

The first step is getting a bootable disk image onto the emulated floppy or CD-ROM. For CD-ROM images, you will need an ISO image from a disk that contains special bits to enable boot ("El Torito" standard). Nothing special is needed when reading the ISO from a working, bootable CD-ROM. To create a bootable floppy, you can format the emulated floppy from the target system, or read the data from a working boot floppy. This can be done from Windows using **Disk Copy** (right click on the drive letter in the Windows Explorer) or by using a program like "RAWRITE".

Once you have a bootable image (CD-ROM or floppy) working on the Server Remote Control unit, you must adjust your BIOS settings to tell it to boot from a USB device. **NOTE**: You must select **USB CD-ROM** as the boot device for the BIOS, if using a CD-ROM image and **USB Floppy** if using a floppy image.

Logout

Clicking on **Logout** will terminate your Web Interface section. To re-initiate the Web Interface, you will be required to re-enter your username and password.

VNC
Connect
Disconnect

To launch or disconnect a Virtual Network connection with the controlled computer, click on **Connect** or **Disconnect** as appropriate

15

The **Admin** functions allow you to access all of the features you will need to perform an initial configuration of the SV1115IPEXT.

Dynamic Host Configuration Protocol (DHCP)

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

IP Addresses and Routing

This table allows you to assign IP information for the LAN and WAN ports separately. If you are using DHCP, the values for the LAN port will be filled in automatically and any changes made will not affect the setup. If **Ethernet Bridging** is enabled, the WAN port will use the same settings as the LAN port, and any changes will not affect the setup for that port. Adjusting the setting for the WAN port allows you greater control over how the SV1115IPEXT is configured for access from outside the local network, particularly if a firewall or proxy is in use.

Domain Name Server (optional)

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

Clicking the **Commit** button applies any changes made on this page, but leaves the old settings active until the next time the unit restarts. Clicking **Make changes effective now** applies the changes and restarts SV1115IPEXT so the new settings take effect immediately.

16

Ethernet Address (MAC Address)


```
Ethernet Address (MAC Address)

LAN: 00:0e:c5:00:51:50

WAN: 00:0e:c5:00:51:51
```
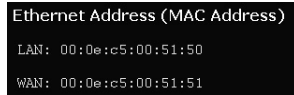
This is the Ethernet hardware address of this unit's LAN/WAN port. It is set at the factory and cannot be changed. You may need this number to configure your DHCP server.

Ethernet Bridging


```
Ethernet Bridging

Bridge LAN and WAN ports together:

Disabled  ⌄    Commit and Apply
```

When Ethernet bridging is enabled, the two Ethernet ports are virtually connected inside the SV1115IPEXT. Packets arriving on either port that are not meant for it will be forwarded out to the other port, when appropriate. IEEE-802.1d ("Spanning Tree Protocol") is implemented to avoid broadcast storms and to determine the topology of the network.

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

User Accounts

User Accounts

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 into the VNC console. Selecting **Delete** permanently removes the user from the system. If you enter values for a user that does not already exist under **Edit User Details**, the system will create that user for you when you click **Record changes**. If the user already exists, you will change the password for that user.

System Ident

Machine Name

This is a name that is used to uniquely identify this machine. You might want to create a DNS entry that matches this name. The name is provided as the **Client Name** for the DHCP server. It is also shown at the top of each page in the web browser interface and is the "desktop name" for VNC clients.

17

Other identification details
These values are for information purposes. They are visible from the VNC client and via SNMP (if enabled).

Location
This string is sent as the system.sysLocation value over SNMP. It should describe the location of this system.

Contact Name
This string is sent as the system.sysContact value over SNMP. It should describe who to contact regarding this machine. Typically it includes an email address.

Network Address
This value is not used in our configuration, but is meant to store a user-defined value that identifies the controlled machine on the network. The official DNS name of the controlled machine is a obvious value to put here, but you may use it for any purpose.

Description
A user-defined description for the controlled machine.

Security

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.

Compatiblity

The **Compatibility** menu offers features that may offer enhanced functionality with certain KVM and power products, such as StarTech.com's Remote Power Switch (PCM8155HNA). These can be left at their default values if you are not connecting the unit to a KVM or power management device.

