USTIP

P2-USTIP1, P2-USTIP2

Release 1.2.1.5.3

User Guide

USTIP-0F-v1.2.1--E
March 2011
255-30-6000

This page intentionally left blank.

Copyright and Trademark Information

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial 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. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

CE c UL us LISTED 1F61 I.T.E.

For assistance in the North or South America, please contact the Raritan Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail tech@raritan.com

Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, Eastern.

For assistance around the world, please see the last page of this guide for regional Raritan office contact information.

Power Safety Guidelines

To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup UPS, power the computer, monitor and appliance off the supply.

Rack Mount Safety Guidelines

In Raritan products which require Rack Mounting, please follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the appliances (see **Appendix A: Specifications**).
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, such as power strips (other than direct connections), to the branch circuit.

Login

- The default USTIP login user name is **admin**, and the default password is **raritan**. This user has administrative privileges.
- Passwords are case sensitive and must be entered in the exact case combination in which they were created.
- The default password **raritan** must be entered entirely in lowercase letters.
- To ensure security, change the default password as soon as possible. The new password can comprise a maximum of 8 characters.

Default IP Address

- USTIP ships with the default IP address of 192.168.0.192

Firmware

- This manual applies to USTIP TRS Firmware version 4.5.0.5.12 and above.

Contents

Figures

Chapter 1: Introduction

USTIP Overview

Thank you for purchasing Raritan's USTIP, the industry-leading solution for multi-platform, high-performance, network-based, remote KVM console access. This product is a critical part of Raritan's Paragon family, which is designed for managing multiple servers of different platforms.

USTIP enables highly-secure, multi-user, bandwidth-efficient, and software-independent access to your servers' KVM consoles via a web browser for one or two users. It uses Raritan's powerful frame-grabber and Video Compression Algorithm to capture, digitize, and compress the video signal before transmitting to a remote PC. The remote user has direct access and total control of target servers for maintenance, administration, and trouble-shooting, from running GUI applications to BIOS-level troubleshooting, and even rebooting.

A Paragon II system consists of several components: Main switching units (M Units), which serve as base units and matrix switches, securely connecting users to servers; Stacking units (S Units), which allow you to expand your system and connect to the M Units while conserving space; Computer-Interface Modules (CIMs) connected to each server; and either the User Station (P2-UST), which connects your keyboard, monitor, and mouse to the M unit and provides an intuitive On-Screen User Interface for accessing attached servers, or the Enhanced User Station (P2-EUST), providing all of the P2-UST features, plus superior video quality with manual skew compensation.

In addition, the P2-USTIP1 and P2-USTIP2, one-and two-worker user stations, have integrated IP access and includes KVM over IP capability for anytime, anywhere access and control of servers along with a slim design and GUI for point-and-click remote access. The P2-USTIP supports IP access, enabling one or two remote users to access Paragon II-connected servers from anywhere via Web browser. The P2-USTIP2 also supports 128-bit SSL encryption and local authentication through Paragon II, or centralized authentication when used with Raritan's CommandCenter Secure Gateway.

Use USTIP for convenient access to servers anytime, from anywhere:

- Control servers from within the building or across a campus
- Manage servers at branch offices from a central site
- Provide remote support for worldwide data centers
- Troubleshoot, reconfigure, and reboot servers from home
- Provide convenient and secure lights-out server management

Access via Internet, LAN/WAN, or dial-up Modem

USTIP provides a broad array of remote access methods to control any server connected to a Raritan KVM Switch. Since servers can also be accessed out-of-band with USTIP, remote access to mission-critical target servers is always available - even if the network is down.

For reading ease, P2-USTIP1 and P2-USTIP2 units are called simply "USTIP."

Product Photos

Figure 1 Front and Rear Views of the P2-USTIP

Figure 2 P2-USTIP1 Unit with Paragon UMTs

Figure 3 P2-EUST, P2-UST, and P2-USTIP1 Units

Product Features

Access

- Remote KVM access via the Internet, LAN/WAN, or dial-up modem
- Simultaneous switch or server access by up to two users
- Web browser accessible
- Remote access to serial devices (VT100) connected to USTIP serial port

Performance

- Superior compression algorithm for exceptional performance
- No impact on target server performance
- Automatic sensing of video resolution for optimum display
- High-performance mouse tracking and synchronization

Reliability

- External modem using a dedicated modem port allows servers to be accessible even if network is unavailable

Security

- SSL 128-bit RSA public key, 128-bit RC4 private key encryption
- Single, configurable TCP port for firewall protection

Administration

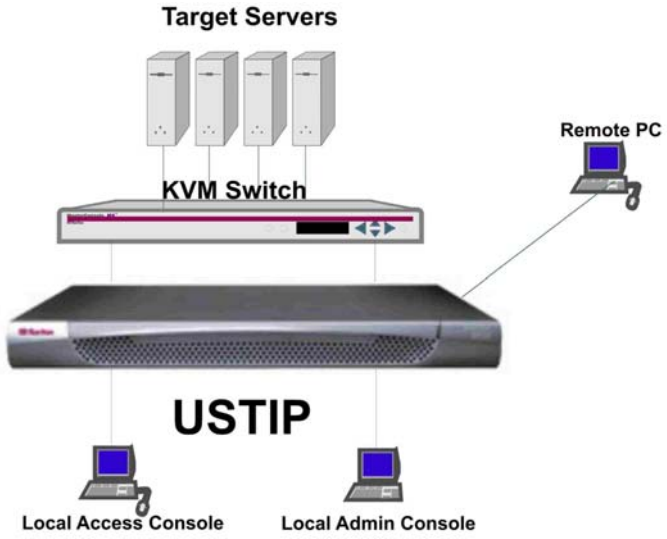
- Remote Administration via Web Browser interface
- Simplified installation and user interface
- User console for direct analog access to KVM switch
- Extensive downloadable user event log
- DHCP or fixed IP addressing
- Supports Raritan's CommandCenter-Secure Gateway and PCCI, Raritan's Paragon–CommandCenter Integration

Others

- Supports the use of a 121-key Cortron rugged keyboard (part number 536-0062) at the local side
- Supports the newest daylight saving time (DST) starting from 2007 for US

Terminology

This manual makes use of the following terms to indicate components of a typical USTIP configuration. While reading the manual, please refer to the diagram below for clarification when necessary. This manual uses the following terms.



Target Server(s)	Servers to be accessed remotely via USTIP and its connected KVM configuration.
Remote PC	A Windows-based computer used to access and control target servers connected to USTIP.
Local Access Console	A user console consisting of a PS/2 keyboard, PS/2 mouse, and VGA monitor, directly attached to USTIP to control target servers locally (not through the network). Single-port USTIP models (USTIP1) allow connection of one local access console.
Local Admin Console	A VT100 terminal directly attached to USTIP's **Admin** port, is used for administration and setup. From this console, you can access USTIP administration menus directly. You cannot view Target Servers of the connected KVM configuration using this screen. Although USTIP also allows remote administration via the network, the local admin console provides the most convenient means to perform initial setup.

Chapter 2: Installation

Configuring Target Servers

Before installing USTIP, first configure any target servers that you wish to access via USTIP, in order to ensure optimum performance, as outlined below. Note that the following configuration requirements apply only to *target servers*, not to the computers that you will be using to access USTIP remotely.

Server Video Resolution

For optimal bandwidth efficiency and video performance, target servers running graphical user interfaces such as Windows, X-Windows, Solaris, and KDE should be configured with desktop backgrounds set to a predominantly solid, light-colored graphic. Backgrounds featuring photos or complex gradients should be avoided.

Ensure that the server's video resolution and refresh rate are supported by USTIP, and that the signal is non-interlaced. USTIP supports the following video resolutions:

Text Modes	
640x480 @ 60Hz	1024x768 @ 60Hz
640x480 @ 72Hz	1024x768 @ 70Hz
640x480 @ 75Hz	1024x768 @ 75Hz
640x480 @ 85Hz	1024x768 @ 85Hz
720x400 @ 70Hz	1152x864 @ 60Hz
720x400 @ 85Hz	1152x864 @ 70Hz
800x600 @ 56Hz	1152x864 @ 75Hz
800x600 @ 60Hz	1280x960 @ 60Hz
800x600 @ 72Hz	1280x1024 @ 60Hz
800x600 @ 75Hz	
800x600 @ 85Hz	

Windows XP Settings

On target servers running Microsoft Windows XP, disable the "Enhanced Pointer Precision" option, and set the mouse motion speed exactly to the middle speed setting. These parameters are found in: **Start → Control Panel → Mouse → Pointer Options**.

Note: *For Target Servers running Windows NT, 2000, or XP, you may wish to create a username to be used only for remote connections through USTIP. This allows you to keep the Target Server's slow mouse pointer motion/acceleration settings exclusive to the USTIP connection only, as other users may desire faster mouse speeds.*
Windows XP and 2000 login screens revert to pre-set mouse parameters that differ from those suggested for optimal USTIP performance; therefore, mouse sync will not be optimal at these screens. If you are comfortable adjusting the registry on Windows target servers, you can obtain better USTIP mouse synchronization at login screens by using the Windows registry editor to change the following settings: Default user mouse motion speed = 0; mouse threshold 1= 0; mouse threshold 2 = 0.

Windows 2000 / ME Settings

On target servers running Microsoft Windows 2000 / ME, set the mouse pointer acceleration to "none" and the mouse motion speed exactly to the middle speed setting. These parameters are found in: **Start → Settings → Control Panel → Mouse → Motion**.

Windows 95 / 98 / NT Settings

On target servers running Microsoft Windows 95 / 98 / NT, set the mouse motion speed to the slowest setting in **Start → Settings → Control Panel → Mouse → Motion**.

Linux Settings

On target servers running Linux graphical interfaces, set the mouse acceleration to exactly 1 and set threshold to exactly 1.

As mentioned above, please ensure that each target server running Linux is using a resolution supported by USTIP at a standard VESA resolution and refresh rate. Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values.

To check for these parameters:

- Go to the Xfree86 Configuration file XF86Config
- Using a text editor, disable all non-USTIP supported resolutions
- Disable the virtual desktop feature, which is not supported by USTIP
- Check blanking times (+/- 40% of VESA standard).
- Restart computer

Note: *In many Linux graphical environments, the command* ***CTRL****+****ALT****+ + [plus sign key] will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.*

Sun Solaris Settings

All target servers must be configured to one of the display resolutions supported by USTIP. The most popular supported resolutions for Sun machines are:

- 1024x768@60Hz
- 1024x768@70Hz
- 1024x768@75Hz
- 1024x768@85Hz
- 1152x900@66Hz
- 1152x900@76Hz
- 1280x1024@60Hz

Target servers running the Solaris operating system must output VGA video (H-and-V sync, not composite sync). To change your Sun video card output from composite sync to the non-default VGA output, first issue the **Stop+A** command to drop to bootprom mode. Then, issue the command:

```
setenv output-device screen:r1024x768x70
```

to change the output resolution. Issue the "boot" command to reboot the server.

