Safety Guidelines

WARNING! Read and understand all sections in this guide before installing or operating this product.

WARNING! Connect this product to an AC power source whose voltage is within the range specified on the product's nameplate. Operating this product outside the nameplate voltage range may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to an AC power source that is current limited by a suitably rated fuse or circuit breaker in accordance with national and local electrical codes. Operating this product without proper current limiting may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to a protective earth ground. Never use a "ground lift adaptor" between the product's plug and the wall receptacle. Failure to connect to a protective earth ground may result in electric shock, fire, personal injury and death.

WARNING! This product contains no user serviceable parts. Do not open, alter or disassemble this product. All servicing must be performed by qualified personnel. Disconnect power before servicing this product. Failure to comply with this warning may result in electric shock, personal injury and death.

WARNING! Use this product in a dry location. Failure to use this product in a dry location may result in electric shock, personal injury and death.

WARNING! Do not rely on this product's receptacle lamps, receptacle relay switches or any other receptacle power on/off indicator to determine whether power is being supplied to a receptacle. Unplug a device connected to this product before performing repair, maintenance or service on the device. Failure to unplug a device before servicing it may result in electric shock, fire, personal injury and death.

WARNING! Only use this product to power information technology equipment that has a UL/IEC 60950-1 or equivalent rating. Attempting to power non-rated devices may result in electric shock, fire, personal injury and death.

WARNING! Do not use a Raritan product containing outlet relays to power large inductive loads such as motors or compressors. Attempting to power a large inductive load may result in damage to the relay.

WARNING! Do not use this product to power critical patient care equipment, fire or smoke alarm systems. Use of this product to power such equipment may result in personal injury and death.

WARNING! If this product is a model that requires assembly of its line cord or plug, all such assembly must be performed by a licensed electrician and the line cord or plugs used must be suitably rated based on the product's nameplate ratings and national and local electrical codes. Assembly by unlicensed electricians or failure to use suitably rated line cords or plugs may result in electric shock, fire, personal injury or death.

WARNING! This product contains a chemical known to the State of California to cause cancer, birth defects, or other reproductive harm.
Safety Instructions

1. Installation of this product should only be performed by a person who has knowledge and experience with electric power.

2. Make sure the line cord is disconnected from power before physically mounting or moving the location of this product.

3. This product is designed to be used within an electronic equipment rack. The metal case of this product is electrically bonded to the line cord ground wire. A threaded grounding point on the case may be used as an additional means of protectively grounding this product and the rack.

4. Examine the branch circuit receptacle that will supply electric power to this product. Make sure the receptacle's power lines, neutral and protective earth ground pins are wired correctly and are the correct voltage and phase. Make sure the branch circuit receptacle is protected by a suitably rated fuse or circuit breaker.

5. If the product is a model that contains receptacles that can be switched on/off, electric power may still be present at a receptacle even when it is switched off.
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（V C C I）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.

If a power cable is included with this product, it must be used exclusively for this product.

CAUTION:
To reduce the risk of shock — Use indoors only in a dry location. No user serviceable parts inside. Refer servicing to qualified personnel. For use with IT equipment only. Disconnect power before servicing.
Contents

Safety Guidelines ii

Safety Instructions iii

Chapter 1  Introduction 1
  Hardware Requirements ................................................................. 1
  Software Requirements ............................................................... 2
  Plug and Play .............................................................................. 2

Chapter 2  USB-Cascading Applications 3
  Appropriate Applications ............................................................. 3
  Best Practices ........................................................................... 5
  Inappropriate Applications .......................................................... 5

Chapter 3  USB-Cascading Instructions 6
  USB-Cascading Restrictions .......................................................... 6
  Cascading Raritan Devices ............................................................ 6
  Setting the Cascading Mode .......................................................... 8
    Port Number Syntax ................................................................... 9
    Port Forwarding Examples ...................................................... 11

Chapter 4  Network Access 14
  Finding the IP Address ................................................................. 14
  Local Console ............................................................................ 14
  MAC Address ............................................................................ 15
  LCD Display ............................................................................. 15
  HTTP/HTTPS Access .................................................................. 16
    Supported Web Browsers ....................................................... 17
    Using the Web Browser .......................................................... 17
Chapter 1  Introduction

Raritan provides a USB-cascading solution, which enables multiple Raritan devices to share the network connectivity after cascading them through the USB interface.

Each individual device in the USB-cascading configuration can be accessed and administered over the Internet from anywhere. Besides, each device in this configuration can be upgraded respectively.

In This Chapter
Hardware Requirements.............................................................................1
Software Requirements...............................................................................2
Plug and Play............................................................................................2

Hardware Requirements

The following Raritan products support the USB-cascading feature.

- PX2 series power distribution units (PDUs)
- PX3 series power distribution units
- EMX asset management devices
- Branch Circuit Monitor (BCM)
- PX3TS transfer switch

The USB-cascading configuration comprises either identical or diverse Raritan products. For example, you can cascade PX2 PDUs only, or you can cascade PX2, PX3, EMX, PX3TS and BCM devices in the USB-cascading configuration.
Chapter 1: Introduction

Software Requirements

A Raritan device must run an appropriate firmware to support the USB-cascading feature. Depending on the firmware version implemented, the maximum number of cascaded devices that are supported in a USB-cascading configuration differs.

► Firmware versions supporting a maximum of four Raritan devices:
  • PX2 series: 2.3.1 or later
  • PX3 series: 2.5.10 or later
  • EMX series: 2.1.0 or later
  • BCM series: 2.3.1 or later

► Firmware versions supporting a maximum of eight Raritan devices:
  • PX2 series: 2.5.20 or later
  • PX3 series: 2.5.20 or later
  • EMX series: 2.5.0 or later
  • BCM series: 2.5.20 or later
  • PX3TS series: 2.6.0 or later

Different firmware versions support a different number of cascading modes.

- Those supporting four devices support the network 'Bridging' mode only.
- Those supporting eight devices support both 'Bridging' and 'Port Forwarding' modes. See Setting the Cascading Mode (on page 8).

If the 'Port Forwarding' mode is intended, you must upgrade all devices to support two cascading modes.

Check firmware versions before cascading Raritan devices and upgrade any device as needed. See Updating the Raritan device Firmware (on page 33).

Plug and Play

The USB-cascading solution is a plug-and-play function. This means you can cascade or uncascade a Raritan device in the USB-cascading configuration at any time, and the shared network connectivity is immediately in effect or lost based on the USB connection status.
Chapter 2  USB-Cascading Applications

This chapter illustrates several USB-cascading scenarios using PDUs, and points out best practices and the condition the USB-cascading solution should be avoided.