SNMP

The **SNMP** menu allows you to configure the SV1115IPEXT so it can be recognized and managed using industry-standard Simple Network Management Protocol software.

RADIUS

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.

18

RADIUS Configuration

Use RADIUS for login: Disabled

Servers

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): 2

Number of retries (per server): 3

Click here to save your RADIUS changes and apply them: Commit

Remember to enable RADIUS after configuring it. While RADIUS authentication is enabled, the locally defined accounts on the Server Remote Control unit 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.

Modem

Enable this to allow the modem to answer the phone and start a PPP connection.
Enable modem connections (PPP) via serial port/modem.

Serial Ports

The **Serial Ports** menu allows you to manage and connect to devices connected to the unit using the R-Port on the SV1115IPEXT.

Time/Date

Date and time are stored without consideration for time zone. If you are controlling multiple sites in different time zones, we recommend you use UTC (Universal Coordinated Time, also sometimes called GMT or Zulu) for all machines.
If the computer you are using to view this page knows the correct time, just press the button to set the time and date to the same time as your browser.

Firmware

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

Auto Self Upgrade
The SV1115IPEXT unit includes an innovative feature allowing it to upgrade itself over the Internet. Simply click on the button labeled **Upgrade to Latest** and the unit will go out to the Internet and download the latest version of the system firmware and then install it. If it cannot access the Internet directly (perhaps due to a web proxy or other firewalls), then a page will be shown that causes your

19

browser to download the required file. Save this file to disk and then upload it as described in the next section, **Manual Upload**.

Manual Upload

Enter the name of the firmware file that you downloaded 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 the unit before this operation completes successfully.
• 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, the upload could simply be slow.
• Each distributed file upgrades a different component of the system. Be sure to apply all files provided 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.

Auto Self Upgrade

Clicking the **Upgrade to latest** button will automatically download and install necessary revisions. To download upgrades for manual installation, please click on **Get latest version**.

Purchase Options

Certain firmware features may be offered separately from the base unit, in order to reduce the initial cost for the Server Remote Control unit.
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, such as: **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. Type 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.

Info
Status
Port Numbers
Help
Site Map
Copyright

The **Status** 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 provides a table allowing you to change TCP port values for services available on the SV1115IPEXT. By default, they are factory-set to common Internet values. You may wish to enhance security by disabling services that you will not use with the unit. To disable a service, change its port number to 0. For flexibility, both the LAN and WAN ports can be configured separately. When you have made any necessary

20

changes, click **Commit Changes** to use the settings the next time the SV1115IPEXT restarts. To force the unit to restart immediately, click **Restart Servers**.

Help Menu

Provides an FAQ (Frequently Asked Questions) listing to assist you with the features and operation of the SV1115IPEXT.

Site map Menu

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

Copyright Menu

Provides the Terms of Use and other information related to the firmware and software on the SV1115IPEXT.

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 SV1115IPEXT. While not intended to be a substitute for the Web interface, it does allow you to configure some of the same functions. The menu list below describes the options that can be modified through the terminal interface.

Note that you must use the **W** option to confirm and apply any changes made before you

```
---------------------------------
Server Remote Control Network Setup
---------------------------------


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

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

  DHCP is enabled. Current lease information:

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

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

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

Ethernet bridge: Disabled

Machine name: noname

Commands (press one key, then Enter):

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

  *  -> These values ignored due to DHCP.


Choice:
```

exit the terminal session. If you changed the status of the **Ethernet Bridging** feature, you will also need to power the SV1115IPEXT on and off again to enable your changes.

Accessing the VNC Interface

There are three ways to communicate with the Server Remote Control unit in order to control the host computer:

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

Web Interface

Using SV1115IPEXT's web 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 click on the **Connect** button, located in the Main Menu.

You may need to upgrade Java support in your browser; however, most modern browsers come with a version of Java that is compatible with this application. The Java VNC client makes a connection back to the Server Remote Control 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 are updated accordingly.

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 leading VNC clients.   Depending on your needs, there are several popular freeware, shareware, and commercial VNC clients available. Contact your system administrator or local software vendor for assistance. **NOTE**: Some native VNC clients may require a flag or setting indicating they should use

22

BGR233 encoding by default. If this flag is not set, you may see a garbled picture and the client will fail. The Unix versions of VNC require the flag -bgr233. For examples on using this flag, review the commands in the following section.