Alternatively, you may contact your Raritan representative to purchase a video output adapter. 13W3 Suns with composite sync output require APSSUN II Raritan guardian for use with USTIP. HD15 Suns with composite sync output require 1396C Raritan converter to convert from HD15 to 13W3 and an APSSUN II Raritan guardian converter to support composite sync. HD15 Suns with separate sync output require an APKMSUN Raritan guardian for use with USTIP.

Note that KVM switch brands other than Raritan's may or may not properly handle PS/2-to-Sun signals.

On target servers running the Solaris operating system, set the mouse acceleration value to exactly 1 and threshold to exactly 1. Set this at the graphical user interface (shown below), or with the command line "xset mouse a t" where "a" is the acceleration and "t" is the threshold.

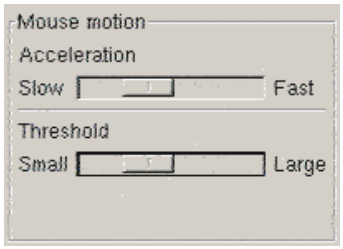


Figure 4 Set Mouse Motion

Apple Macintosh Settings

For target servers running an Apple Macintosh operating system, while using USTIP to access and control your target server, you must set the USTIP client (Raritan Remote Client) to "single cursor" mode. Dual cursor mode is not supported, and the two mouse pointers will not appear in sync if you attempt to control a Macintosh server via USTIP in dual cursor mode.

Configuring Network Firewall Settings

If you wish to access USTIP through a network firewall, your firewall must allow communication on TCP Port 5000. Alternatively, USTIP can be configured to use a different TCP port of your own designation (see **Chapter 3: Administrative Functions, *Network Configuration***).

In order to take advantage of USTIP's web-access capabilities, the firewall must allow inbound communication on TCP Port 443 – the standard TCP port for HTTPS communication. In order to take advantage of USTIP's redirection of HTTP requests to HTTPS (so that users may type the more common, "http://192.168.0.192", instead of "https://192.168.0.192"), then the firewall must allow inbound communication on TCP Port 80 – the standard TCP port for HTTP communication.

Physical Connections

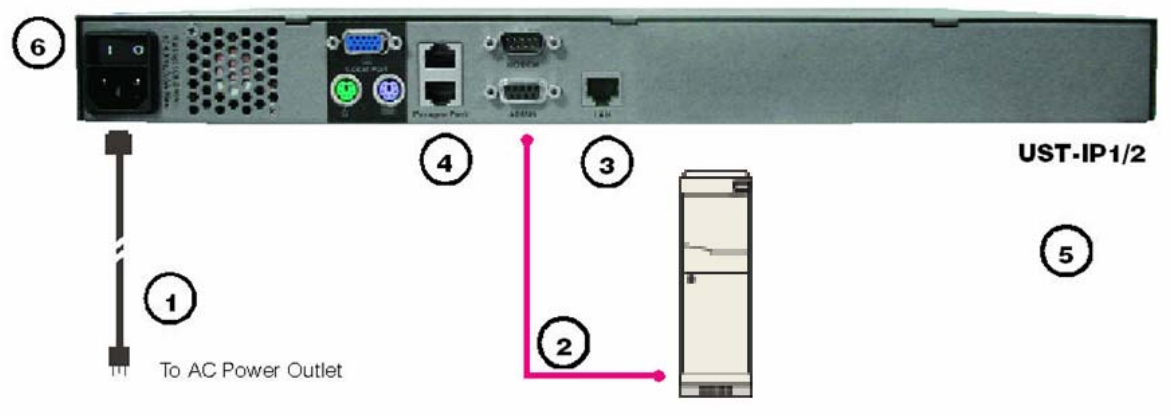


Figure 5 P2-USTIP2 Rear Panel Connections

Attaching a Local Console for Initial Configuration

1. Attach the included AC power cord to the USTIP unit and plug the other end into a nearby AC power outlet.
2. Connect the client PC to the USTIP ADMIN Port using a serial (DB9) cable.
3. Connect a standard Ethernet cable from the Network Port to an Ethernet switch, hub, or router.
4. On a USTIP1 unit, connect the single Paragon port to the User port on your UMT unit using a CAT5 cable. On a USTIP2 unit, connect both the upper and the lower Paragon ports to User ports on your UMT unit using CAT5 cables. The upper Paragon port allows you to download the Paragon database to the USTIP unit, and the lower Paragon port allows local access to the Paragon unit.
5. Launch a HyperTerminal session from the client PC. To access the Serial Admin Port, use HyperTerminal to configure specific settings with the following steps:
   A. In Windows, click on the **Start** menu in the lower left corner, then click **Programs → Accessories → Communications → HyperTerminal** to start a session.
   B. Name the HyperTerminal session, select a session icon - if required - and then click **OK.**
   C. In the **Connect To** window, click on the **Connect Using** drop-down arrow and select **COM1** (or other option, depending on where your PC's serial cable is connected) and click **OK.**
   D. In the **COM1 Properties** window, click on the **Port Settings** tab. Make sure the **Bits per second** is set to **115200** and **Flow control** is set to **NONE.** Click **OK.**
   E. On the **File** menu, click **Properties**; click on the **Settings** tab, then click on the **Emulation** drop-down arrow and select **VT100.**
      i. Click **ASCII Setup** and ensure that the checkbox before **Wrap lines that exceed terminal width** is checked.
      ii. Click **OK.**
      iii. Click **Terminal Setup** and ensure that the checkbox before **Keypad application mode** is checked.
      iv. Click **OK.**
   F. Click **OK.**
6. Power ON USTIP.

***Note**: HyperTerminal is not available in Windows Vista. For Windows Vista users, you can download the free terminal emulation software PuTTY from Internet for serial connection.*

Initial Configuration

During initial configuration, the **USTIP Setup Wizard** helps you quickly set up USTIP for the first time. The USTIP Setup Wizard appears only when accessing the Administrative Menus on a non-configured USTIP, and guides you through initial configuration parameters. The easiest way to perform this initial configuration is by using the Local Admin Console (see 'Physical Connection' instructions in the previous sections).

1. Power ON USTIP via the power switch on the back of the USTIP unit.
2. The Welcome to USTIP Setup Wizard Screen will appear on the Local Admin Console.

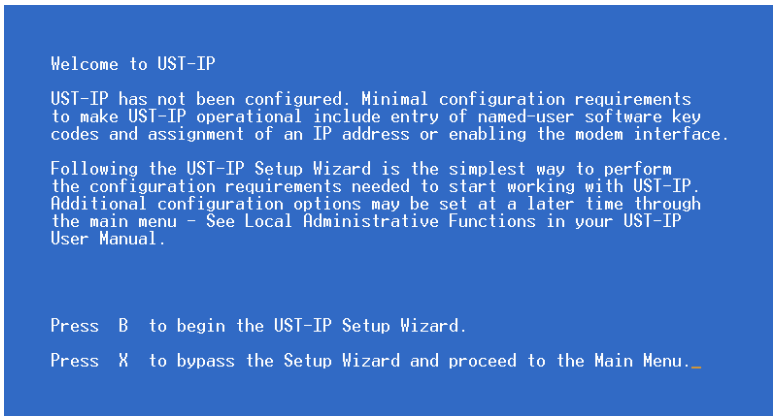


Figure 6 USTIP Wizard Screen

3. Press the letter **B** on the Local Admin Console keyboard to begin the USTIP Setup Wizard.
4. The Network Configuration Screen appears.

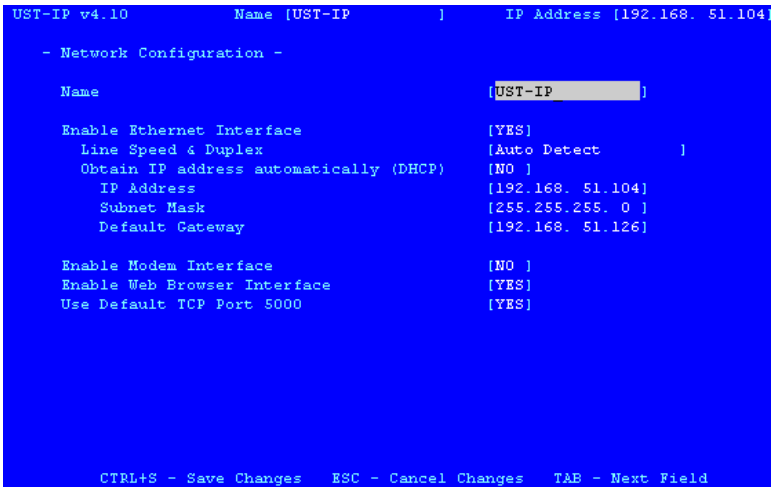


Figure 7 USTIP Network Configuration Screen

5. Use the **Tab**, ↑ or ↓ keys to select each line on the Network Configuration screen and the **space bar**, or the ← or → keys to toggle between available entries. Press the **Enter**, **Tab** or ↓ keys when your entry on each line is complete. Below are descriptions of each field, and the appropriate values to assign.

- **Name**: Designate a unique name for this USTIP unit, for example, "MiamiDataCenter." Please note that this name should contain only alphanumeric characters, no spaces or symbols permitted. The default name is **USTIP**.
- **Enable Ethernet Interface**: Designates whether USTIP should enable its Ethernet adapter as active (default: YES).

***Note:** Network connections must be 10BASE-T or 100BASE-TX Ethernet*

- **Line Speed & Duplex:** Enter the visual efficiency for the monitor:
  - Auto detect 10 Mbps/Full Duplex
  - 10 Mbps/Half Duplex
  - 100 Mbps/Full Duplex
  - 100 Mbps/Half Duplex
- **Obtain IP address automatically (DHCP):**
  - **YES:** Enables dynamic IP addressing for USTIP. Each time USTIP boots, it requests an IP address from the local DHCP server. Note that this setting can make remote access to USTIP from outside the LAN difficult, since the dynamically assigned IP address must be known in order to initiate a connection.
  - **NO (default)**: Assigns a fixed IP address to the USTIP unit (recommended).
    - **IP Address**: Type the IP address for USTIP given by your Network Administrator.
    - **Subnet Mask**: Type a Subnet Mask provided by your Network Administrator.
    - **Default Gateway**: Type the Default Gateway if your Network Administrator specifies one.
- **Enable Modem Interface**: Enables Dial-up Modem access (default: YES). For USTIP, an external serial modem must be connected in order for this function to work properly.

- **Enable Web Browser Interface**: Enables Web browser access to USTIP (default: YES).
- **Use Default TCP Port 5000:**
  - **YES (default):** Utilizes the default port 5000.
  - **NO:** Enter an alternate port number.