In This Chapter

Appropriate Applications ................................................................. 3
Best Practices ..................................................................................... 5
Inappropriate Applications ................................................................. 5

Appropriate Applications

When it is necessary to reduce the number of Ethernet connections or save networking costs, apply the USB-cascading solution.

In the USB-cascading configuration, all Raritan devices are cascaded using USB cables and only the first Raritan device in the chain is connected to the LAN.

The following illustrate a few USB-cascading scenarios using Zero U PDUs. Red lines in the diagrams represent USB connections.

- **When your firmware supports up to four devices:**
  - Scenario 1: Cabinet 1 has four PDUs cascaded, all of which share one Ethernet connection.
Chapter 2: USB-Cascading Applications

- **When your firmware supports up to eight devices:**
  - Scenario 2: Cabinet 1 and Cabinet 2 have four PDUs respectively. These eight PDUs are cascaded, sharing one Ethernet connection.
  - Scenario 3: Cabinet 1 through Cabinet 4 have two PDUs respectively. These eight PDUs are cascaded, sharing one Ethernet connection.
**Best Practices**

One Ethernet connection per cabinet is better than one Ethernet connection across cabinets because of the following advantages:

- Easier to manage or maintain one cabinet when all of the cabling and connections are located in the same cabinet.
- Reduces the cross-cabinet cabling.

An eight-device cascaded configuration saves the most Ethernet connections and costs, and it is recommended when:

- Ethernet ports are expensive or limited.
- Available IPv4 addresses are limited.

**Inappropriate Applications**

Though the USB-cascading solution helps decrease the Ethernet connections and costs, there are two scenarios where this solution is NOT recommended:

- **High network reliability is required:**
  The USB-cascading solution increases the number of network bridging points for cascaded devices, which may result in network unreliability. Therefore, when high network reliability is required, establish a separate Ethernet connection for each Raritan device to minimize the number of potential network failure points.

- **High bandwidth is required:**
  The USB bandwidth between the master and the first slave device is 12Mbit/s. Due to this bandwidth limitation, the actual data transfer rate for all slave devices ranges between 8Mbit/s and 10Mbit/s. If high bandwidth is required, such as transmission of webcam videos, directly connect that Raritan device to the network to optimize the data transfer rate.
Chapter 3  USB-Cascading Instructions

This chapter describes the USB-cascading limitations, instructions and various methods to identify a cascaded Raritan device.

In this guide, the master device refers to the first device in the USB-cascaded configuration and slave devices refer to all subsequent devices connected to the master device.

In This Chapter

USB-Cascading Restrictions .....................................................................6
Cascading Raritan Devices .......................................................................6
Setting the Cascading Mode .....................................................................8

USB-Cascading Restrictions

- All devices in the USB-cascading configuration must be running appropriate firmware. See Software Requirements (on page 2).
- Depending on the firmware version you are using, up to four or eight Raritan devices can be connected.
- Only the Ethernet interface on the master device is enabled. The Ethernet interface on slave devices is disabled automatically. See Ethernet Disabled Scenarios on Slave Devices (on page 44).
- The Ethernet connectivity on the master device must be wired. That is, a standard network cable is required.
- Your network switch’s port security settings must support the USB-cascading solution. Make sure that packets forwarding is enabled for the Ethernet port where the master device is connected.
- The USB-cascading solution is NOT supported over a wireless network.

Cascading Raritan Devices

Only specific types of Raritan products support the USB-cascading function. See Hardware Requirements (on page 1).

To cascade Raritan devices:

1. Verify that the Raritan devices to be cascaded are running appropriate firmware versions by choosing Maintenance > Device Information in the web interface.

   If any device is running an inappropriate firmware, upgrade it. See Updating the Raritan device Firmware (on page 33).

2. Select one of the devices as the master device and connect it to the LAN via a standard network cable.
3. Connect the USB-A port of the master device to the USB-B port of an additional Raritan device via a USB cable. This additional device is Slave 1.

4. Connect Slave 1’s USB-A port to the USB-B port of another Raritan device via a USB cable. The second additional device is Slave 2.

5. Connect Slave 2’s USB-A port to the USB-B port of another Raritan device via a USB cable. The third additional device is Slave 3.

6. If your firmware supports eight devices, you may cascade four more devices. See Software Requirements (on page 2).

<table>
<thead>
<tr>
<th>Number</th>
<th>Device role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Master device</td>
</tr>
<tr>
<td>2</td>
<td>Slave 1</td>
</tr>
</tbody>
</table>
### Setting the Cascading Mode

This section only applies to the firmware versions that support two cascading modes. See **Software Requirements** (on page 2).

The Ethernet sharing mode applied to the USB-cascading configuration is either network bridging or port forwarding. This mode is determined by the master device only.

If bridging mode is intended, you must configure the network settings of each cascaded device respectively via the web interface or CLI.

If port forwarding mode is intended, you only need to configure the master device's network settings.

See **Configuring Network Settings** (on page 35).

> **To configure the cascading mode via the web interface:**

1. Log in to the master device.
2. Choose Device Settings > USB Cascading. The USB Cascading Configuration dialog appears.
3. Verify that the "Position in cascaded chain" field shows zero (0), indicating that this Raritan device is the master device.
4. Select the preferred cascading mode in the "Cascading mode" field.
   - Bridging: Each device in the USB-cascading configuration is accessed with a different IP address. This is the default.
   - Port Forwarding: Each device in the USB-cascading configuration is accessed with the same IP address with a different port number assigned. The port numbers vary based on the networking protocol and device position in the chain. See **Port Number Syntax** (on page 9).
5. Click OK.
6. If selecting Port Forwarding, a list of port numbers for various networking protocols will be available on the "Protocol to Port Mapping" tab of each cascaded device.
Chapter 3: USB-Cascading Instructions

Return to the same dialog and click the "Protocol to Port Mapping" tab to view the master device’s port numbers.

### Port Number Syntax

When the Port Forwarding mode is active, all devices in the USB-cascading configuration share the same IP address. To access these devices, you must assign an appropriate port number, which is either a 5NNXX port number for any cascaded device or the standard TCP/UDP port for the master device.

#### Syntax of 5NNXX port numbers:

- NN is a two-digit number representing the network protocol as shown below:

<table>
<thead>
<tr>
<th>Protocols</th>
<th>NN</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>00</td>
</tr>
<tr>
<td>HTTP</td>
<td>01</td>
</tr>
<tr>
<td>SSH</td>
<td>02</td>
</tr>
<tr>
<td>TELNET</td>
<td>03</td>
</tr>
<tr>
<td>SNMP</td>
<td>05</td>
</tr>
<tr>
<td>MODBUS</td>
<td>06</td>
</tr>
</tbody>
</table>
Chapter 3: USB-Cascading Instructions

- XX is a two-digit number representing the device position as shown below:

<table>
<thead>
<tr>
<th>Position</th>
<th>XX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master device</td>
<td>00</td>
</tr>
<tr>
<td>Slave 1</td>
<td>01</td>
</tr>
<tr>
<td>Slave 2</td>
<td>02</td>
</tr>
<tr>
<td>Slave 3</td>
<td>03</td>
</tr>
<tr>
<td>Slave 4</td>
<td>04</td>
</tr>
<tr>
<td>Slave 5</td>
<td>05</td>
</tr>
<tr>
<td>Slave 6</td>
<td>06</td>
</tr>
<tr>
<td>Slave 7</td>
<td>07</td>
</tr>
</tbody>
</table>

For example, to access the Slave 4 device via Modbus, the port number is 50604. See Port Forwarding Examples (on page 11) for further illustrations.

