Raritan.

A brand of **legrand**

BCM2 Series Power Meter

User Guide

Release 3.3.10

FreeType Project Copyright Notice

Portions of this software are copyright © 2015 The FreeType Project (www.freetype.org). All rights reserved.

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，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。　　　VCCI－A

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.

Safety Information

Welcome

RISK OF EQUIPMENT DAMAGE

- This product is designed only for use with 0.33V output current transducers (CTs).
- DO NOT USE CURRENT OUTPUT (e.g. 5A) CTs ON THIS PRODUCT.
- Failure to follow these instructions can result in overheating and permanent equipment damage.

For use in a Pollution Degree 2 or better environment only. A Pollution Degree 2 environment must control conductive pollution and the possibility of condensation or high humidity. Consider the enclosure, the correct use of ventilation, thermal properties of the equipment, and the relationship with the environment. Installation category: CAT II or CAT III

Provide a disconnect device to disconnect the meter from the supply source. Place this device in close proximity to the equipment and within easy reach of the operator, and mark it as the disconnecting device. The disconnecting device shall meet the relevant requirements of IEC 60947-1 and IEC 60947-3 and shall be suitable for the application. Disconnecting fuse holders can be used in the USA and Canada. Provide overcurrent protection and disconnecting device for supply conductors with approved current limiting devices suitable for protecting the wiring.

If the equipment is used in a manner not specified by the manufacturer, the protection provided by the device may be impaired.

This symbol indicates an electrical shock hazard exists.

Documentation must be consulted where this symbol is used on the product.

BCM2 Series Power Meter Release 3.3.10 User Guide

Contents

Raritan.
A brand of legrand

Raritan.
A brand of ☐ legrand

Chapter 1 Introduction

In This Chapter

Product Models

BCM2 software applies to both the Power Meter Series modular power meter and branch circuit monitor products (PMM, PMB, PMMC, and PMC), and the BCM2 power meter product.

Raritan.
A brand of legrand

Product Overview - PM Series Power Meters

Raritan PM series power meters is a modular power metering solution comprising three components.

PMM: a 3-phase power meter with neutral and earth current monitoring.

PMB: a 96 channel branch circuit monitor that plugs into PMM. A PMM+PMB monitors a panel board mains and branch circuit.

PMC: power meter controller. One PMC controls up to 70 PMM or 8 PMM+PMB. Interconnection uses standard shielded CAT-5 cable. All modules receive redundant power and continue to function as long as one or more PMM remain powered.

Raritan PM series power meters are designed for ease of use:

CTs are available in various ratings and contain built-in burden resistors so they can be snapped onto live wires without damage.

CT orientation is not critical because meter auto-corrects polarity for any CT installed backwards.

CT connections are made close to branch circuits using multi-conductor wiring harnesses with individual CT wire-pairs labeled and terminated with a keyed connector.

PMM
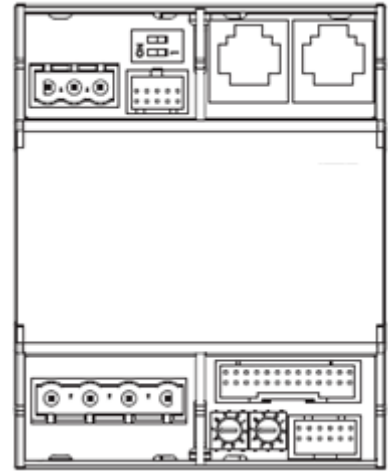
PMB
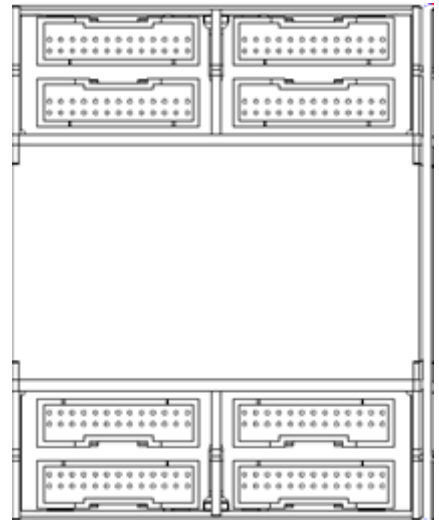
PMC
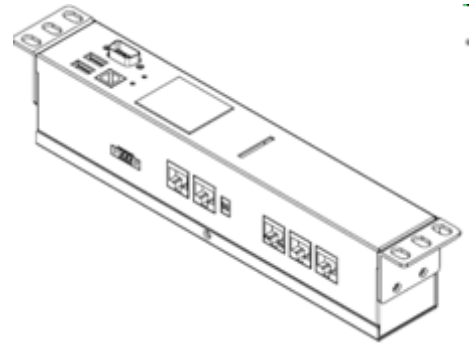
Product Overview - BCM2 Series