***Note:** In order to access USTIP from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000 or the non-default port configured above.*

6. Press **CTRL+S** to save entries. The Main Menu will appear.
7. On the Main Menu, select **[R] Restart or shutdown the USTIP**, and press **ENTER.**
8. When prompted, press the letter **R** on your keyboard to restart USTIP.
9. USTIP will restart and the USTIP Initialization screen appears upon boot up.
10. USTIP is now ready for initial connection.

Accessing USTIP Local Admin Port

To access the local admin console port from your USTIP device, use HyperTerminal to configure specific settings for a PC and at least one additional setting for a laptop computer. Please perform the following steps:

1. In Windows, click on the **Start** menu. Click **Programs,** then click **Accessories,** click **Communications,** and then click **HyperTerminal** to start a session.
2. Name the session, select a session icon if required, and click **OK.**
3. In the Connect To window, click on the **Connect Using** drop-down arrow and select **COM1** (or other option, depending on where your PC's serial cable is connected).
4. Click **OK.**
5. In the COM1 Properties window, click on the **Port Settings** tab:
   A. Click on the **Bits per second** drop-down arrow and select **115200.**
   B. Click on the **Flow control** drop-down arrow and select **NONE.**
   C. Click **OK.**
6. On the **File** menu, click **Properties,** and then click on the **Settings** tab:
   A. Click on the **Emulation** drop-down arrow and select **VT100.**

B. Click **ASCII Setup.** In the ASCII Setup window, ensure that only the option **Wrap lines that exceed terminal width** is checked. If any other options are checked, you may have display issues.
C. Click **OK.**
D. Click **Terminal Setup.** In the Terminal Settings window, ensure the option **Keypad application mode** is checked (this option must be specified for most laptop computers).

7. Click **OK.**
8. Click **OK.**

Remote Connection Using Raritan Multi-Platform Client and Raritan Remote Client

After installing USTIP, establish an initial network connection using Raritan Multi-Platform Client (MPC) or Raritan Remote Client (RRC). MPC and RRC are Raritan's graphical user interfaces for USTIP, IP-Reach, and Dominion KX products, providing remote access to the target servers connected to Raritan KVM over IP devices. Both can be installed to use stand-alone, or accessed remotely.

Non-Windows users must use Raritan Multi-Platform Client, and Windows users running Internet Explorer must use Raritan Remote Console.

Note: *Please see the* ***Raritan Multi-Platform Client and Raritan Remote Client User Guide,*** *available on Raritan's Website http://www.raritan.com/support/productdocumentation, or on the Raritan User Manuals & Quick Setup Guides CD ROM included with your Dominion KX shipment for details on installing and operating MPC and RRC as standalone applets or for remote access.*

MPC Requirements

All installations of Raritan MPC require Sun Microsystems' Java Runtime Environment (JRE) version **1.4.2_05** or greater. You may need some configuration depending on your OS and browser; configuration instructions are provided with the JRE download.

Determine your version of the JRE on the Java webpage:
http://www.java.com/en/download/help/testvm.xml

Note: *Raritan does not support JRE version 1.5.0_02 and 1.6 for use with MPC.*

Supported Browsers

MPC supports the following browsers:

- Internet Explorer 6, 7 and 8
- Firefox® 1.5, 2.0 and 3.0
- Mozilla® 1.7
- Safari 2.0

Launching MPC

To launch MPC from a machine running any browser except Internet Explorer, type **http://<IP address>** into the address line, where **<IP address>** is the IP address of your Raritan device. Please note that the MPC applet will launch in a new window that **does not** contain a Menu bar, Tool bar, Scroll bar, or Address bar. If you are running Windows, toggle to other open windows using the command **ALT+TAB.**

You can install MPC as a standalone applet, described further in the **Raritan Multi-Platform Client and Raritan Remote Client User Guide**.

Important: You must disable any pop-up blockers in order to launch MPC.

Launching RRC

Important: RRC works only with MS Internet Explorer. If you are using a different Web browser, MPC will load automatically.

1. Log on to any Windows-based computer with network access to USTIP.
2. If you are using Windows NT, 2000, XP, or 2003, ensure that you are not a "restricted" user.
3. Launch Microsoft Internet Explorer (ensure that your Internet Explorer security settings allow the download and execution of ActiveX controls).

***Note:** The IE default security setting of **Medium** is sufficient.*

4. In the Internet Explorer Address bar, type the IP address assigned to the USTIP. Press **ENTER** to load and launch the web access client, **Raritan Remote Client (RRC)**.

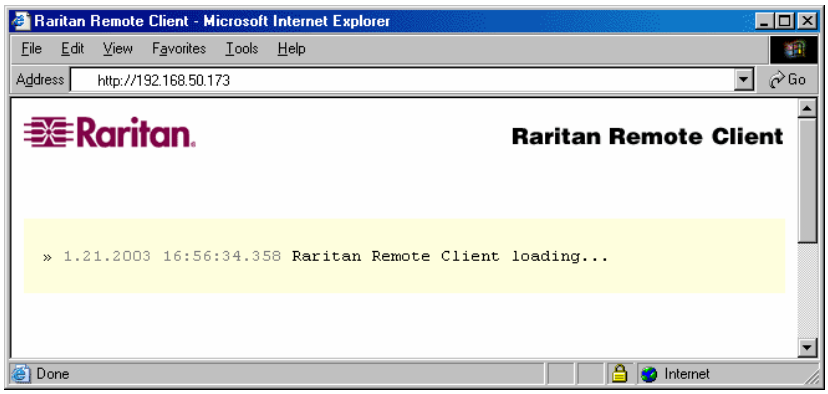


Figure 8 RRC Connection Window

5. After RRC launches, a device tree of all automatically detected Raritan devices found on your subnet is displayed on the left side of the screen. If you do not find your USTIP unit listed by name, create an icon manually by selecting **Connection → New Profile**.
6. Double-click on the icon that corresponds to your USTIP unit.

Establishing a Connection

When you double-click on your USTIP icon, its login screen appears. Log on with your username and password (default: **admin/raritan**) to connect to your USTIP unit. Use the Navigator, on the left side of the MPC or RRC window, to select and connect to a server port.

Note: *When changing the default password through RRC or MPC, make sure the new password consists of 8 or less characters because UMT only accepts a maximum of 8 characters for the password. For password change instructions, see the "KVM and Serial Access Clients" user guide, which can be downloaded from the Raritan website at the following URL -- http://www.raritan.com/support/dominion-kx-ii/v-2-1-8/user-guides/.*

Please note that the RRC window shown below is slightly different from the MPC window: the MPC window has a Message panel below the Navigator. The Message panel offers a simplified log display of connection attempts and other significant system events.

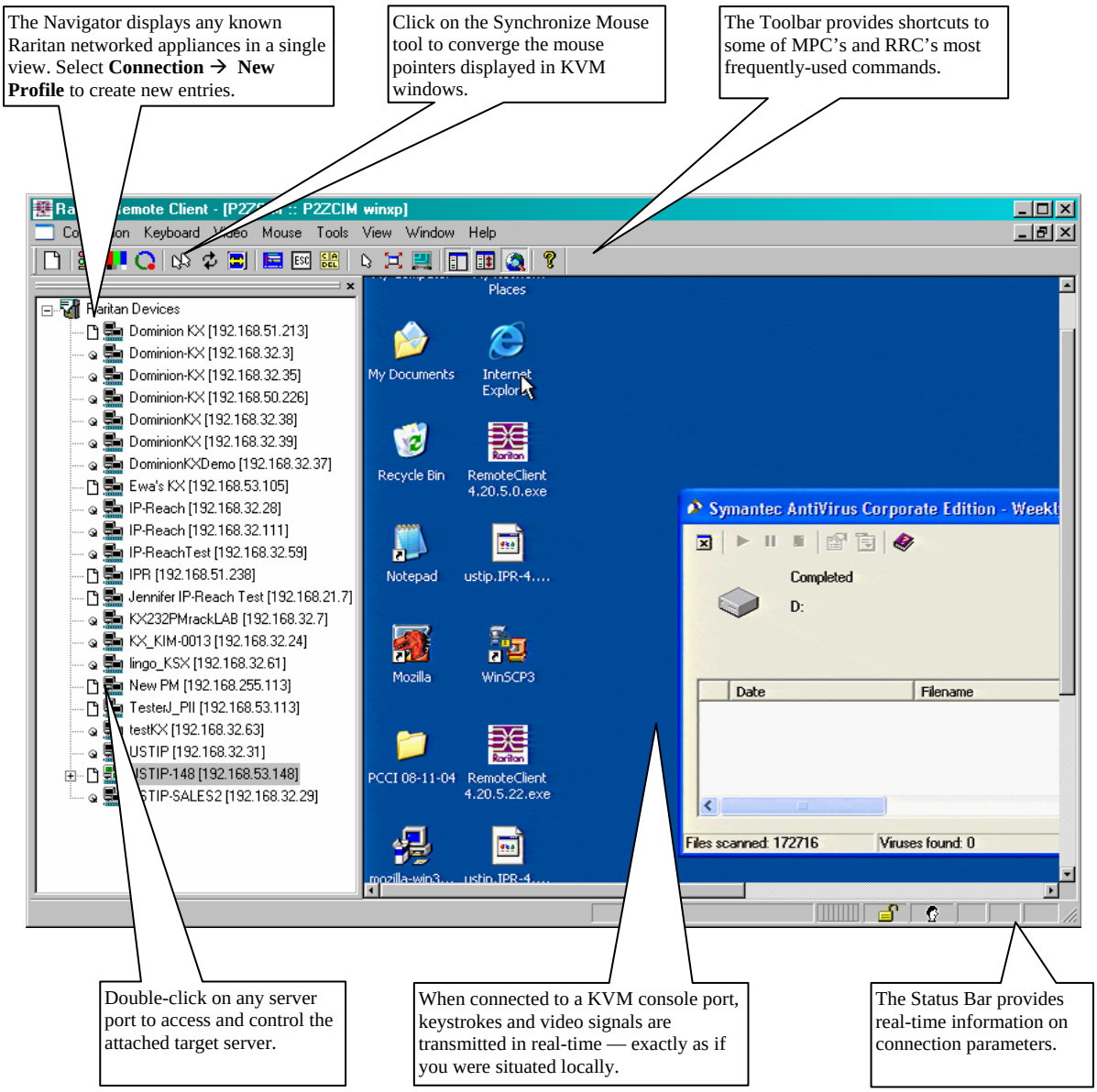


Figure 9 RRC Window

Mouse Pointer Synchronization

When controlling a target server, MPC and RRC display two mouse cursors: one belonging to your client workstation and the other belonging to the target server. When properly configured, the two mouse cursors will align. Should you experience difficulty with mouse synchronization, please refer to the section **Configuring Target Servers**, at the beginning of this chapter.