SSH Tunnel (with Native VNC client)

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

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

Same command, but using the WAN port:
ssh -f -l admin -L 15900:127.0.0.1:5900 10.0.0.98 sleep 60
vncviewer -bgr233 127.0.0.1::15900

Notes:
• A copy of these commands, with appropriate values filled in for your current system setting, is provided in the on-line help page. This allows you to "cut-and-paste" the required commands accordingly.
• You have 60 seconds to type the second command before the SSH connection will be terminated.
• The port number "15900" is arbitrary in the above example and can be any number (1025...65535). It is the port number used on your client machine to connect your local SSH instance with the VNC client. If you want to tunnel two or more systems, you will need to use a unique number for each instance on the same SSH client machine.
• Some Unix versions of the VNC client have integrated SSH tunneling support. Some clients require your local user id to be the same as the userid on the system.

Use a command like this: **vncviewer -bgr233 -tunnel 10.0.0.34:22**

Using the VNC Menu

One of the unique features of this product is the VNC menu system. Whenever you see a window with a dark blue background and grey edges, this window has been inserted into the VNC datastream so that it is effectively laid over the existing video. These menus allow you to control the many features of the SV1115IPEXT without using the web interface or a custom client.

Welcome Window

23

When you initially connect to the system, a **Welcome Window** will appear, indicating 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 known as 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 Server Remote Control unit. The second number measures round trip time (RTT) of the connection when it was first established.

Resync: Re-aligns the remote and local mouse points so they are on top of each other.

Redraw: Redraws the entire screen contents; occurs immediately.

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

USB: Resets the USB connection by simulating an unplug and replug. Forces operating system to recognize the USB keyboard, mouse and emulated disk drive.

÷4, ÷8: Switches to thumbnail mode, at indicated size (i.e. 1/8th, 1/4)

Ctrl-Alt-Del: Sends this key sequence to the host. Works immediately.

Alt-F4: Sends the key sequence to host (closes windows).

KVM: Sends the KVM "hotkey" sequence. This function is only enabled when you have configured the unit to expect a particular brand of KVM downstream. It sends the key sequence to launch the KVM's on-screen display (OSD) menu. This button is only present when a KVM model is selected in the Web interface.

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.

Disk: Shows the USB emulated disk menu.

24

In/Ej: Insert or eject the emulated USB disk. Enabled only if the host recognizes the USB disk.

R/W: Shows if the disk image is readable and/or writable. If the disk is readable, the **R** letter will be white. Whenever the host reads from the disk, the **R** letter will glow green for a few seconds. Whenever the host is writing to the disk, the **W** letter will glow for a few seconds.

8M: The type of USB disk selected is indicated here. The letters **Flpy** indicate floppy disk and **CD** indicates emulated CD-ROM.

PS/2: This area will show either PS/2 (as in this example) or USB to indicate if keyboard and mouse are being emulated via USB connection or PS/2 signals. If **Autosync** appears beneath this indicator, the mouse pointers on the local mouse and the VNC session will be synchronized automatically.

[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 that has a screen size 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 the 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, quickly 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:

25
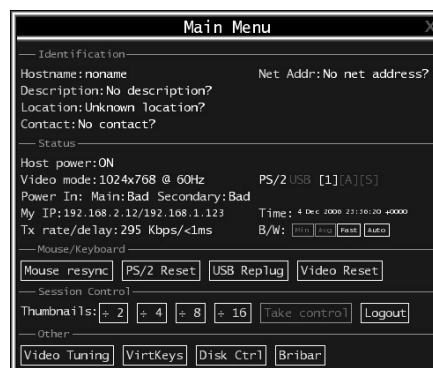
The main menu window may be moved by clicking and dragging on the title bar. It can be closed by pressing **Escape**, or by clicking on the red X in the top right corner.
Here is a guide outlining various fields from the Main Menu. Most of the functions operate immediately. Other functions require a 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 unit.

• **B/W Min/Avg/Max/Auto:** Bandwidth control. current operation will be indicated with white highlighting. If you choose **Min**/**Avg**/**Max** then you will override the default, Auto. As the automatic mode measures actual network performance, you may see the current mode switch from **Min** up to **Avg** or **Max**. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.