Tip: The full list of each cascaded device's port numbers can be retrieved by choosing Device Settings > USB Cascading > 'Protocol to Port Mapping' after logging in to each cascaded device. See Setting the Cascading Mode (on page 8).

▶ Standard TCP/UDP ports:

The master device can be accessed not only through 5NNXX port numbers but through standard TCP/UDP ports as listed in the following table.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Port Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>TELNET</td>
<td>23</td>
</tr>
<tr>
<td>SNMP</td>
<td>161</td>
</tr>
<tr>
<td>MODBUS</td>
<td>502</td>
</tr>
</tbody>
</table>

In the Port Forwarding mode, the Raritan device does NOT allow you to modify the standard TCP/UDP port configuration, including HTTP, HTTPS, SSH, Telnet, SNMP and Modbus/TCP.
Port Forwarding Examples
This section illustrates the way to access cascaded devices in the Port Forwarding mode.

Assumption: Three Raritan products are cascaded via USB. The Port Forwarding mode has been activated. The IP address assigned to this USB-cascaded configuration is 192.168.84.77.

In addition to the IP address, it requires the assignment of the appropriate port to access each cascaded device.

- To access the master device, assign proper 5NNXX port numbers or standard TCP/UDP ports.
  See Port Number Syntax (on page 9) for information on port numbers.
- To access any slave device, assign proper 5NNXX port numbers.

Master device:
Position code for the Master device is 00 so each port number is 5NN00 as shown in the following table.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Port numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>50000</td>
</tr>
<tr>
<td>HTTP</td>
<td>50100</td>
</tr>
<tr>
<td>SSH</td>
<td>50200</td>
</tr>
<tr>
<td>TELNET</td>
<td>50300</td>
</tr>
<tr>
<td>SNMP</td>
<td>50500</td>
</tr>
<tr>
<td>MODBUS</td>
<td>50600</td>
</tr>
</tbody>
</table>

Access examples using 5NN00 ports:
- To access the master device via HTTPS, the IP address is: https://192.168.84.77:50000/
- To access the master device via HTTP, the IP address is: http://192.168.84.77:50100/
- To access the master device via SSH, the command is: ssh -p 50200 192.168.84.77

Access examples using standard TCP/UDP ports:
- To access the master device via HTTPS, the IP address is: https://192.168.84.77:443/
- To access the master device via HTTP, the IP address is: http://192.168.84.77:80/
Chapter 3: USB-Cascading Instructions

- To access the master device via SSH, the command is:
  
  `ssh -p 22 192.168.84.77`

► **Slave 1 device:**

Position code for the Slave 1 device is 01 so each port number is 5NN01 as shown in the following table.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Port numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>50001</td>
</tr>
<tr>
<td>HTTP</td>
<td>50101</td>
</tr>
<tr>
<td>SSH</td>
<td>50201</td>
</tr>
<tr>
<td>TELNET</td>
<td>50301</td>
</tr>
<tr>
<td>SNMP</td>
<td>50501</td>
</tr>
<tr>
<td>MODBUS</td>
<td>50601</td>
</tr>
</tbody>
</table>

Access examples:

- To access Slave 1 via HTTPS, the IP address is:
  
  `https://192.168.84.77:50001/`

- To access Slave 1 via HTTP, the IP address is:
  
  `http://192.168.84.77:50101/`

- To access Slave 1 via SSH, the command is:
  
  `ssh -p 50201 192.168.84.77`

► **Slave 2 device:**

Position code for the Slave 2 device is 02 so each port number is 5NN02 as shown in the following table.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Port numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>50002</td>
</tr>
<tr>
<td>HTTP</td>
<td>50102</td>
</tr>
<tr>
<td>SSH</td>
<td>50202</td>
</tr>
<tr>
<td>TELNET</td>
<td>50302</td>
</tr>
<tr>
<td>SNMP</td>
<td>50502</td>
</tr>
<tr>
<td>MODBUS</td>
<td>50602</td>
</tr>
</tbody>
</table>

Access examples:

- To access Slave 2 via HTTPS, the IP address is:
  
  `https://192.168.84.77:50002/`
- To access Slave 2 via HTTP, the IP address is:
  \textit{http://192.168.84.77:50102/}
- To access Slave 2 via SSH, the command is:
  \textit{ssh -p 50202 192.168.84.77}
Chapter 4  Network Access

The master device functions as the network bridge and can transmit IP packets between the LAN and all slave devices connected to it. Therefore, you can remotely access the master and every slave device via the Web, SNMP, SSH, or Telnet interface, or manage them via Raritan's Power IQ or dcTrack™.

In This Chapter
Finding the IP Address .................................................................14
HTTP/HTTPS Access ......................................................................16
SSH/Telnet Access ...........................................................................18
SNMP Management ...........................................................................19
Power IQ and dcTrack Management ...............................................20

Finding the IP Address

There are various ways to retrieve the IP address of a Raritan device.

- Access the local console.
- Use the device’s MAC address and common networking tools.
- Operate the LCD display if the Raritan device is a PX3 PDU, PX3TS, BCM or EMX.

Local Console

The IP address of the master or slave device can be found in each device’s local console, which is a command line interface (CLI).

To access the local console, first connect the desired Raritan device to the computer using a serial RS-232 cable, and then use a terminal emulation program on the computer to access it.

Tip: For a master device, you can also access its local console via a USB connection.

You can use any terminal emulation programs for local access to the command line interface.

This section illustrates HyperTerminal, which is part of Windows operating systems prior to Windows Vista.

To get the IP address using HyperTerminal:
1. Connect your computer to the Raritan device via a local connection.
2. Launch HyperTerminal on your computer and open a console window. When the window first opens, it is blank.
Make sure the COM port settings use this configuration:

- Bits per second = 115200 (115.2Kbps)
- Data bits = 8
- Stop bits = 1
- Parity = None
- Flow control = None

3. In the communications program, press Enter to send a carriage return to the Raritan device. Now you should see the Raritan device’s IP address displayed in the terminal.