For additional information on using MPC and RRC, please refer to the **Raritan Multi-Platform Client and Raritan Remote Client User Guide,** available on Raritan's Website http://www.raritan.com/support/productdocumentation (under Dominion KX), or on the Raritan **User Manuals & Quick Setup Guides** CD included with your Dominion KX shipment.

Note to CommandCenter Users

If you are using USTIP in a CommandCenter configuration, perform the installation steps as outlined above. After completing the steps in this chapter, please consult the CommandCenter Secure Gateway User Guide on Raritan's Product Documentation Web page (http://www.raritan.com/support/productdocumentation) to proceed with your installation. The rest of this user guide applies primarily to users deploying USTIP without the integration functionality of CommandCenter.

Chapter 3: Operation – Administrative Functions

Accessing the Administrative Functions

Access and execute Administrative functions via local admin console, or via remote administration. Only administrators (users with administrative privileges) can access the USTIP Administrative Menus. Please note that users are not actually configured on the USTIP; the USTIP uses the Paragon user database and Paragon Administrator privileges.

Local Admin Console

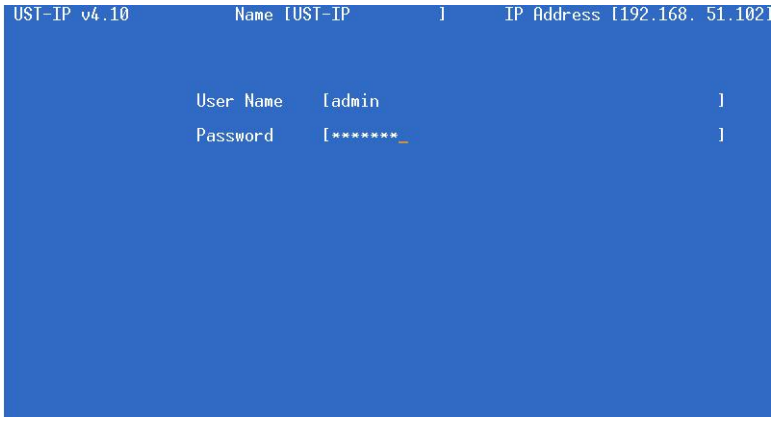


Figure 10 USTIP Admin Console

Power ON the USTIP unit via the power switch on the back of the unit.

Note: *The default USTIP login user name is* ***admin,*** *with the password* ***raritan****. This user has administrative privileges. Passwords are case sensitive and must be entered in the exact case combination in which they were created. The default password* ***raritan*** *must be entered entirely in lowercase letters. The password cannot be changed from USTIP. When connected to a UMT, it will adopt the UMT's administrator password.*

Important: The USTIP Administration menus shown here administer only USTIP settings, not Paragon settings.

Remote Admin Console

Another way to access USTIP administrative functions is to do so remotely, using MPC or RRC.

Any administrative user logged on to USTIP at a Remote PC can perform administrative functions remotely to make changes to the system, as long as USTIP is set to allow remote administration privileges.

Note: *Only users with administrator privileges can access the Remote Admin feature.*

To access the Administrative menus from RRC, double click on the Admin path entry displayed on the Navigator for the USTIP unit you wish to configure.

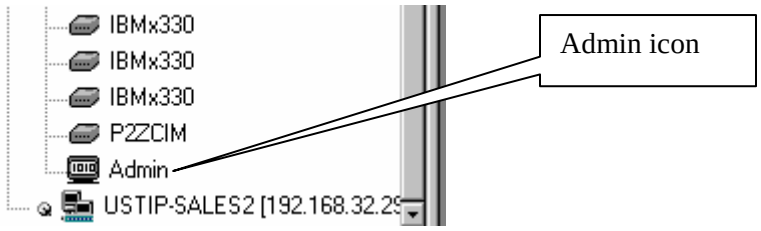


Figure 11 Admin Icon in Navigator

Navigating the Administrative Menus

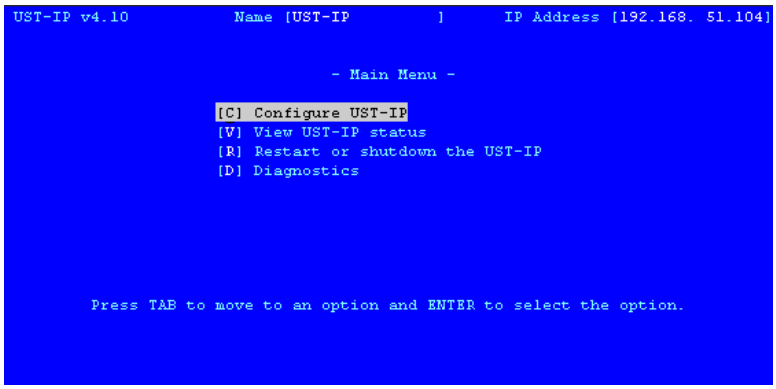


Figure 12 USTIP Main Menu

- To activate a menu: either press the **TAB** or ↑ and ↓ keys on your keyboard to highlight the menu selection you want to view (*or* press the letter in brackets before your choice) and then press **ENTER.**
- After editing any sub-menus, press **CTRL+S** to save changes. **You must press CTRL+S before exiting any screen you have changed.**
- To return to a previous menu, press **ESC.**
- View the text along the bottom of each screen for additional options.
- After changing the Network Configuration, you must reboot.

Network Configuration

Use the **TAB, ↑,** or **↓** key to highlight **[C] Configure UST-IP** on the Main Menu (or press **C**) and press **ENTER.** At the Configuration Menu, select **[N] Network Configuration** and press **ENTER.** Please note that after you have made changes to the Network Configuration, you must press **CTRL+S** to save your changes. Reboot after all changes are saved to apply them to your Network.

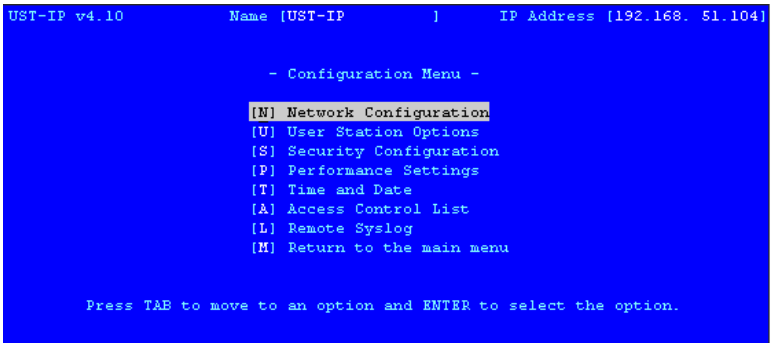


Figure 13 Configuration Menu

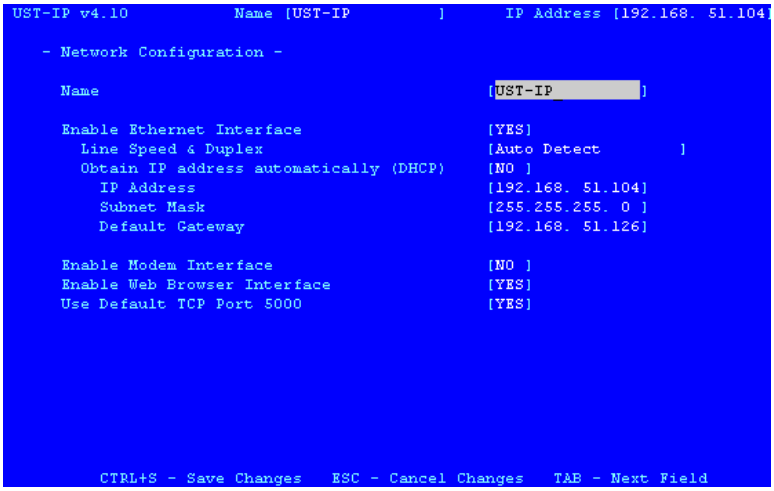


Figure 14 Network Configuration Screen

- **Name:** Designate a unique name for this USTIP unit, for example, "Miami Data Center." The default name is USTIP.
- **Enable Ethernet Interface:** Designates whether USTIP should enable its Ethernet adapter as active (default: YES).

Note: *Network connections must be 10BASE-T or 100BASE-TX Ethernet*

- **Line Speed & Duplex:** Auto detect 10 Mbps/Full Duplex, 10 Mbps/Half Duplex, 100 Mbps/Full Duplex, or 100 Mbps/Half Duplex
- **Obtain IP address automatically (DHCP):**
  - **YES**: Enables dynamic IP addressing for USTIP. Each time USTIP boots, it will request an IP address from the local DHCP server. Note that this setting can make remote access to USTIP from outside the LAN difficult, since the dynamically assigned IP address must be known in order to initiate a connection.
  - **NO (default)**: Assigns a fixed IP address to the USTIP unit (recommended).
    - **IP Address**: Enter the IP address for USTIP given by your Network Administrator.

  - **Subnet Mask**: Enter a Subnet Mask provided by your Network Administrator.
  - **Default Gateway**: Enter the Default Gateway if your Network Administrator specifies one.

- **Enable Modem Interface:** Enables Dial-up Modem access (default: YES). For USTIP, an external serial modem must be connected in order for this function to work properly.
- **Enable Web Browser Interface**: Enables web browser access to USTIP (default: YES).
- **Use Default TCP Port 5000**:
  - **YES** (default): Utilizes the default port 5000.
  - **NO**: Enter an alternate port number.

Note: *In order to access USTIP from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000, or the non-default port configured above.*

User Station Options

Select **[U] User Station Options** on the Configuration Menu to configure the User Station. In the User Station Configuration screen, use the ← and → arrows on your keyboard to set **Port Priority** to favor **None, Remote**, or **Local** users.

On the P2-USTIP1 model,

- If you set Port Priority to **Remote,** a Remote user will be prompted to terminate the Local user session when attempting to connect to the same USTIP unit.
- If you set Port Priority to **Local,** a Local user automatically terminates a Remote user session when attempting to connect to the same USTIP unit.
- If you set Port Priority to **None,** there is no capability to automatically terminate a user session. Instead, the first user to connect to a port, regardless of Remote or Local status, maintains access to that port until that user terminates the session. Other users attempting to connect will be notified that the port is busy.

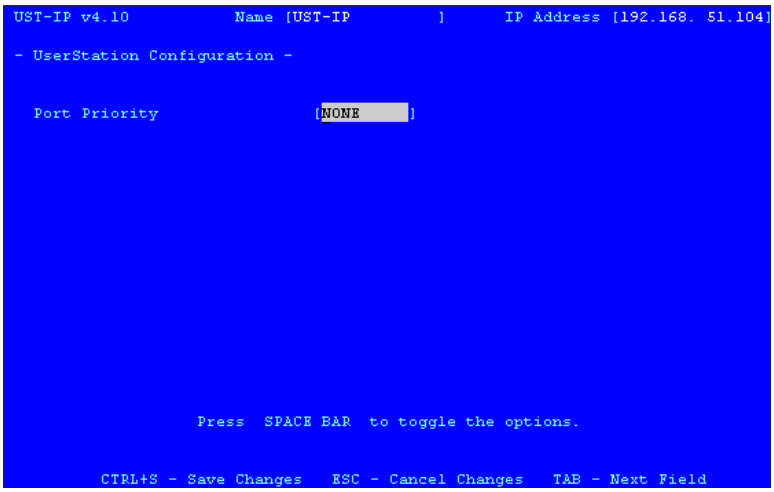


Figure 15 USTIP UserStation Configuration Screen

On the P2-USTIP2 model, two ports are available for connection. The second port will always be used before the first port, leaving the first free until another user attempts to connect.