• **Mouse Resync:** Resynchronizes the mouse pointer so that the local and remote mouse pointers are on top of each other.

• **PS/2 Reset:** Resets the PS/2 emulation going to the host and to the attached PS/2 devices. This can be used if the mouse stops responding or the PS/2 keyboard isn't working.

• **USB Replug:** Simulates unplugging the USB connector and then plugging it back in. If the host is not recognizing USB input devices, this button may be used to restore functionality.

• **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. **Please note:** It is important that multiple users not be connected to the same physical network.

• **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 adjustment does not provide a good quality picture.

• **VirtKeys:** Virtual keyboard provides a menu with special keys that are often hard to generate but needed by the remote system. The most common key sequence is the [**Ctrl**] – [**Alt**] – [**Del**].

26

- **Disk Ctrl:** Emulated USB disk control submenu. Shows status of **floppy/Ramdisk** or CD-ROM and permits easy "insertion" or "eject".

- **KVM Menu:** Generates the key sequence used to access the on-screen menu for an enterprise-class KVM switch. When these conventional KVM switches are combined with the SV1115IPEXT, this key makes accessing their built-in menu easier, especially from the Java client. This button will only be shown when an external KVM has been enabled via the web interface.

- **Bribar:** Closes or reopens the Bribar window along the bottom of the screen.

VirtKeys Menu

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
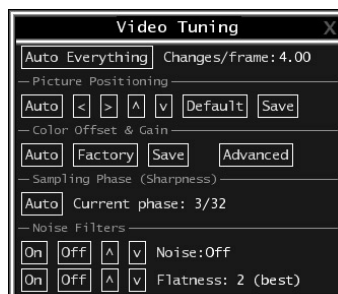
Use the **Auto Everything** button to automatically fine-tune all three adjustments. If the

27

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 host computer. Do not allow scaling, cropping or any other changes to that image. Press the **Auto** button and the system will calibrate color for the best possible picture in approximately one minute. If the system cannot find the test pattern on the screen, it will say so. Check that the pattern isn't scaled or covered up. It's important to perform this operation in 24-bit or 32-bit color video mode (i.e. truecolor). Although the algorithm may work in 16-bit or 8-bit color video modes, the results will not be optimum and usually it won't be able to 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 added control of the video settings of your VNC sessions.

Sampling Phase does not normally need to be used since SV1115IPEXT 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.

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

28

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 also be digitized and sent over the network. Quality video cards, in our experience, offer better performance simply because they don't add analog noise.

- Some external KVM switches generate video noise as well. Try to keep cables short, in order to reduce this effect.

- Enable the **Noise Filter** option (on the **Video Tuning** menu) to mitigate noise issues.

Network performance

- The SV1115IPEXT 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 unit will send as much data as your network connection and VNC client allow.

- Network latency, which is the total time it takes for a packet to get to the SV1115IPEXT and come back, has the biggest impact on perceived performance and usability. Network bandwidth has a lesser effect, particularly when just moving the mouse around. Only a few bytes need to be sent when the mouse is moving (and nothing else is changing on the screen), but the round-trip-time limits the hand-eye coordination of the user if it is too great. Both actual bandwidth and measured network latency are shown in the **Main Menu**.

Using the Advanced Video Tuning Feature
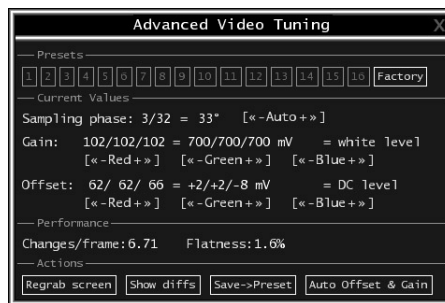
The **Advanced Video Tuning** menu allows you to adjust the qualities of the video in your VNC sessions, and can be accessed by clicking the **Advanced** button on the **Video Tuning** VNC menu. While many users will probably allow the SV1115IPEXT to automatically configure the video properties, you can use this menu to exercise a great

29

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, 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 cancelled.

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 or largest values, respectively. The '**<<**' and '**>>**' buttons decrease or increase 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 noise has on 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.