Raritan BCM2 is a 96 channel branch circuit monitor.

Models available with or without built-in meter controller, with power line cords or field wiring terminals.

One meter controller (built-in or external) interconnects one to eight BCM2. Built-in controller is top or front mountable.   External controller rack mounts or attaches to PDU access door.

▶   BCM2_96xx (with built-in controller)   ▶   External meter controller
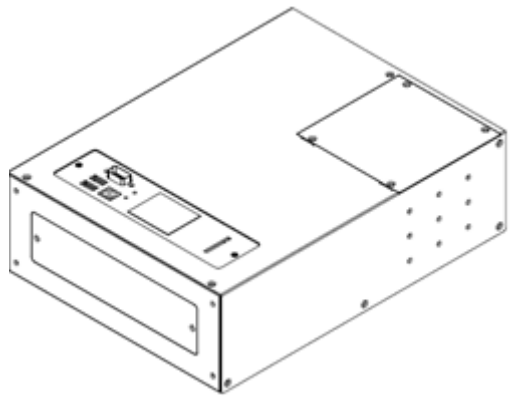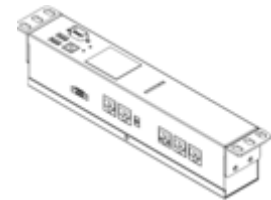
Mounting kits are available for subfloor, rack or wall. Floor and rack mount kits hold one or two BCM2 meters.
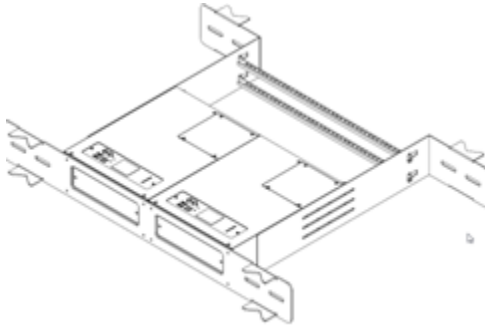
BCM2_FLOOR_MOUNT_KIT   BCM2_RACK_MOUNT_KIT   BCM2_WALL_MOUNT_KIT
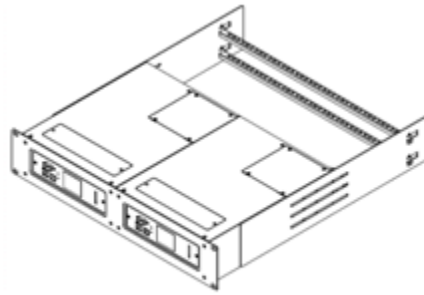
Chapter 2   Installation and Initial Configuration

- This equipment must only be installed and serviced by qualified electrical personnel.
- Read, understand and follow the instructions before installing this product.
- See *Safety Information* (on page iii).

In This Chapter

Hardware Installation

Please refer to the Quick Setup Guide for your product. The printed guide is in your product box, or you can download from the BCM2 Support page on Raritan.com

BCM2 Series Branch Circuit Monitor Quick Setup Guide

Power Meter Series Quick Setup Guide

Login and Configuration

Connect your PC directly to the BCM2 to complete the initial configuration.

▶ **To access the web interface at the rack:**

1. Disable the wireless interface of the PC.
2. Connect a cat 5 cable between the PC and BCM2 network ports.
3. Open a browser. Enter the URL "https://pdu.local". The login page appears.