- If you set Port Priority to **Remote,** the first Remote user connects to port 2, and if a second Remote user attempts to connect and there is a Local user on port 1, the second Remote user is prompted to terminate the Local user's session.
- If you set Port Priority to **Local,** a Local user automatically terminates a Remote user session (if Remote users are on both ports, the second port connection is terminated).

- If you set Port Priority to **None,** there is no capability to automatically terminate a user session. Instead, the first user to connect to either port maintains access to that port until the user is finished. Other users attempting to connect will be notified that the port is busy.

Note: *When two users connect to the same P2-USTIP2 device, two heads will appear on the status bar of the client, such as Raritan Remote Client (RRC) or Multi-Platform Client (MPC).*

Security Configuration

Select **[S] Security Configuration** on the Configuration Menu to set the USTIP security parameters.

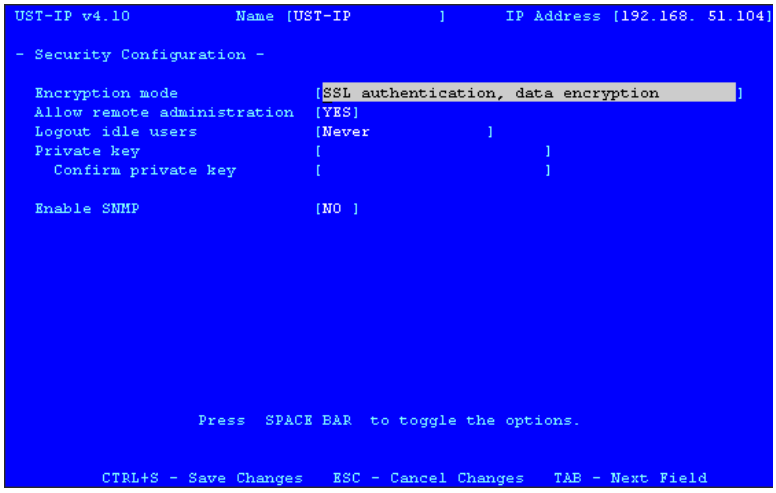


Figure 16 USTIP Security Configuration Screen

- **Encryption mode:** Toggle through the choices and select the desired level of encryption for initial connection authentication and remote session video data transfer.
  - **No encryption**: No encryption or security. Neither the initial connection authentication nor remote video data transfer is encrypted.
  - **SSL authentication, NO data encryption:** This mode secures user names and passwords, but not KVM data. 128-bit Secure Socket Layer (SSL) protocol provides a private communications channel between USTIP and the Remote PC during initial connection authentication. No encryption security in place during remote KVM data transfer.
  - **SSL authentication, data encryption (default):** This mode secures user names, passwords, and KVM data. 128-bit Secure Sockets Layer (SSL) protocol provides a private communications channel between USTIP and the Remote PC during initial connection authentication. After authentication, KVM data is also transferred with 128-bit encryption, but using a proprietary protocol more efficient than SSL.
  - **SSL authentication, SSL data encryption:** This mode secures user names and passwords, and provides high-level security for KVM data. 128-bit Secure Sockets Layer (SSL) protocol provides a private communications channel between USTIP and the Remote PC during initial connection authentication. 128-bit SSL encryption is also in place during remote KVM data transfer.

Note: *SSL data encryption increases the amount of data that must be sent over the remote connection, and is, therefore, not recommended for modem or very slow Internet connections. The default setting "SSL authentication, data encryption" offers exactly the same level of security with a higher level of efficiency.*

- **Allow remote administration:**
  - **NO:** To keep access to all Administrative Functions available only from the USTIP Admin Console, and not from a Remote PC.
  - **YES (default):** Allows remote access to all Administrative USTIP Functions by administrators logged on at a Remote PC.
- **Logout idle users:** This option is not available for configuration. Whether the idle remote users will be disconnected will be based on the setting defined in the Paragon system.
- **Private key**: Enter a private key password. This private key acts as a second level of password protection. Only remote users who know the private key password, in addition to their user name and password, can log in and connect to USTIP.
  - **Confirm private key:** Enter private key password again for re-confirmation.

To configure private key

You must perform the following steps to create a private key password.

1. Press the **Tab** key to advance to the **Private key** field and type a private key number; the private key can be up to 23 alphanumeric characters. Do not use special characters, such as # or $ (if special characters are included, the private key will fail).
2. Press **Tab** once and retype the private key in the **Confirm private key** field.
3. Press **CTRL+S** on your keyboard to save the private key. A confirmation message appears.
4. Restart the USTIP device to save the private key on your server. Please note that rebooting the USTIP should take approximately 60 seconds, but may take longer, depending on your Paragon configuration.

In order for the private key functionality to work correctly after you have rebooted the USTIP device, you must modify the USTIP profile in the Raritan Remote Client (RRC). Please perform the following steps:

1. After you have reconnected to the RRC, scroll down in the Navigator window and right-click on the USTIP icon.
2. Click **Modify Profile** in the shortcut menu.
3. Click on the **Security** tab.
4. Type the Private Key you just entered in the **Private Key** field of the USTIP Security Configuration menu.
5. Retype the Private Key in the **Confirm Private Key** field.
6. Click **OK** to save the Private Key to the USTIP profile.
   You may now log onto your USTIP device remotely through the RRC.

Note 1: *Private key passwords are case sensitive. For remote user login, they must be entered by the user in the exact case combination in which they were created here.*
Note 2: *Private key passwords must be alphanumeric. Special characters cannot be used.*

- **Enable SNMP:** Toggles whether USTIP responds to SNMP GET REQUESTS

Performance Settings

Select **[P] Performance Settings** on the Configuration Menu to set up USTIP's video data transfer and bandwidth parameters.

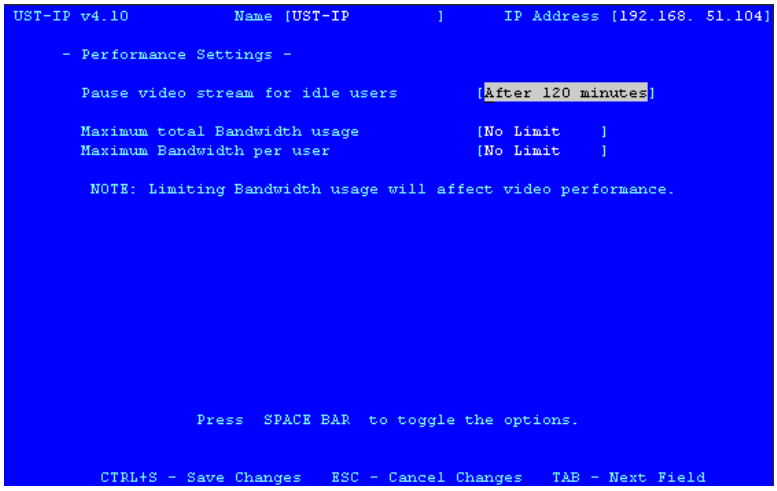


Figure 17 USTIP Performance Settings Screen

- **Pause video stream for idle users**: Pausing the flow of video data during periods of prolonged inactivity will prevent an inactive user from needlessly consuming bandwidth.
  - **Never (default):** Video data will continually be sent to Remote PC, constantly updating the screen, even if the remote user is Idle, sending no active input to USTIP.
  - **After 5, 15, 30, 60, or 120 minutes:** Video data flow to the Remote PC will pause after the selected time period has passed with no active input from the Remote PC.
- **Maximum total Bandwidth usage**: Sets an upper limit to the amount of bandwidth that can be consumed by this one USTIP unit.
  - **No Limit (default):** USTIP can consume as much bandwidth as needed.
  - **10, 5, 2, or 1 megabit or 512, 256, 128 kilobit**: Total bandwidth available to be consumed by this USTIP **unit** is limited to the selected quantity. The lower the bandwidth allowed, the slower the performance that may result.
- **Maximum Bandwidth per user**: Sets an upper limit to the amount of bandwidth that can be consumed by each user logged onto this one USTIP unit.

Note: *Control of USTIP and a connected Target Server is based on first active keyboard/mouse input, so multiple users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control.*

  - **No Limit (default):** Each **active** user can consume as much bandwidth as needed.
  - **10, 5, 2, or 1 megabit or 512, 256, 128 kilobit:** Bandwidth consumed by each active user during the **operation** of this USTIP unit is limited to the selected quantity. The lower the bandwidth allowed, the slower the performance that may result.

Press **CTRL+S** to save changes or **Esc** to cancel changes, and return to Configuration Menu. Saved Performance Settings changes will not take effect until USTIP is restarted.

Time and Date

Select **[T] Time and Date** on the Configuration Menu to view and adjust current date and time on the USTIP unit. Once saved, Time and Date changes will not take effect until USTIP is restarted.

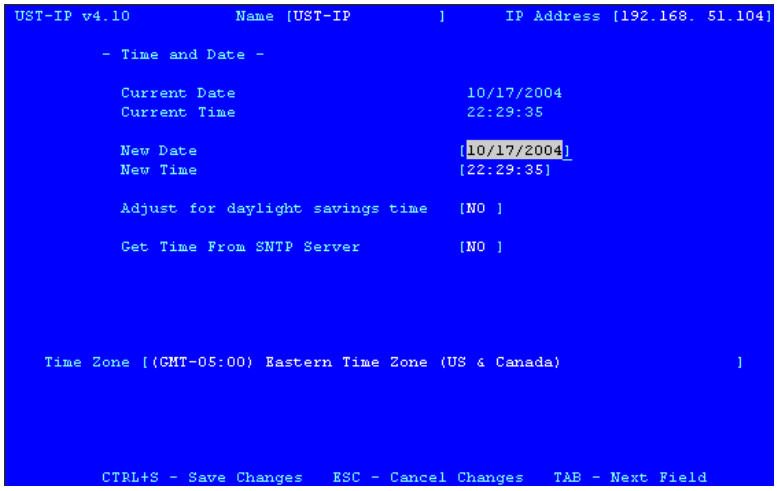


Figure 18 Time and Date Screen

- **New Date / New Time:** To manually input changes to current date and time values.
- **Adjust for daylight savings time:** Toggle between YES and NO to reflect whether your country or state follows the daylight savings time procedure.
- **Get Time From SNTP Server:** Indicates whether USTIP time/date should be automatically synchronized with the time/date of an external SNTP server.
  - **Primary Server IP Address:** IP address of first SNTP server to attempt time synchronization.
  - **Secondary Server IP Address:** IP address of second SNTP server to query, if primary server is unavailable.
  - **User standard UDP port 123:** Allows user to modify UDP port used for SNTP time synchronization. Consult your SNTP server administrator to determine if this value should be adjusted.
- **Time Zone:** Select the time zone in which your USTIP unit is physically located.