30

Disk Control Menu

```
┌────────────────────────────────────────┐
│         Disk Control            X       │
├────────────────────────────────────────┤
│ Status:Inserted: 8M Ramdisk             │
│                                         │
│ Access:Host broken? Not talking to USB disk. │
│  ┌──────┐ ┌─────┐ ┌───────────┐         │
│  │Insert│ │Eject│ │USB Replug │         │
│  └──────┘ └─────┘ └───────────┘         │
└────────────────────────────────────────┘
```

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

Using the IPMI Feature

Background
To offer a more complete remote server control solution, the SV1115IPEXT offers a power management feature that allows remote hardware restarts and the ability to power the host computer on and off. You may be able to take advantage of this feature if the host computer you are managing supports IPMI (Intelligent Platform Management Interface).

Host Computer Requirements
The host 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 host 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 host 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 host 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 host computer's operating system.

If the Host Computer Does Not Support IPMI
If the host computer you are managing with the SV1115IPEXT 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 Remote Power Switch (PM815NAS). For more information about this product, visit www.startech.com or

31

contact your local StarTech.com dealer.

Connecting the SV1115IPEXT for IPMI Control

You can use either serial port on the SV1115IPEXT to send IPMI access; your choice will determine the type of cable you will use to make the connection. The **DTE Serial** port on the front panel requires the use of a null modem serial cable. The **DCE Serial** port on the rear panel requires the use of a straight through serial cable.

Connect a female end of a serial cable to the serial port that is configured for IPMI access on the host computer. Connect the opposite end (male if connecting to the **DCE Serial** port, female if connecting to the **DTE Serial** port) to the SV1115IPEXT.

DTE Serial (Front Panel)   DCE Serial (Rear Panel)

Configuring IPMI on the SV1115IPEXT
Once you have connected the IPMI-configured serial port to the SV1115IPEXT and enabled the software option, you can begin to configure IPMI settings through the Web interface. 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).

You will be presented with the IPMI Status menu. Make the following changes to enable IPMI:

32

- Enable IPMI (Intelligent Platform Management Interface via serial port: select **Enabled**.

- Select which serial port to use: select either Front serial port (**DTE pin out**) or Rear serial port (**DCE pin out**) based on how the SV1115IPEXT is connected to the IPMI serial port on the host computer.

- Select baud rate to use: select a value from the menu between 9600 bps and 115,200 bps based on the configuration on the host computer's IPMI settings.

- BMC Password: Enter the password twice assigned to the BMC in the host computer's BIOS setup software.

Note that the selected baud rate should match the host computer's setting. Problems with the BMC password (as well as any other error information) will be recorded in the SV1115IPEXT's system log on the Status page of the Web interface. If the host 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 SV1115IPEXT allows you to monitor the status of the host 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 host computer being managed. 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 (shown above):

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

33

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

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.

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

From the **Home** screen:

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 host computer.

Turn ON: Powers on the host computer.

Turn OFF: Powers off the host computer.

Pulse Diag Int: Restarts operating system on host computer.

Graceful off: Powers down operating system on host computer.

From the **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 host computer on or off depending on the current state of the host computer; equivalent to pressing the POWER button on the host computer.

NOTE: IPMI may not automatically close the host 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.

Using the Modem Feature

Background
The modem feature allows the SV1115IPEXT to act as an Internet connection server for

34

increased security and flexibility in connecting with the host computer. Unlike the TCP/IP connection used with the standard Web configuration and VNC clients, the modem creates a one-to-one connection between the SV1115IPEXT and the computer you are using to manage the host computer that is essentially private, as it bypasses the public Internet completely. **Note:** this feature 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 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.

Connecting a Modem

The SV1115IPEXT 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 SV1115IPEXT.

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 SV1115IPEXT, but simply reflect the line conditions at the time the connection is made.

The **DTE** Serial port on the front panel can be used for serial port configuration when the modem is connected. It requires the use of a null modem serial cable.

The **DCE** Serial port on the rear panel is used to connect the modem to the

35

SV1115IPEXT and requires the use of a straight through serial cable.

Rear Panel (DCE Serial port)

Front Panel (DTE Serial port)

Place the modem near the SV1115IPEXT 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 **DCE** Serial connection on the rear panel of the SV1115IPEXT.

Modem configuration
Although most connections will work appropriately with the default settings on SV1115IPEXT, manual changes can be made. To do so:

Login to the Web interface as **Admin**. Click **Modem**, listed on the left side of the main page. 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 SV1115IPEXT'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 initialization ("init") string is the command (using the standardized Hayes AT command set) that the SV1115IPEXT 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.