Note: If you haven’t configured the Raritan device, see its Quick Setup Guide, which accompanies the product and is also available on the Raritan website’s Support section (http://www.raritan.com/support/).

MAC Address

A label is affixed to the Raritan device, showing both the serial number and MAC address of this device.

If necessary, you can find its IP address through the MAC address by using commonly-used network tools. Contact your LAN administrator for assistance.

LCD Display

The IP address is available in the Device mode, which is indicated by the alphabet ‘d’ shown at the top of the LCD display. Note that the LCD display only shows the IPv4 address (if available).

Below illustrates the IP address information shown on the LCD display.
Chapter 4: Network Access

<table>
<thead>
<tr>
<th>Section</th>
<th>Example information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>'d' means the LCD display has entered the Device mode.</td>
</tr>
<tr>
<td>2</td>
<td>The LCD display is showing 192, which is one of the IP address octets. It will cycle through four octets of the IP address.</td>
</tr>
<tr>
<td>3</td>
<td>'i4' indicates that the IP address shown on the LCD display is an IPv4 address.</td>
</tr>
<tr>
<td>4</td>
<td>The word 'MASTER' indicates the PX is the master device in a USB-cascading configuration. For a standalone PX, this word is NOT displayed.</td>
</tr>
</tbody>
</table>

If you connect your PX to the wireless network, a Wi-Fi icon is displayed at the bottom-right corner.

![Wi-Fi icon with 'd' and 'H MASTER' on LCD display]

To retrieve the IP address:

1. Press the MODE button until device settings are displayed, indicated by a 'd' in at the top left of the display.
2. The LCD display cycles between the four octets of the IPv4 address, indicated by "i4" at the upper right corner of the display.

For example, if the IPv4 address is 192.168.84.4, the LCD display cycles through it as shown below:

192 --> 168 --> 84 --> 4

HTTP/HTTPS Access

You can remotely access the web interface of any Raritan device in a USB-cascaded configuration by using a web browser. See Supported Web Browsers for a list of supported web browsers.
Chapter 4: Network Access

**Supported Web Browsers**
The following web browsers can be used to access a Raritan device’s web interface. For details, see the online help or User Guide for your Raritan device.

- Internet Explorer®
- Firefox®
- Safari®
- Google® Chrome®
- IOS

**Using the Web Browser**
The web interface allows a maximum of 16 users to log in simultaneously.

You must enable JavaScript in the web browser for proper operation.

- **To log in to the web interface:**
  1. Open a browser, such as Microsoft Internet Explorer or Mozilla Firefox, and type this URL:
     
     ```
     http(s)://<ip address>
     ```
     where `<ip address>` is the IP address of the Raritan device.
  2. If a security alert message appears, click OK or Yes to accept. The Login page then opens.
  3. Type your user name in the User Name field, and password in the Password field.
     
     Note: Both the user name and password are case sensitive. Click Clear to clear either the inputs or any error message that appears.
  4. If a security agreement is displayed on the Login page, accept it. To select the agreement checkbox using the keyboard, press the Space bar.
     
     Note: If you do not accept the security agreement, you cannot log on to the Raritan device.
  5. Click Login or press Enter. The Raritan device page opens.
Chapter 4: Network Access

Note: Depending on your hardware configuration, elements shown on the web interface may appear slightly different from this image.

SSH/Telnet Access

All devices in the USB-cascaded configuration support the SSH or Telnet service.

You can remotely log in to the command line interface using an SSH or Telnet client, such as PuTTY.

Note: PuTTY is a free program you can download from the Internet. See PuTTY’s documentation for details on configuration.

To log in using SSH or Telnet:

1. Ensure SSH or Telnet has been enabled. See Modifying Network Service Settings in the User Guide.
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

   login as:
3. Type a name and press Enter. The name is case sensitive.

*Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.*

Then you are prompted to enter a password.

```
login as: admin
admin@192.168.84.88's password: 
```

4. Type a password and press Enter. The password is case sensitive.

5. After properly entering the password, the # or > system prompt appears. See Different CLI Modes and Prompts in the User Guide for more information.

*Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was once used to log in to this product's web interface or CLI.*

You are now logged in to the command line interface and can begin administering the Raritan device.

**SNMP Management**

In the USB-cascading configuration, the SNMP capability of each Raritan device remains unchanged. A cascaded device is able to send SNMP notifications and communicate with an SNMP manager.

**SNMP Notifications**

To make a Raritan device in the USB-cascaded configuration send out SNMP traps or informs to an SNMP destination when an event occurs, you have to configure the SNMP notification setting on that device. For details, see the section titled Configuring SNMP Notifications in the online help, which is available from the application or on the Raritan website's **Support section** (http://www.raritan.com/support/).

**Third-Party SNMP Managers**

A third-party SNMP manager can communicate with any Raritan device in the USB-cascaded configuration. There are no differences made to the SNMP accessibility regardless of whether the device is a master or slave device.

To allow a Raritan device to communicate with an SNMP manager, you must enable the SNMP agent implemented on that device and download the latest SNMP MIB for your SNMP manager. For details, see the section titled Enabling SNMP in the online help, which is available from the application or on the Raritan website's **Support section** (http://www.raritan.com/support/).
Power IQ and dcTrack Management

The way to manage a cascaded Raritan device with Raritan's Power IQ and dcTrack™ is the same as managing a standalone Raritan device.

**Power IQ**

Raritan's Power IQ is a software application that collects and manages the data from different PDUs installed in your server room or data center. With this software, you can:

- Do bulk configuration for multiple PDUs
- Name outlets on different PDUs
- Switch on/off outlets on outlet-switching capable PDUs

For more information on Power IQ, see either of the following:


**dcTrack**

Raritan's dcTrack™ is a software application that collects the data of all components implemented in the data center, including power and non-power items, and then administers and maintains the data center efficiently after the data center building is completed in dcTrack.

Each Raritan device in the USB-cascaded configuration can be added to dcTrack, and communicate with dcTrack via SNMP separately.

For more information on dcTrack, see the online help accessible from the dcTrack application.
Chapter 5  Identifying Cascaded Devices

You can retrieve a Raritan device’s USB-cascading status by operating one of the following interfaces:

- Web interface: Accessible via HTTP or HTTPS.
- Command line interface (CLI): Accessible via SSH, Telnet or the serial interface.
- SNMP: An SNMP manager is required.
- LCD display: Use the LCD only if your Raritan device has the LCD display.

Before you can remotely access a Raritan device, you need to get its IP address. See Finding the IP Address (on page 14).

In This Chapter

Using the Web Interface..............................................................21
Using the CLI.................................................................................28
Using the SNMP..........................................................................30
Using the LCD Display ...............................................................31

Using the Web Interface

This section explains how to identify a cascaded Raritan device through the web interface. The web interface differs depending on your firmware versions.