Press **CTRL+S** to save changes or **Esc** to cancel changes, and return to the Configuration Menu. Saved Radius Configuration changes will not take effect until USTIP is restarted.

Access Control List

Select **[A] Access Control List** on the Configuration Menu to set accessibility in the Access Control List (ACL) and allow or deny specific IP Addresses or ranges of IP Addresses to connect to the USTIP unit.

If entering a range of IP Addresses, type the starting and the ending IP Address values in the **Start** and **End** columns; use the **TAB** key to navigate through the fields. Use the ← and → keys to select **Allow** or **Deny** for each line item. Press **CTRL+S** when finished.

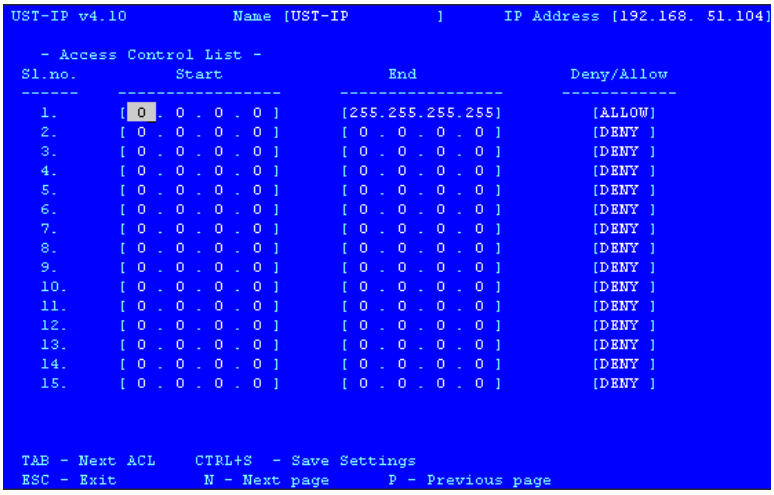


Figure 19 Access Control List Screen

Remote Syslog

Select **[L] Remote Syslog** on the Configuration Menu to allow remote users to save the server logs. Use the ← and → keys to select **Yes** or **No.**

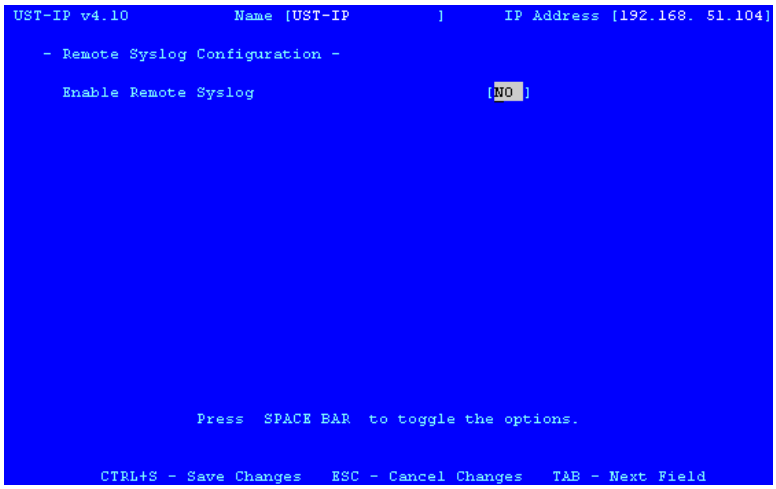


Figure 20 Remote Syslog Configuration Screen

If you select **Yes**, type the IP Address to which you want to save the Syslog in the **Remote Syslog Server IP** field, specify the information to save in **Syslog Priority Threshold** (for example, Notices, Debugs, Emergency messages, etc.), and select the category of data in the **Syslog Category** field. Press the **TAB** key to advance through these fields, and use the ← and → keys to make selections. When finished, press **CTRL+S** to save changes and return to the Remote Syslog screen.

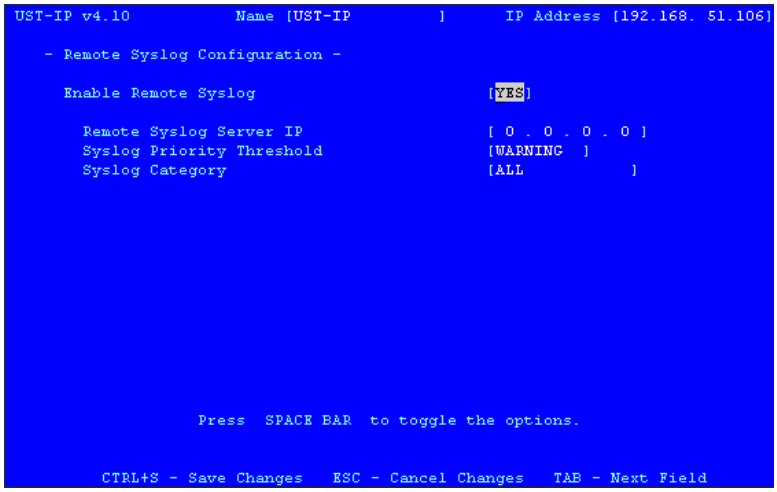


Figure 21 Remote Syslog Configuration Options

View USTIP Status

The USTIP Event Log screen shows a log file containing information about USTIP log-in and connection activities. This Event Log stores USTIP events, such as user login or logout, bad login attempts, Admin login, and logout at the USTIP Admin console, Admin changes to the system configuration, Admin user profile additions, changes, or deletions, modem activity, system startup and shutdown, and all errors that occur, with the date and time of each event. Please see **Appendix C: Troubleshooting** for a listing of error codes with their meaning and suggested solution. Up to 2,048 events can be stored in one log file.

USTIP also auto-recovers from fatal errors. If a fatal error occurs, it is recorded and USTIP automatically reboots. If a non-fatal error occurs, it is recorded and USTIP waits until all users are logged off the system, and then it reboots to make sure the previous non-fatal error does not escalate to a fatal error.

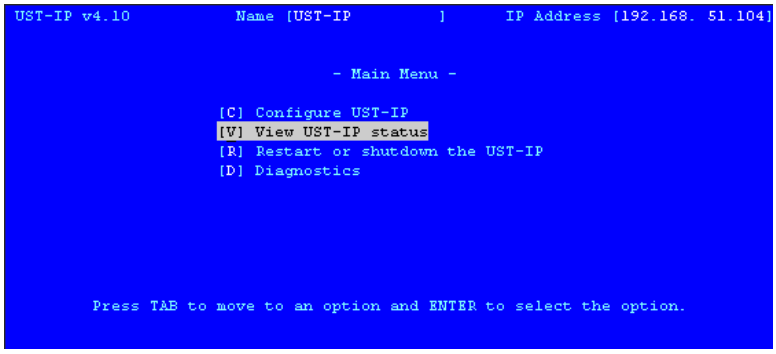


Figure 22 USTIP Main Menu

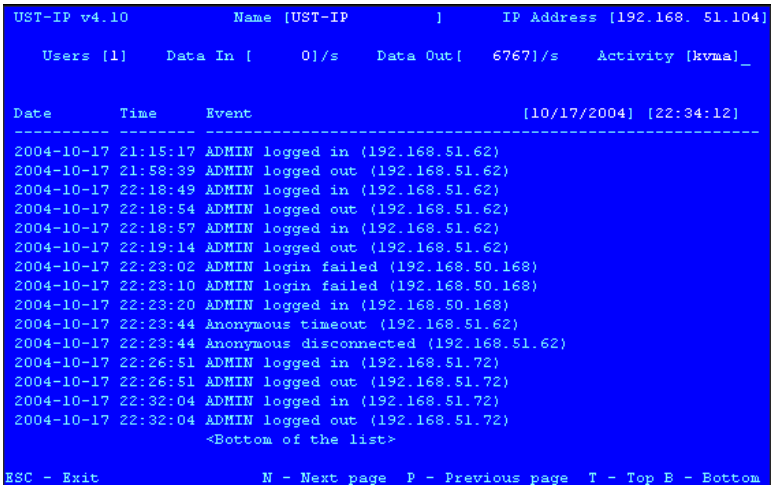


Figure 23 Status Log Screen

Restart or Shutdown the USTIP

You can restart or shut the USTIP unit down from the Main Menu. **Restart R**, **Shutdown S**, or **Cancel Esc** the restart or shutdown command. **R** Restarts the USTIP unit and brings the USTIP Admin Console back to the USTIP Initialization screen.

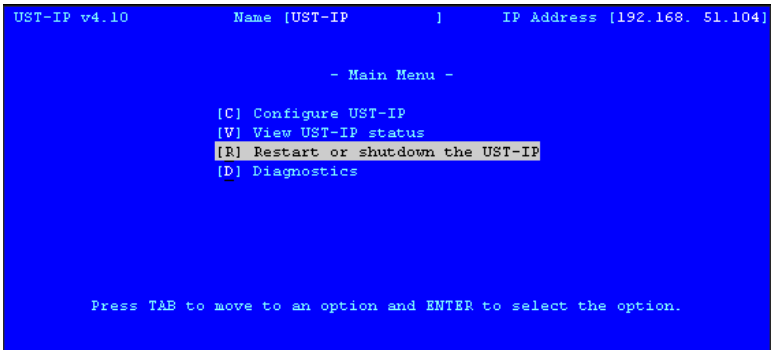


Figure 24 USTIP Main Menu

Diagnostics

To view the USTIP Diagnostic Console, press **D** at the Main Menu.

Please do not activate the Diagnostics screen unless you are fully trained and know the meanings and intended use of these commands; these functions are available in order to assist Raritan Technical Support in the event of problems. Please contact Raritan Technical Support if you require more information.