   If the URL does not resolve, use the IP address of the PMC. Retrieve the direct IP address using the LCD display: Menu > Device Information, scroll to the IPV4 settings. Enter the IP address in the web browser:"https://IP address/"

4. Login with the default username and password. Allow 30 seconds for first connection.
   - Username: admin
   - Password: raritan

Configuring Power Meters and Branch Circuit Monitors

You can configure your product with a spreadsheet, or in the product's web interface.

▶ **To configure with a spreadsheet:**

Go to Raritan.com and download the configuration spreadsheet from the BCM2 Support page. Follow the instructions in the spreadsheet.

▶ **To configure with the product web interface:**

Make a network connection to the product. See *Login and Configuration* (on page 6). Follow the instructions in this guide, starting with: *Scan Power Meters* (on page 7).

Scan Power Meters

① Click Power Meters.

If nothing is configured, scan begins immediately in the Unconfigured Meters section. Click Rescan to refresh the list.

② Click the power meter or panel in the discovered list to configure it.

③ Types:

PM: 3-phase

Panel: BCM

Configure Power Meter

①   Enter a name.

     Select the circuit type:

②   ▪   Single Phase

     ▪   Split Phase

     ▪   3-phase

③   Enter the mains circuit breaker rating.

④   Select the checkbox for each CT installed.

     Enter the CT rating. Ratings are marked on the CT.

⑤   Click OK.

     The configured power meter displays in the dashboard and Power Meters page.

Power Meter 9 (PMM-1)	⋮

Settings

Name	❶	PMM-1
Type	❷	3-Phase

Modbus

Enable Modbus Access	☐
Modbus Address	

Main Circuit

Circuit Rating	❸	200	A
Phase CT		☑ 60	A
Neutral CT	❹	☑ 200	A
Earth CT		☑ 200	A

✖ Ca... ❺   ✔ OK

Configure Panel Mains Circuit

①   Enter a name.

     Select the circuit type:

②
- Single Phase
- Split Phase
- 3-phase

③   Enter the number of circuit positions in the panel.

     Select the panel layout: one or two columns.

     Select the circuit position numbering style: sequential or odd/even.

④   Enter the current rating (circuit breaker rating) of the circuit.

⑤   Select the checkbox for each CT installed.

     Enter the CT rating. Ratings are marked on the CT.

⑥   Click OK.

Configuration Panel 1

Settings

Name	❶	Panel Mains 1
Type	❷	3-Phase

Panel Layout

Number of Circuit Positions		96
Panel Layout	❸	Two Columns
Circuit Position Numbering		Odd/Even

Modbus

Enable Modbus Access	☐
Modbus Address	

Main Circuit

Circuit Rating	❹	250	A
Phase CT		☑ 60	A
Neutral CT	❺	☑ 60	A
Earth CT		☑ 60	A

❻   ✖ Cancel   ✔ OK

Raritan.
A brand of legrand

Configure Panel Branch Circuits

(1) In the Power Meters page, click the panel.

The Panel details page opens.
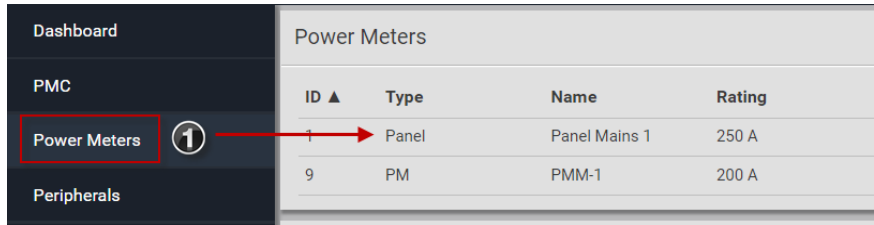
(2) In the Panel Branch Circuits section, click the circuit position to open the pop-up menu.