See Software Requirements (on page 2) for information on different firmware versions.

► When your firmware supports two cascading modes:

1. Log in to the desired Raritan device using a supported web browser. See HTTP/HTTPS Access (on page 16).
2. Choose Maintenance > Device Information. The Device Information dialog appears.
3. Select the Network tab and locate the Interface section. The Interface section contains four read-only fields as listed below.
## Chapter 5: Identifying Cascaded Devices

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking Mode</td>
<td>Indicates how the Raritan device is connected to the LAN.</td>
</tr>
<tr>
<td></td>
<td>- Wired: The device is connected to the LAN through a standard network cable.</td>
</tr>
<tr>
<td></td>
<td>- Wired (USB): The device is connected to the LAN through a USB-cascaded configuration. In other words, it is a slave device.</td>
</tr>
<tr>
<td>Cascading Mode</td>
<td>Shows the cascading mode being activated. See [Setting the Cascading Mode](on page 8).</td>
</tr>
<tr>
<td>Cascade Position</td>
<td>Indicates the position of the Raritan device in the USB-cascading configuration.</td>
</tr>
<tr>
<td></td>
<td>- 0 (zero) represents the master device.</td>
</tr>
<tr>
<td></td>
<td>- A non-zero number represents a slave device. 1 is the 1st slave, 2 is the 2nd slave, 3 is the 3rd slave and so on.</td>
</tr>
<tr>
<td>Cascaded Device Connected</td>
<td>Indicates whether the presence of a slave device is detected on the USB-A port.</td>
</tr>
<tr>
<td></td>
<td>- yes: Connection to a slave device is detected.</td>
</tr>
<tr>
<td></td>
<td>- no: NO connection to a slave device is detected.</td>
</tr>
</tbody>
</table>

- A master device shows 0 (zero) in the Cascade Position field and yes in the Cascaded Device Connected field.
Chapter 5: Identifying Cascaded Devices

Note: If a master device has NO slave devices connected to it, it is a standalone device.

- A slave device in the middle position shows a non-zero number which indicates its exact position in the Cascade Position field and yes in the Cascaded Device Connected field.
Chapter 5: Identifying Cascaded Devices

The following diagram shows 1, indicating it is the first slave.

- The final slave device shows a non-zero number which indicates its position in the Cascade Position field and no in the Cascaded Device Connected field.
Chapter 5: Identifying Cascaded Devices

The following diagram shows 2, indicating it is the second slave.

![Device Information](image)

**When your firmware supports the 'Bridging' mode only:**

1. Choose Maintenance > Device Information. The Device Information dialog appears.
2. Select the Network tab and locate the Interface section. The Interface section contains two read-only fields: Networking Mode and Cascaded Device Connected.
A master device shows **Wired** in the Networking Mode field and **yes** in the Cascaded Device Connected field.
A slave device in the middle position shows *Wired (USB)* in the Networking Mode field and *yes* in the Cascaded Device Connected field.
Chapter 5: Identifying Cascaded Devices

- The final slave device shows *Wired (USB)* in the Networking Mode field and *no* in the Cascaded Device Connection field.

![Device Information](image)

### Using the CLI

This section explains how to identify a cascaded Raritan device through the CLI. The ways to identify a cascaded device vary according to your firmware version.

See **Software Requirements** (on page 2) for information on different firmware versions.

► **When your firmware supports two cascading modes:**

1. Log in to the CLI of the desired Raritan device. To use the SSH or Telnet service, see *SSH/Telnet Access* (on page 18).
2. Type either of the following CLI commands and press Enter.
   
   ```
   # show cascading
   ```

   ```
   # show cascading details
   ```
3. Locate the 'Position' field displayed onscreen.
   - A master device shows 0 (Master).
If a master device has NO slave devices connected to it, it is a standalone device. See step 4 for how to determine the presence of a connected slave device.

- A slave device shows a non-zero number which indicates its position. For example:
  1 (Slave 1) is the first slave device.
  2 (Slave 2) is the second slave device.

4. To check whether a slave device is connected to the Raritan device’s USB-A port, type either of the following CLI commands.

```
# show network
```

A final slave device or a standalone device shows no in the "Cascaded device connected" field, indicating that there is no slave device connected to its USB-A port. Otherwise, it shows yes.

```
Cascaded device connected: no
```

► When your firmware supports the 'Bridging' mode only:

1. Log in to the CLI.
2. Type either of the following CLI commands.

```
# show network
```

3. Locate the "Networking mode" and "Cascaded device connected" fields displayed onscreen.

- A master device shows Wired in the "Networking mode" field and yes in the "Cascaded device connected" field.

```
Networking mode: Wired
Cascaded device connected: yes
```

- A slave device in the middle position shows Wired (USB) in the "Networking mode" field and yes in the "Cascaded device connected" field.

```
Networking mode: Wired (USB)
Cascaded device connected: yes
```

- A final slave device shows Wired (USB) in the "Networking mode" field and no in the "Cascaded device connected" field.

```
Networking mode: Wired (USB)
Cascaded device connected: no
```
Later firmware versions retrieve more USB-cascading information via SNMP than earlier firmware versions. See **Software Requirements** (on page 2) for information on different firmware versions.

The `unitConfigurationTable` in SNMP contains entries for USB-cascading information. One SNMP MIB manager, such as an MIB browser, is required for the following operation.

**When your firmware supports two cascading modes:**

1. Launch your SNMP MIB manager and connect to the desired Raritan device.

2. To identify the USB-cascaded state of the Raritan device, retrieve the value of either of the following:
   - **SNMP name** - `pduDaisychainMemberType`
   - **SNMP object identifier (OID)** - `1.3.6.1.4.1.13742.6.3.2.2.1.41`

Check which of the following values is returned.

<table>
<thead>
<tr>
<th>SNMP value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>standalone (0)</td>
<td>The Raritan device is a standalone device. It is not in the USB-cascading configuration.</td>
</tr>
<tr>
<td>master (1)</td>
<td>The Raritan device is a master device in the USB-cascading configuration.</td>
</tr>
<tr>
<td>slave (2)</td>
<td>The Raritan device is a slave device in the USB-cascading configuration.</td>
</tr>
</tbody>
</table>

3. If your Raritan device is a slave device, you can find out whether it is the final one by retrieving the value of either of the following:
   - **SNMP name** - `cascadedDeviceConnected`
   - **SNMP object identifier (OID)** - `1.3.6.1.4.1.13742.6.3.2.2.1.58`

Check which value is returned. A final slave device has NO slave device connected to its USB-A port.