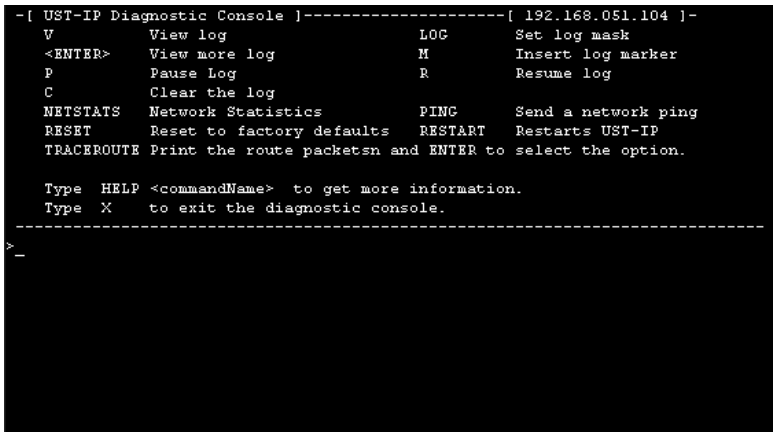


Figure 25 Diagnostic Console

Appendix A: Specifications

ITEM	DIMENSIONS (WXDXH)	WEIGHT	POWER
P2-USTIP1	1U 19” Rackmount Case: 17.2” (W) x 11.46” (D) x 1.72” (H) 440mm (W) x 291mm (D) x 44 mm (H)	8.05 lbs. (3.65 kg)	115V/230V 50/60 Hz 0.3A
P2-USTIP2	1U 19” Rackmount Case: 17.2” (W) x 11.46” (D) x 1.72” (H) 440mm (W) x 291mm (D) x 44 mm (H)	8.16 lbs. (3.7 kg)	115V/230V 50/60 Hz 0.6A

Remote Connection

Network: 10BASE-T, 100BASE-TX Ethernet
Modem: Dedicated Modem Port
Protocols: TCP/IP, UDP, NTP, Syslog, DHCP, HTTP, HTTPS, SSL

Raritan Remote Client (RRC) Software

Operating System Requirements: Windows XP / NT / ME / 2000

KVM Input

Supported Resolutions:

Text Modes	
640x480 @ 60Hz	1024x768 @ 60Hz
640x480 @ 72Hz	1024x768 @ 70Hz
640x480 @ 75Hz	1024x768 @ 75Hz
640x480 @ 85Hz	1024x768 @ 85Hz
720x400 @ 70Hz	1152x864 @ 60Hz
720x400 @ 85Hz	1152x864 @ 70Hz
800x600 @ 56Hz	1152x864 @ 75Hz
800x600 @ 60Hz	1280x960 @ 60Hz
800x600 @ 72Hz	1280x1024 @ 60Hz
800x600 @ 75Hz	
800x600 @ 85Hz	

Cable Specifications

Category 5e UTP cable to connect to network.

Paragon download cable to connect from Admin Port to local PC port.

KVM Switch Specifications

Supports KVM switches utilizing an On-Screen User Interface, including Raritan's Paragon, Z-Series, MasterConsole MX^4, and MasterConsole II product lines.

Output Specifications

Local Access Console: PS/2 Keyboard, PS/2 Mouse, HD15 Video

Local Admin Port: DB9F

Appendix B: Frequently Asked Questions

QUESTION:	ANSWER:
What is USTIP?	USTIP is the easiest, fastest, most reliable way to remotely access and manage multiple servers connected to a Paragon II - no matter where you are or where your servers are located.
How does USTIP work?	USTIP connects to the Cat5 Paragon switch. Using Raritan's powerful frame-grabber and compression technology, it captures, digitizes, and compresses the video signal before transmitting to a remote PC.
What level of control does a USTIP remote user have over attached Target Servers?	The remote user has direct access and total control of target servers for maintenance, administration, and troubleshooting, from running GUI applications to BIOS-level troubleshooting, and even rebooting.
Remote Access Software has been available for a long time. What makes USTIP different?	With USTIP, the USTIP software runs only on the USTIP unit itself, not on each individual Target Server. Traditional Remote Access Software solutions require software to be loaded and running on each Target Server, which must offer a supporting Operating System. This can create compatibility, performance, and reliability issues on mission critical Target Servers.
What remote access connection methods can USTIP accommodate?	USTIP provides network administrators with a choice of remote access via Internet, LAN/WAN, or dial-up modem. That means servers can be accessed both in and out of band, so remote access to mission-critical target servers is always available - even if the network is down.
What types of computers can USTIP remotely control?	USTIP connects directly to Paragon, and therefore supports SUN, Mac, Serial, etc.
Is special software required for the Remote PC?	Use USTIP with Raritan Multi-Platform Client or Raritan Remote Client; please speak with your Raritan reseller for additional information.
Which Raritan KVM Switches will work with USTIP?	Currently, USTIP is supported with the Paragon II line of switches.
Can I continue to access my KVM configuration locally?	Yes. USTIP features a special Direct Analog User port for direct access to the KVM configuration. This pass through port provides an additional local access point, which is especially important for single user switches or for providing critical access to servers if the network is down.
Does USTIP support LDAP/RADIUS?	No; it must be part of a Paragon configuration, and requires the Paragon username and password.

QUESTION:	ANSWER:
Is USTIP easy to install?	USTIP is very easy to install. Just connect it to a user port on an existing KVM configuration and assign an IP address and/or telephone number for modem access.
How Is USTIP administration carried out?	Administrators access USTIP through a connected USTIP Admin Console. A simple keyboard driven interface of menus offers straightforward access to USTIP setup and control. User profiles, security settings, configuration and diagnostics are just a few of the options available. The USTIP Admin Console can be removed from the server room once initial USTIP setup is complete, after which all configuration may be performed remotely via web browser.
Are there security features to protect my Target Servers from an unauthorized remote connection?	Yes. USTIP provides many layers of security. USTIP can be configured to provide high-level connection authentication and video data transfer security during a remote session. User names, passwords, private-keys, and Secure Socket Layer (SSL) 128-bit encryption are all available. USTIP can also function as a RADIUS client. In addition, all Raritan KVM Switches that feature an On-Screen User Interface (OSUI) come with a complete security scheme, requiring user name and password access to Servers as designated by the network administrator.
Is there a double login using USTIP?	No, only single login. A double login exists if you use IP-Reach with Paragon.
Is there Web-Based Access?	Remote access can be obtained via a web browser to the USTIP1's IP address. ▪ Connection from any Windows-based PC - Windows 2000, or XP ▪ Microsoft Internet Explorer, Mozilla, and Netscape
How does USTIP handle a local and remote user when trying to access USTIP?	USTIP1 – the local and remote user share 1 path USTIP2 – the 1st path is shared with local and remote users, the 2nd path is dedicated for remote users USTIP1 operates under three working modes where the user is able to assign priority to either the local, remote user or provide a "first come first serve basis" via the admin console for the Local port or the Remote port.
Can I customize USTIP to enhance performance relative to my specific KVM configuration?	Yes. A variety of fine-tuning procedures are available. Automatic Color calibration, KVM On-Screen Display tuning, and Target Mouse Pointer adjustments all serve to enhance USTIP performance.
Can I customize USTIP to enhance performance with regard to different remote access methods and situations?	Yes. USTIP offers a variety of performance enhancements to optimize a chosen connection method. Color Depth, Progressive Update, and Internet Flow Control are just a few of the adjustment options available to speed response time. Color Depth, for example, can be adjusted all the way down to black and white to decrease the data load during an emergency midnight modem connection to mission-critical servers over low-bandwidth.

QUESTION:	ANSWER:
Can I use USTIP in a VPN?	Yes. USTIP fits most network configurations utilizing standard TCP/IP. The network administrator simply adds USTIP as a node on the network via the USTIP Admin Console.
What is the slowest connection USTIP can handle?	USTIP offers scalable performance based on bandwidth available, down to 20kbps.
Can I perform a Dial-up modem connection to USTIP over a PBX line?	No. Modems require an analog telephone line.
Can I use USTIP within my local network?	USTIP can be used in any computer network that supports its Ethernet connection.
When does USTIP use TCP? UDP?	Both TCP and UDP are used by USTIP. However, TCP is essential, whereas UDP is optional. UDP is used only for one USTIP feature, automatic detection ("browse") of USTIP units in a subnet. If you do not employ the browse feature (and by extension, are not using DHCP), then USTIP will only communicate using TCP.

This page intentionally left blank.

Appendix C: Troubleshooting

Problems and Suggested Solutions

REMOTE CONNECTION PROBLEM	SOLUTION
I cannot connect to USTIP via dial up modem.	Ensure that you have specified the modem device for your Remote PC in the Add Connection Window (Dial-up type connection) modem field. Although concurrent connections may be enabled (either globally or individually), the modem in USTIP will only accommodate one remote connection at a time – ensure that someone else is not already connected via modem. Ensure that your user profile has modem access enabled and that USTIP is configured to enable a modem interface on the Network Configuration Screen. Ensure that the communication port chosen by the network administrator on the **Network Configuration** screen matches the port set in your connection profile.
I cannot connect to USTIP via LAN/WAN or Internet.	Re-check the IP settings for USTIP from the USTIP Admin Console or remote **Admin Console** window. Accessing the **Network Configuration** screen, ensure that the IP addresses set for "IP Address, Subnet Mask, and Default Gateway" are still set correctly, per your Network Administrator's instructions. Ensure that your user profile has network access enabled and that USTIP is configured to enable a network interface. Ensure that the communication port chosen by the network administrator on the **Network Configuration** screen matches the port set in your connection profile. Ensure that the network configuration is correct by sending a PING from the Remote PC to USTIP. Ensure that your private key is set correctly.
I cannot connect to USTIP via Web Browser.	Re-check the IP settings for USTIP from the USTIP Admin Console or remote **Admin Console** window. Accessing the **Network Configuration** screen, ensure that the IP addresses set for "IP Address, Subnet Mask, and Default Gateway" are still set correctly, per your Network Administrator's instructions. Ensure that your user profile has Web Browser access enabled and that USTIP is configured to enable Web Browser.
I cannot connect to USTIP and seem to be stuck at the **Login** window.	Ensure that you are using a valid and correct user name and password. Ensure that you are typing user name and password in the exact upper and lowercase combinations in which they were created. Drag the **Login** window to the side and view **Connection Status** window behind it. The **Connection Status** window will show details on your connection attempts, and may offer specifics on the problem.

DIRECT ANALOG USER CONSOLE PROBLEM	SOLUTION
The Direct Analog User Console does not function.	Make sure the KVM switch is functioning properly. Make sure that USTIP is turned on. USTIP must be powered on for the Direct Analog User Console to function. The cable located inside USTIP that connect the Direct Analog User Console port(s) may have disconnected – Contact Raritan Technical Support for assistance.
I cannot seem to gain steady keyboard/mouse control of the active Target Server from a Direct Analog User Console.	Keyboard/mouse control of a Target Server from a Direct Analog User Console is shared on a first active keyboard/mouse input basis with any remote users who may be currently connected. Ensure that no remote users are currently attempting to control the active Target Server.
I cannot view the Target Server that I am looking for from a Direct Analog User Console.	Ensure that you are looking at the Direct Analog User Console connected to the correct User Port. Remember, Direct Analog User Consoles can be attached to User Ports 1 through 4. Each User Console will view the path of the matching KVM Port. For example, the User Console attached to User Port 1 will view the KVM path attached to KVM Port 1. Similarly, the User Console attached to User Port 2 will view the KVM path attached to KVM Port 2, and so on.