36

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 SV1115IPEXT. 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 SV1115IPEXT'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 SV1115IPEXT. 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.**

•   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 SV1115IPEXT.
•   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

37

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 SV1115IPEXT, 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 or WAN ports:

> **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 in 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 host computer's desktop to make the dial-up connection as efficient as possible.

- When the modem feature is enabled, you can use a "line modem" connection on the serial port using a serial cable to begin a PPP session. If you are using the DTE Serial port on the front panel, use a null modem serial cable. If you have disconnected the modem and are using the DCE Serial port on the rear panel for the PPP connection, use a straight through serial cable. When the modem is not actively connected, you can begin a PPP session at up to 460 kbps. To hang up and re-connect the modem, end the PPP session.

- If you need to configure the device over a serial connection while the modem option is enabled, connect a serial cable (see immediately above for instructions on what type of cable to use for the port you are accessing on the SV1115IPEXT) and begin a terminal session following the instructions under **Terminal Configuration Using a Serial Cable** in this manual. Once connected, you will see the following message:

Expecting a modem, if human, type admin password (Or start PPP)

Type the password for user **admin** and press **Enter**. The password will not appear on the screen. The configuration menu will appear. Make the changes you wish or press **q** and **Enter** to exit and leave the modem connection active.

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.

38

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 SV1115IPEXT. 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: xxxxxxxxx
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. Using Optional Serial Remote Control (R-Port) Modules

Serial Remote Control operation

Background
The SV1115IPEXT offers a unique way to expand the functionality of the base product. Using the integrated **R-Port** on the rear panel, you can manage up to 8 serial devices using a specialized daisy-chain technology. The SV1115IPEXT 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 modules 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 Serial Remote Control Modules to the SV1115IPEXT
The cable for each serial device is similar to a phone cable and uses an RJ-14 connector. For the first module, connect the cable (provided) to the **R-Port** on the rear panel of the SV1115IPEXT. Connect the opposite end to the **DATA OUT** (or similar) port on the Serial Remote Control unit. 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 SV1115IPEXT, you can connect additional modules to the **DATA IN** (or similar) port on the previous module in the chain. Once the cabling is attached, the module 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.

39

Configuring/Viewing Serial Remote Control Modules through the Web Interface
Once you have one or more R-Port serial devices connected, you will able to configure and manage them through the Web interface. You may need to modify the default settings on SV1115IPEXT to match your various R-Port modules' default configuration. Consult the documentation that came with your R-Port module to determine if you need to modify the default settings to complete the installation. To be able to configure your R-Port modules, you must be logged in as **admin**. Other users will be able to view which modules 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:

#: You can assign a value (**1** ~ **99**) to each attached serial remote control module. 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 module. 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 module itself. All common baud rates between 300 and 115,200 bps are supported.

Mode: Sets the character framing scheme that the SV1115IPEXT will use with the R-Port module. 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.

IPMI: Shows the IPMI command interface for the device, if applicable.
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

40

attached R-Port modules.

Advanced Configuration Using the Integrated SSH Shell
In most cases, configuring the SV1115IPEXT 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 module in a live terminal session. Commands you type will be echoed on the terminal screen. The module also offers a simple menu system that allows you to change its configuration settings (similar to the function of the menus in a terminal software package). 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)
        1 – 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. These commands are not sent to the device you are managing and relate to the RPORT module itself.

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 SV1115IPEXT using port 22 (default).

Log 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 devices you wish to manage).   Alternatively, you can enter the command **connect -l** to see a list of active devices.

Operating Notes
• If the power supply to the R-Port modules you have connected becomes faulty (short, overload) then the R-Port LED on the front panel of the SV1115IPEXT will show red.

41

Under normal operations, this light should remain green. The R-Port connector on the rear panel also has an LED that mirrors the status of the light on the front panel. (Note: The rear LED status was reversed on some early units, where red=normal and green=fault. This does not affect operation in any way, but a green LED on the front panel and a red LED on the rear panel indicates that you have one of these units.)