<table>
<thead>
<tr>
<th>SNMP value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>true (1)</td>
<td>A slave device has been connected to this Raritan device’s USB-A port.</td>
</tr>
<tr>
<td>false (2)</td>
<td>No slave device is connected to this Raritan device’s USB-A port.</td>
</tr>
</tbody>
</table>
When your firmware supports the 'Bridging' mode only:

Use the cascadedDeviceConnected object to determine whether your Raritan device is a USB-cascaded device. See step 3 in the above procedure for details.

Using the LCD Display

This section only applies to Raritan products that have an LCD display.

A USB-cascaded device's position can be found by operating its LCD display. Use the MODE button to switch between different modes. When in device mode, a small "d" is displayed in the upper left corner.

Below illustrates a slave device's position shown on the LCD display.

<table>
<thead>
<tr>
<th>Section</th>
<th>Example information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>'d' means the LCD display has entered the Device mode.</td>
</tr>
<tr>
<td>2</td>
<td>'CA' indicates that the USB-cascading information is being displayed.</td>
</tr>
<tr>
<td>3</td>
<td>'SLAVE' indicates that this Raritan device is a slave device.</td>
</tr>
<tr>
<td>4</td>
<td>The number 1 means the device position is Slave 1.</td>
</tr>
</tbody>
</table>

To retrieve the device's USB-cascading position information:

1. Press the MODE button until device settings are displayed, indicated by a 'd' in at the top left of the display.

2. Press the FUNC button until 'CA' is displayed at the top right of the display.

3. The device's position is represented by any number defined below:

<table>
<thead>
<tr>
<th>Number</th>
<th>Device position</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Master device</td>
</tr>
<tr>
<td>Number</td>
<td>Device position</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------</td>
</tr>
<tr>
<td>1</td>
<td>Slave 1</td>
</tr>
<tr>
<td>2</td>
<td>Slave 2</td>
</tr>
<tr>
<td>3</td>
<td>Slave 3</td>
</tr>
<tr>
<td>4</td>
<td>Slave 4</td>
</tr>
<tr>
<td>5</td>
<td>Slave 5</td>
</tr>
<tr>
<td>6</td>
<td>Slave 6</td>
</tr>
<tr>
<td>7</td>
<td>Slave 7</td>
</tr>
</tbody>
</table>

*Note: For a standalone Raritan device, its position is always the number 0.*

*Tip: Always attach the Ethernet cable to the new MASTER device after disconnecting or reversing the USB cable, or the device’s USB-cascading status will not get updated automatically on the LCD display. For example, if you disconnect the USB cable from a slave device, connect the Ethernet cable to that slave device to update its USB-cascading status.*
Chapter 6  Updating the Raritan device Firmware

You can upgrade each individual Raritan device in the USB-cascading configuration through the web interface. The upgrade procedure is completely identical to a standalone Raritan device.

The Raritan device firmware files are available on the Raritan website’s Support section (http://www.raritan.com/support/).

You must be the system administrator or log in to the user profile with the Firmware Update permission to update the Raritan device's firmware.

If applicable to your model, download the latest firmware file from the Raritan website, read the release notes, then start the upgrade. If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

**Warning:** Do NOT perform the firmware upgrade over a wireless network connection.

**To update the firmware:**
2. In the Firmware File field, click Browse to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload status.
4. When the upload is complete, version information of both the existing firmware and uploaded firmware is shown, providing you a last chance to terminate the update.
5. To view the certificate of the uploaded firmware, click View Certificate. **Optional.**
6. To proceed with the update, click Update Firmware. The update may take several minutes.

**Warning:** Do NOT power off the Raritan device during the update.

During the firmware update:
- A progress bar appears in the web interface, indicating the update status.
- The LED or LCD display on the Raritan device shows three digits: ‘FuP’ or ‘FUP.’
- No users can successfully log in to the Raritan device.
- The user management operation, if any, is forced to suspend.
Chapter 6: Updating the Raritan device Firmware

7. When the update is complete, a message appears, indicating the update is successful.

8. The Raritan device resets, and the Login page re-appears. You can now log in and resume your operation.

Note 1: The other logged-in users are also logged out when the firmware update is complete.

Note 2: If you are using the Raritan device with an SNMP manager, download its MIB again after the firmware update to ensure your SNMP manager has the correct MIB for the latest release you are using. See Using SNMP in the online help.
Appendix A Configuring Network Settings

Network settings can be configured through either the web interface or command line interface (CLI). This appendix only shows basic operation. For details, see the online help or User Guide for your Raritan device.

In This Chapter
Configuration via Web Interface...............................................................35
Configuration via CLI ...............................................................................36

Configuration via Web Interface
When you are able to connect to the master or slave device over Internet, you can use the web interface to change its network settings.

► To change initial network settings:
1. Launch a web browser and type the IP address of the Raritan device in the address bar.
2. Accept any warnings that may appear and log in to that Raritan device using the administrator account.
   - User name: admin
   - Password: raritan (or a new password if you have changed the password)
3. If this is the first time for you to log in to the Raritan device, you are prompted to change the password. Then type the new password.
5. Click the IP Protocol tab to enable IPv4, IPv6 or both.
6. Depending on which IP protocol has been enabled in the above step, click the corresponding tab to change the IP address settings.
   - If IPv4 is enabled, click the IPv4 Settings tab.
   - If IPv6 is enabled, click the IPv6 Settings tab.
   - If both is enabled, click both tabs to configure IP addresses respectively.
Appendix A: Configuring Network Settings

**Configuration via CLI**

If you want to configure a master or slave device's network settings via CLI, you must connect that device to a computer via a serial RS-232 connection. The master device's CLI can be also accessed through a USB connection.

**To configure network settings via CLI:**

1. On the computer connected to the Raritan device, open a communications program such as HyperTerminal or PuTTY.
2. Select the appropriate COM port, and set the following port settings:
   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   *Tip: For a USB connection, you can determine the COM port by choosing Control Panel > System > Hardware > Device Manager, and locating the "XXX Serial Console" under the Ports group, where XXX represents this product's name.*

3. In the communications program, press Enter to send a carriage return to the Raritan device.
4. The Raritan device prompts you to log in. Both user name and password are case sensitive.
   a. At the Username prompt, type `admin` and press Enter.
   b. At the Password prompt, type `raritan` and press Enter.
5. If you are prompted to change the password, follow onscreen instructions to type your new password.
6. The # prompt appears.
7. Type `config` and press Enter.
8. To configure network settings, type appropriate commands, and press Enter. All commands are case sensitive.
   a. To set the networking mode, type this command:
      ```
      network mode <mode>
      ```
      where `<mode>` is `wired` (default) or `wireless`.
   b. For the wired network mode, you may configure the LAN interface settings. In most scenarios, the default setting (auto) works well and should not be changed unless required.
Appendix A: Configuring Network Settings

<table>
<thead>
<tr>
<th>To set</th>
<th>Use this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN interface speed</td>
<td>network interface LANInterfaceSpeed &lt;option&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;option&gt; = auto, 10Mbps, or 100Mbps.</td>
</tr>
<tr>
<td>LAN interface duplex mode</td>
<td>network interface LANInterfaceDuplexMode &lt;mode&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;mode&gt; = half, full or auto.</td>
</tr>
</tbody>
</table>

*Tip: You can combine multiple commands to configure multiple parameters at a time. For example, network interface LANInterfaceSpeed <option> LANInterfaceDuplexMode <mode>*

c. For the wireless network mode, you must configure the Service Set Identifier (SSID) parameter.