KEYBOARD PROBLEM	SOLUTION
USTIP is not accepting keyboard commands from the Remote PC.	The **USTIP** window of TRC must be the active window for proper keyboard control. Ensure the window in which you are typing is active. Try clearing the keyboard signals to ensure that the release or breakcode signal has been received – alternately press the **CTRL**, **Shift** and **Tab** keys rapidly a few times on your keyboard. Ensure the remote user has keyboard and mouse privileges. Exit the USTIP software and then restart it again.
I pressed the Caps Lock key on my Remote PC. The CAPS indicator on the USTIP **Status Bar** appeared, but the Caps Lock indicator light is not lit on my Remote PC keyboard.	This is normal. Use the indicators on the **Status Bar** to determine CAPS key status for the Target Server. If a local user at the Direct Analog User Console's keyboard has changed a Lock key status (Caps-Lock, Num-Lock, or Scroll-Lock) on the Target Server, then server status may not match the state of the Remote PC's keyboard.
The Keyboard is not functioning and the green LED on the back of USTIP for at least one of the KVM ports is not blinking, but rather constantly lit.	Reset the keyboard chips within USTIP by recycling power to it. Make sure you power down both USTIP and all attached KVM switches at the same time. Otherwise the KVM chips in USTIP will draw power from the KVM switches and fail to reset.
I am accessing USTIP via the Web Browser and the keyboard does not function. I type, but nothing happens.	Click the window title bar under the USTIP toolbar to activate the viewing window. If the viewing window is not the active window, the keyboard will not function.

KVM ON-SCREEN USER INTERFACE (OSUI) PROBLEM	SOLUTION
Log out of KVM on disconnect is set to YES in the **Security Configuration** screen, but USTIP is not logging out of the KVM upon remote user disconnection.	Make sure that the Hotkey set in the **Options** window is the same Hotkey that commands the OSUI of the base KVM switch attached to USTIP.

MOUSE PROBLEM	SOLUTION
Target Server Mouse Pointer tracks too slowly after **USTIP Mouse Pointer**. Immediately after switching to a new Target Server channel the mouse stops and/or is out of sync.	When working from a Remote PC, a slight delay between the larger **USTIP Mouse Pointer** and the smaller **Target Server Mouse Pointer** is normal due to uncontrollable lags in the speed of the remote connection – Internet, direct dial modem, or network. With each new video image viewed, USTIP automatically re-syncs and aligns the mouse pointers. Wait a few seconds after switching to each new video image for automatic re-calibration to take place and the two mouse pointers will line up with each other. If you do not wish to wait for this auto calibration, or you find the two mouse pointers out of sync at any time; click **Synchronize Mouse**, or simultaneously press the keys **CTRL-ALT-S**. This will manually re-align the two pointers. Adjust the motion of the **Target Server Mouse Pointer**. For Windows 2000 based Target Servers, set the mouse motion speed on each Target Server to the middle speed setting between Slow and Fast and the mouse motion acceleration speed on each Target Server to Off or None. For Windows ’95, ’98, and NT based Target Servers, set the mouse motion speed on each Target Server to the slowest setting. Color Settings are not optimally calibrated. Please see the **Raritan Multi-Platform Client and Remote Client User Guide,** available on Raritan’s Website http://www.raritan.com/support/productdocumentation, or on the Raritan User Manuals & Quick Setup Guides CD ROM for additional information.
The larger **USTIP Mouse Pointer** does not track or is not in sync (not aligned) with the smaller **Target Server Mouse Pointer.**	Click **Synchronize Mouse**, or press **CTRL-ALT-S**. Ensure each Target Server uses a standard Windows mouse driver. For Windows 2000 based Target Servers, set the mouse motion speed on each Target Server to the middle speed setting between Slow and Fast and the mouse motion acceleration speed on each Target Server to None. For Windows ’95, ’98, and NT based Target Servers, set mouse motion speed on each Target Server to slowest setting possible. Click **Auto-sense Video** or simultaneously press **CTRL-ALT-A**.

MOUSE PROBLEM	SOLUTION
USTIP is not accepting my mouse.	USTIP will not support a serial type mouse or non-standard mouse drivers. It does support a PS/2 style mouse and standard Windows mouse drivers. Other mouse drivers may function with USTIP, but will require extensive changes to the mouse settings until a functioning mix of motion settings is found. If you must use a mouse driver on a Target Server that is not currently supported by USTIP, try setting the mouse acceleration to none and the mouse speed to slow.
USTIP Mouse Pointer and the **Target Server Mouse Pointer** do not sync up in certain Windows NT Administration screens, like the NT log on screen.	Windows NT Administration or Log On screens may revert to default mouse pointer motion/acceleration speeds. As a result, mouse sync may not be optimal at these screens. If you are comfortable adjusting the registry on the Windows NT Target Server, you can obtain better USTIP mouse sync at NT Administration screens by entering the Target Server's registry editor and changing the following settings: default user mouse motion speed = 0; mouse threshold 1 = 0; mouse threshold 2 = 0.

TARGET SERVER PROBLEM	SOLUTION
When I reboot a Target Server through USTIP, from a Remote PC, I cannot access the Target Server's BIOS. It seems USTIP is not accepting the BIOS entry command keystroke.	To access a Target Server's BIOS first temporarily de-select the **Sense video mode changes automatically** checkbox in the **Video Settings** window, accessed with **Video Settings** on the USTIP toolbar. Video auto-sensing slows remote viewing of the reboot process and makes it difficult to send BIOS access keystrokes to the Target Server from a Remote PC, because auto-sensing tells USTIP to work constantly to keep up with the Target Server's feverishly changing video screens during reboot. De-selecting the auto-sense checkbox frees USTIP to accept and convey BIOS access keystrokes. It also aides in the quick interpretation of rapidly changing video screens. Be sure to re-select the checkbox when finished with BIOS access.

USTIP PROBLEM	SOLUTION
I cannot power down USTIP.	The main power switch for USTIP is on the back of the unit. To turn off USTIP hold the power key down for a few seconds. To turn USTIP back on, press the power button again.

VIDEO PROBLEMS	SOLUTION
After switching to a different Target Server channel the video is not clear. Sometimes there is a black edge at the boundary of the Target Server's screen.	Click **Auto-sense Video** or simultaneously press the keys **CTRL-ALT-A**. USTIP will adjust the video settings. If the video does not become clear, additional manual video setting adjustments may be necessary. Contact Raritan Technical Support to discuss changes to the **Video Settings** window. Ensure all Target Servers have standard blanking times. Horizontal and vertical blanking times should closely approximate VESA standard values.
When viewing a Target Server remotely, the video image is filled with moving block of incorrect color that seem to track next to the movement of the mouse pointer.	The Color Settings on the Video Settings tab in the **Video** window are not set correctly. Attempt manual adjustment until the color blocking ceases or run the Automatic Color Calibration Routine.
The screen is filled with small visual errors, or grains of missing color, which need to be cleaned up.	Click **Refresh Screen** on the USTIP toolbar or simultaneously press the keys **CTRL-ALT-R**.
The video seems to be stuck in Auto Sense mode and the auto sensing message in the middle of the screen keeps counting higher and higher.	Pressing **Auto-sense Video** while auto sensing is occurring will stop the auto sense process. Check your Target Server resolution to ensure USTIP supports it.

WEB BROWSER PROBLEMS	SOLUTION
I cannot connect to USTIP via Web Browser.	Re-check the IP settings for USTIP from the USTIP Admin Console or remote **Admin Console** window. Accessing the **Network Configuration** screen, ensure that the IP addresses set for "IP Address, Subnet Mask, and Default Gateway" are still set correctly, per your Network Administrator's instructions. Ensure that your user profile has Web Browser access enabled and that USTIP is configured to enable Web Browser.

Event Log File and On-Screen Error Codes

USTIP will display or log an error code in the **USTIP Event Log Screen** in the event of a problem occurring. Error codes are eight-digit hexadecimal numbers, containing two parts: the first four denote error type; and the second four digits denote a location code.

These last four digits of the USTIP error code are the most useful in determining what has caused a system failure. Below is a list of location codes (the last four digits of an error code), and their meanings.

ERROR CODE (LAST 4 DIGITS)	MEANING	RECOMMENDATION
0001 – 0003	Memory allocation error	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0004	Could not read the configuration file on startup. The file may be corrupt, the file system may be damaged, or the config file might be from an older version of USTIP.	Reenter the configuration information and reboot. If the problem continues, restore the software and file system from the Recovery CD-ROM.
0005	The config file was missing. This may be the first time you have started USTIP or the file system has become corrupt.	Reenter the configuration information and reboot. If the problem continues, restore the software and file system from the Recovery CD-ROM.
0006	The config file could not be saved. The file system may be corrupt or the hard drive may not be responding.	Retry, but if the problem persists, restore the software and file system from the Recovery CD-ROM.
0007 – 0008	Memory allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0009	Could not find the frame grabber card.	Power off the system and make sure the frame grabber card is inserted firmly. If the problem persists, there may be a problem with your USTIP hardware.
000A	Frame grabber card is not responding correctly.	Power off the system and make sure the frame grabber card is inserted firmly. If the problem persists, there may be a problem with your USTIP hardware.
000B	Memory allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.

ERROR CODE (LAST 4 DIGITS)	MEANING	RECOMMENDATION
000C – 000F	Memory allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0011	The Ethernet controller could not be found.	There is a problem with the USTIP hardware.
0012	The modem could not be found.	Power off the system and make sure the frame grabber card is inserted firmly. If the problem persists, there may be a problem with your USTIP hardware.
0013	Memory allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0014	There is a problem with the IP address.	Check the IP address configuration and reboot.
0015	The DHCP server did not respond. USTIP could not acquire an IP address.	Make sure your DHCP server is operating correctly and then reboot USTIP.
0016 – 0019	There is a problem with one of the USTIP startup files.	Restore the software and file system from the Recovery CD-ROM.
001A	Error occurred while initializing the UDP socket.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001B	Error occurred while initializing the TCP write socket.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001C	Error occurred while initializing the TCP read socket.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001D – 001E	Resource allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001F	Could not listen to the TCP write socket.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0020	Could not listen to the TCP read socket.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.

ERROR CODE (LAST 4 DIGITS)	MEANING	RECOMMENDATION
0021	TCP listen process failed.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0022	UDP listen process failed.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0023	SSL write failed.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0024	SSL read failed.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0025	Memory allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0026 – 0029	Resource allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
002A – 002F	Resource allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0030-0039	Resource allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
003A – 003F	Resource allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0040	Resource allocation error.	Reboot USTIP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.

This page intentionally left blank.

This page intentionally left blank.

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 8 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

Beijing

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5994
Email: support.japan@raritan.com

Europe

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0

Korea

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +82-2-5578730

Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com