(3) Click Create Circuit. The Create Circuit dialog opens.
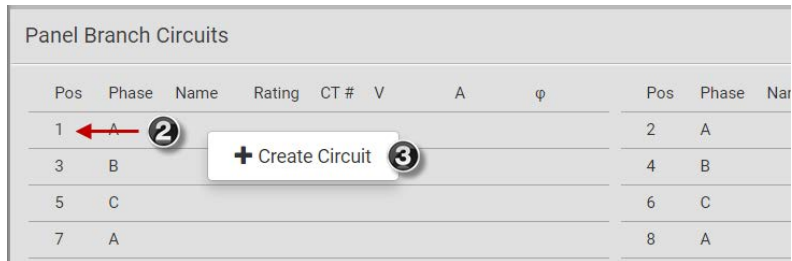
(5) Enter a name for the circuit.

(6) Select the circuit type: One-Phase LN, One-Phase LL, One-Phase LLN, or Three-Phase. Circuit type cannot be changed later.

(7) Enter the current rating of the circuit in Amps.

(8) Enter the rating of the CT connected at this circuit position in Amps.
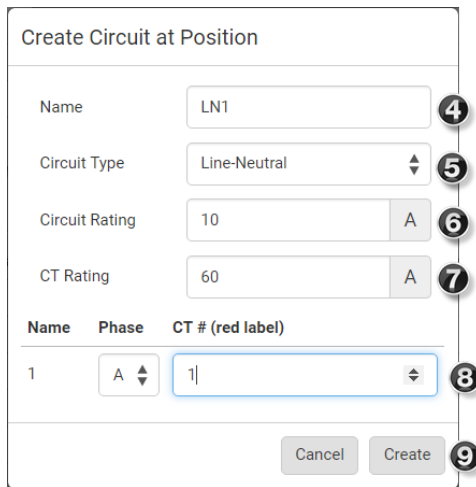
9   Click the Phase or CT# to edit the automatic labels.

10   Click Create.

Circuits appear in the list with a black bracket around the circuit positions.

Panel Branch Circuits					
Pos	Phase	Name	Rating	CT #	V
1	A	Rack 1	20 A	1	0.0 V
3	B			3	
5	C			5	
7	A	Rack 3	20 A	7	0.0 V
9	B			9	
11	C			11	

Raritan.
A brand of legrand

Using the BCM2's Display

▶ **Automatic Mode:**

The BCM2 has a display with automatic and manual modes. In automatic mode, the display scrolls through readings.

```
Power Meter 9              5/8
           Active Power
            0 W
           Reactive Power
            0 var
           Active Energy
            0 Wh
         8:36 AM          Menu ⊙
```

▶ **Manual Mode:**

In manual mode, you can select readings and settings to view.

Press ⊙ or ⊗ to view the Main Menu.

To return to automatic mode, press ⊗ once or several times.

Press ▲ ▼ to choose a menu item.

Press ⊙ to select.

```
          Main Menu
           Alerts
        Power Meters
         Peripherals
         Device Info



 ✖ Back      8:36 AM      Select ⊙
```
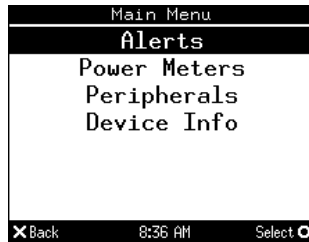
▶ **Power Meters list**

```
            Power Meters
Panel 1 (32 A)                0  V
96 circuit positions
0 circuits                  0.0  A
My Little Panel               0  W

Power Meter 9 (20 A)          0  V
My Standalone Meter
                            0.0  A
                              0  W
 ✖ Back      8:36 AM      Details ⊙
```