<table>
<thead>
<tr>
<th>To set</th>
<th>Use this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>network wireless SSID &lt;ssid&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;ssid&gt; = SSID string</td>
</tr>
</tbody>
</table>

If necessary, configure more wireless parameters shown in the following table.

<table>
<thead>
<tr>
<th>To set</th>
<th>Use this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID</td>
<td>network wireless BSSID &lt;bssid&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;bssid&gt; = AP MAC address or none</td>
</tr>
<tr>
<td>Authentication method</td>
<td>network wireless authMethod &lt;method&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;method&gt; = psk or eap</td>
</tr>
<tr>
<td>PSK</td>
<td>network wireless PSK &lt;psk&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;psk&gt; = PSK string</td>
</tr>
<tr>
<td>EAP outer authentication</td>
<td>network wireless eapOuterAuthentication &lt;outer-auth&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;outer-auth&gt; = PEAP</td>
</tr>
</tbody>
</table>
Appendix A: Configuring Network Settings

<table>
<thead>
<tr>
<th>To set</th>
<th>Use this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP inner authentication</td>
<td><code>network wireless eapInnerAuthentication &lt;inner_auth&gt;</code>&lt;br&gt;<code>&lt;inner_auth&gt; = MSCHAPv2</code></td>
</tr>
<tr>
<td>EAP identity</td>
<td><code>network wireless eapIdentity &lt;identity&gt;</code>&lt;br&gt;<code>&lt;identity&gt; = your user name for EAP authentication</code></td>
</tr>
<tr>
<td>EAP password</td>
<td><code>network wireless eapPassword</code>&lt;br&gt;When prompted to enter the password for EAP authentication, type the password.</td>
</tr>
<tr>
<td>EAP CA certificate</td>
<td><code>network wireless eapCACertificate</code>&lt;br&gt;When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.</td>
</tr>
</tbody>
</table>

*Note: The content to be copied from the CA certificate does NOT include the first line containing "BEGIN CERTIFICATE" and the final line containing "END CERTIFICATE."*

d. To determine which IP protocol (IPv4 or IPv6) is enabled and which IP address (IPv4 or IPv6) returned by the DNS server is used, configure the following parameters.

<table>
<thead>
<tr>
<th>To set</th>
<th>Use this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP protocol</td>
<td><code>network ip proto &lt;protocol&gt;</code>&lt;br&gt;<code>&lt;protocol&gt; = v4Only, v6Only or both</code></td>
</tr>
<tr>
<td>IP address returned by the DNS server</td>
<td><code>network ip dnsResolverPreference &lt;resolver&gt;</code>&lt;br&gt;<code>&lt;resolver&gt; = preferV4 or preferV6</code></td>
</tr>
</tbody>
</table>

e. After enabling the IPv4 or IPv6 protocol in the earlier step, configure the IPv4 or IPv6 network parameters.
To set | Use this command
---|---
IPv4 configuration method | network ipv4 ipConfigurationMode `<mode>`  
`<mode>` = dhcp (default) or static

IPv6 configuration method | network ipv6 ipConfigurationMode `<mode>`  
`<mode>` = automatic (default) or static

- Configure the preferred host name for the IPv4 DHCP or IPv6 automatic configuration.

Note: The `<version>` variable in all of the following commands is either `ipv4` or `ipv6`, depending on the type of the IP protocol you have enabled.

---

To set | Use this command
---|---
Preferred host name (optional) | network `<version>` preferredHostName `<name>`  
`<name>` = preferred host name

Tip: To override the DHCP-assigned DNS servers with those you specify manually, type this command:

```
network `<version>` overrideDNS `<option>`
```

where `<option>` is enable or disable. See the table below for the commands for manually specifying DNS servers.

- For the static IP configuration, configure these parameters.

---

To set | Use this command
---|---
Static IPv4 or IPv6 address | network `<version>` ipAddress  
`<ip address>` = static IP address

IPv4 subnet mask | network ipv4 subnetMask  
`<netmask>` = subnet mask
To set | Use this command
---|---
IPv4 or IPv6 gateway | `network <version> gateway <ip address>`
| `<ip address> = gateway's IP address`
IPv4 or IPv6 primary DNS server | `network <version> primaryDNSServer <ip address>`
| `<ip address> = IP address of the primary DNS server`
IPv4 or IPv6 secondary DNS server (optional) | `network <version> secondaryDNSServer <ip address>`
| `<ip address> = IP address of the secondary DNS server`

9. To quit the configuration mode, type either of the following commands, and press Enter.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply</td>
<td>Save all configuration changes and exit.</td>
</tr>
<tr>
<td>cancel</td>
<td>Abort all configuration changes and exit.</td>
</tr>
</tbody>
</table>

The # prompt appears, indicating that you have quit the configuration mode.

10. To verify whether all settings are correct, type the following commands one by one.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show network</td>
<td>Show network parameters.</td>
</tr>
<tr>
<td>show network ip all</td>
<td>Show all IP configuration parameters.</td>
</tr>
<tr>
<td>show network wireless details</td>
<td>Show all wireless parameters.</td>
</tr>
</tbody>
</table>

*Tip: You can type "show network wireless" to display a shortened version of wireless settings.*

If all are correct, type `exit` to log out of the Raritan device. If any are incorrect, repeat Steps 7 to 10 to change network settings.
Appendix B Accessibility Troubleshooting

Any accessibility problem occurred on one of the devices in the USB-cascading configuration may result in failure to access all subsequent slave devices that are connected to it.

In This Chapter
Possible Root Causes ................................................................. 41
Slave Connection and Disconnection Events ............................... 42
The Ping Tool ................................................................................. 42

Possible Root Causes

The following lists the network accessibility issues and possible root causes.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Probable cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to access the master</td>
<td>● Network connection to the master device is lost.</td>
</tr>
<tr>
<td>device</td>
<td>● No power is supplied to the master device.</td>
</tr>
<tr>
<td>Failure to access a slave</td>
<td>● Network connection to the master device is lost.</td>
</tr>
<tr>
<td>device</td>
<td>● USB connection to the slave device in question or any prior slave device (if available) is lost.</td>
</tr>
<tr>
<td></td>
<td>● No power is supplied to the slave device in question or any prior cascaded devices.</td>
</tr>
</tbody>
</table>
|                                | ● Inappropriate firmware version is loaded to the Raritan device in question or any prior cascaded devices. See Software Requirements (on page 2).