• Hardware handshaking (CTS/RTS) is required for speeds exceeding 9600 bps. It is enabled by default on the SV1115IPEXT, but may need to be enabled on the other end of the connection. For Unix systems, the command is:

stty –crtscts < /dev/[serial port]

• A maximum of four users may simultaneously login to the same module. 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 modules may be connected at any one time*.

• *You plug-in and unplug any R-Port module 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 module while deactivated, but will not be available to users until it is re-initialized*.

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 SV1115IPEXT?
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 SV1115IPEXT. 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 SV1115IPEXT 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

42

will no longer generate a warning if that option is selected. Second, if you install the certificate from the SV1115IPEXT onto the host computer (see below) and if the unit is configured with a domain name ending in .com, .net, .org, .gov, .edu, .us, .ca, .uk, .jp, or .tw (i.e. remotecontrol.mydomain.net) then the warning should no longer occur.

Installing the new certificate…
The following instructions detail how to install the certificate from the SV1115IPEXT onto your local computer (in this case, when using Internet Explorer with Windows XP).

1. Open your Web browser and go to the SV1115IPEXT 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**.

Troubleshooting

Forgotten master password.
You can reset the master password using the serial interface on the unit. Use the **S** command, and type a new password. The old password is not required for this procedure.

Remote mouse and local mouse don't line up.
Use the Mouse resync command in the main menu or press the Resync button on the Bribar. If the mouse pointers still don't line up, verify that mouse acceleration has been disabled.

NOTE: The Windows login screen does not accept the "mouse acceleration" configuration, and always has the mouse accelerated regardless of your configuration. Therefore, on this screen it is best to avoid using the mouse.

After resync, the mouse pointers are still not aligned.
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.

43

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 SV1115IPEXT uses 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.

Don't set LAN and WAN to the same IP Address.
This type of installation will not work. If you want to use both ports in redundant mode, enable the Ethernet bridging option and plug both into the same network. The WAN IP address is not used in that configuration.

Mouse performance is erratic when using the GNOME or KDE desktop in a Linux X-Window environment.
The mouse controls in GNOME and KDE environments offer both an acceleration and sensitivity setting. The following directions correct this issue, and apply to Red Hat Fedora Core 2, but should be similar for other distributions that use GNOME or KDE:

1.   Click the Launch menu icon.
2.   Choose **Preferences** > **Mouse**.
3.   Click the **Motion** tab.
4.   Set the **Acceleration** bar to the setting immediately left of center.
5.   Set the **Sensitivity** bar to the leftmost settings (lowest possible)

44

Specifications

General Specifications

Maximum supported video mode	1600 x 1200 @85Hz
Standard video modes supported	640x400 @ 85Hz 720x400 @ 85Hz 640x480 @ 60Hz, 72Hz, 75Hz, 85Hz 800x600 @ 56Hz, 60Hz, 72Hz, 75Hz, 85Hz 1024x768 @ 60Hz, 70Hz, 75Hz, 85Hz 1152x864 @ 75Hz 1280x960 @ 60Hz, 85Hz 1280x1024 @ 60Hz, 75Hz, 85Hz 1600x1200 @ 60Hz, 65Hz, 70Hz, 75Hz,
Maximum power consumption	15 Watts (5VDC, 3A)
Input Connectors	Video In PS/2 Keyboard PS/2 Mouse USB 'A' x 3 USB 'B' x 1 LAN (RJ45) WAN (RJ45) R-Port (RJ11) DB9 RS-232 Female (Serial DCE) DB9 RS-232 Male (Serial DTE) DC IN (2, with redundancy)
Regulatory certifications	FCC Class A, CE, ROHS

Specifications - Cont'd

Supported Protocols

Service	Description	Benefit
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.

46

About StarTech.com

StarTech.com is "The Professionals' Source for Hard-to-Find Computer Parts". Since 1985, we have been providing IT professionals with the quality products they need to complete their solutions. We offer an unmatched selection of computer parts, cables, server management solutions and A/V products and serve a worldwide market through our locations in the United States, Canada, the United Kingdom and Taiwan.

Visit **www.startech.com** for complete information about all our products and to access exclusive interactive tools such as the Parts Finder and the KVM Reference Guide. StarTech.com makes it easy to complete almost any IT solution. Find out for yourself why our products lead the industry in performance, support, and value.

Revised: 18 May 2007 (Rev. A)

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com