Tip: To determine which Raritan device may be the failure point of network, you may ping each Raritan device in the USB-cascading configuration, or look for the slave-related events in each Raritan device's event log. See Slave Connection and Disconnection Events (on page 42) and The Ping Tool (on page 42).
Appendix B: Accessibility Troubleshooting

Slave Connection and Disconnection Events

Whenever the connection or disconnection of a subsequent slave device is detected, the Raritan device at the USB-A end of the USB cable logs it in the internal log. Note that the Raritan device at the USB-B end of the cable does NOT log these events.

There are two slave-related events:

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB slave connected</td>
<td>This is the log entry that is generated when a Raritan device detects the presence of a slave device on its USB-A port.</td>
</tr>
<tr>
<td>USB slave disconnected</td>
<td>This is the log entry that is generated when it detects the disconnection of a slave device on its USB-A port.</td>
</tr>
</tbody>
</table>

The Ping Tool

The Raritan device provides a ping tool in the web interface and CLI so you can ping any host or Raritan device in your data center.

Using the Web Interface

To log in to the web interface, see HTTP/HTTPS Access (on page 16).

The Ping tool is useful for checking whether a host is accessible through the network or Internet.

To ping a host:
1. Choose Maintenance > Network Diagnostics > Ping. The Ping Network Host dialog appears.
2. In the Host Name field, type the name or IP address of the host that you want to check.
3. In the Number of Requests field, type a number up to 20 or adjust the value by clicking either arrow. This number determines how many packets are sent for pinging the host.
4. Click Run Ping to start pinging the host. A dialog appears, displaying the Ping results.
5. Click Close to quit the dialog.
Using the CLI

You can access the CLI interface by connecting a computer to the Raritan device or using SSH/Telnet. See **SSH/Telnet Access** (on page 18) for details.

You must perform the ping command in the diagnostic mode. To enter the diagnostic mode, type the following command and press Enter.

```
# diag
```

After the diag> or diag# prompt appears, you can perform the ping command.

This ping command sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good. If not, either the host is shut down or it is not being properly connected to the network.

```
diag> ping <host>
```

**Variables:**

- `<host>` is the host name or IP address whose networking connectivity you want to check.

**Options:**

- You can include any or all of additional options listed below in the ping command.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count <code>&lt;number1&gt;</code></td>
<td>Determines the number of messages to be sent. <code>&lt;number1&gt;</code> is an integer number between 1 and 100.</td>
</tr>
<tr>
<td>size <code>&lt;number2&gt;</code></td>
<td>Determines the packet size. <code>&lt;number2&gt;</code> is an integer number in bytes between 1 and 65536.</td>
</tr>
<tr>
<td>timeout <code>&lt;number3&gt;</code></td>
<td>Determines the waiting period before timeout. <code>&lt;number3&gt;</code> is an integer number in seconds ranging from 1 to 600.</td>
</tr>
</tbody>
</table>

The command looks like this syntax when it includes all options:

```
diag> ping <host> count `<number1>` size `<number2>` timeout `<number3>`
```
Appendix C Ethernet Disabled Scenarios on Slave Devices

The Ethernet interface is automatically disabled on slave devices. This appendix illustrates this limitation by showing two scenarios.

In This Chapter
Ethernet Disabled Example 1 ...............................................................44
Ethernet Disabled Example 2 ...............................................................45

Ethernet Disabled Example 1

Raritan device-1 has been directly connected to the LAN. Its Ethernet interface is enabled and networking mode shows Wired.

Raritan device-2 has been directly connected to the LAN. Its Ethernet interface is enabled and networking mode shows Wired.

If now you connect Raritan device-1 to the USB-B port of Raritan device-2 using a USB cable, the following changes occur:

- Raritan device-1 becomes the master device.
- Raritan device-2 becomes a slave device.
- The Ethernet interface on Raritan device-2 is automatically disabled. All of its IP packets are transmitted through Raritan device-1.
- The networking mode of Raritan device-2 changes to Wired (USB), indicating that it is connected to the network through the master device.
Ethernet Disabled Example 2

Raritan device-1 is a master device, which has Raritan device-2 connected to its USB-A port. On Raritan device-1, the Ethernet interface is enabled, and the networking mode shows Wired.

Raritan device-2 is a slave device, whose Ethernet interface has been disabled, networking mode shows Wired (USB), and IP packets are transmitted through the master device.

If you directly connect Raritan device-2 to the LAN now, NO changes occur.

- Raritan device-2 continues to operate as a slave device.
- The networking mode of Raritan device-2 still shows Wired (USB).
- The Ethernet interface on Raritan device-2 remains disabled. All of its IP packets are still transmitted through the master device.
Index

A
Accessibility Troubleshooting • 41
Appropriate Applications • 3

B
Best Practices • 5

C
Cascading Raritan Devices • 6
Configuration via CLI • 36
Configuration via Web Interface • 35
Configuring Network Settings • 8, 35

D
dcTrack • 20

E
Ethernet Disabled Example 1 • 44
Ethernet Disabled Example 2 • 45
Ethernet Disabled Scenarios on Slave Devices • 6, 44

F
Finding the IP Address • 14, 21

H
Hardware Requirements • 1, 6
HTTP/HTTPS Access • 16, 21, 42

I
Identifying Cascaded Devices • 21
Inappropriate Applications • 5
Introduction • 1

L
LCD Display • 15
Local Console • 14

M
MAC Address • 15

N
Network Access • 14

P
Plug and Play • 2
Port Forwarding Examples • 9, 10, 11, 18
Port Number Syntax • 8, 9, 11
Possible Root Causes • 41
Power IQ • 20
Power IQ and dcTrack Management • 20

S
Safety Guidelines • ii
Safety Instructions • iii
Setting the Cascading Mode • 2, 8, 10, 22
Slave Connection and Disconnection Events • 41, 42
SNMP Management • 19
SNMP Notifications • 19
Software Requirements • 2, 6, 7, 8, 21, 28, 30, 41
SSH/Telnet Access • 18, 28, 43
Supported Web Browsers • 17

T
The Ping Tool • 41, 42
Third-Party SNMP Managers • 19

U
Updating the Raritan device Firmware • 2, 6, 33
USB-Cascading Applications • 3
USB-Cascading Instructions • 6
USB-Cascading Restrictions • 6
Using the CLI • 28, 43
Using the LCD Display • 31
Using the SNMP • 30
Using the Web Browser • 17
Using the Web Interface • 21, 42
U.S./Canada/Latin America
Monday - Friday
8 a.m. - 6 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: +81-3-5795-3170
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. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

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