▶ **Power Meter details**

```
Power Meter 9              1/5

Name:     My Standalone Meter

Rating:   20 A

Phase CT: 60 A

Neutral CT: not present

Earth CT:  not present

 ✖ Back      8:37 AM
```
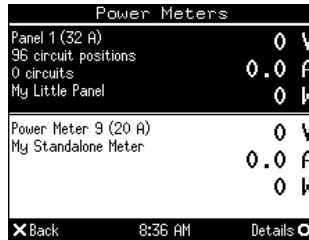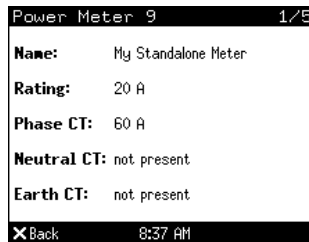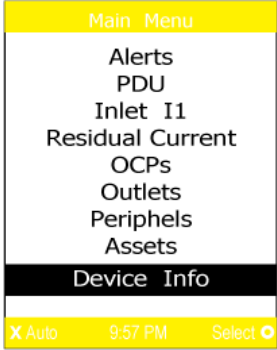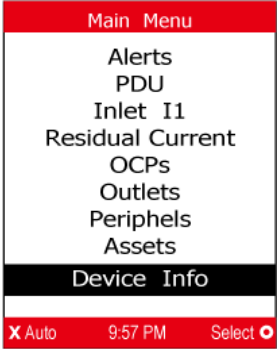
Operating the Dot-Matrix LCD Display

Enter manual mode when you want to operate the dot-matrix LCD display. You can use the dot-matrix LCD display to:

- Show information of the PDU, built-in components, or connected peripheral devices
- Control outlets if your model supports outlet-switching
- Control actuators if any

▶ **Color changes of the display's top and bottom bars:**

- In the manual mode, both the top and bottom bars will turn yellow or red to indicate the presence of any alert. For color definitions, see *Yellow- or Red-Highlighted Sensors* (see "*The Yellow- or Red-Highlighted Sensors*" on page 66, on page 95).

Screen with yellow bars	Screen with red bars
All alerts enter the warning level only. 	Partial or all alerts enter the critical level.

- Both bars turn black when there are NO alerts.

Screen with black bars

```
              Main  Menu
               Alerts
                PDU
               Inlet  I1
          Residual Current
                OCPs
               Outlets
              Periphels
               Assets
             Device  Info
  X Auto       9:57 PM      Select ●
```
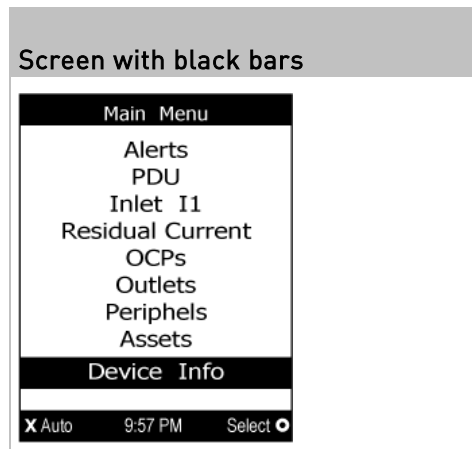
Alerts

The "Alerts" menu command shows a list of the following alerted sensors, including both internal and external sensors.

- Any numeric sensor that enters the warning or critical range if the thresholds have been enabled
- State sensors that enter the alarmed state
- Any tripped circuit breakers or blown fuses

Tip: The same information is available in the web interface's Dashboard. See **Dashboard - Alerted Sensors** *(on page 69).*

If there are no alerted sensors, the LCD display shows the message "No Alerts."

▶ **To view alerted sensors:**

1. Press ⬆/⌃ or ⬇/⌄ to select "Alerts" in the Main Menu, and press ●/○.

2. Alerted sensors, if any, are highlighted in either red or yellow. For color definitions, see *Yellow- or Red-Highlighted Sensors* (see "*The Yellow- or Red-Highlighted Sensors*" on page 66, on page 95).

▪ The top and bottom bars on the LCD display may be yellow or red, depending on the type(s) of available alerts. See *Operating the Dot-Matrix LCD Display* (on page 14).

Number	Description
➊	Sensor names.
➋	Sensor readings and/or states.
	A numeric sensor shows both the reading and state. A state sensor or actuator shows the state only.
	Available states are listed below. For further information, see *Sensor/Actuator States* (on page 97).
	▪ Alarmed
	▪ Lower Critical = below lower critical
	▪ Lower Warning = below lower warning
	▪ Upper Warning = above upper warning
	▪ Upper Critical = above upper critical
	▪ Open (for overcurrent protectors)

3. Press ⊙/⌃ or ⊙/⌄ to view additional pages. When there are multiple pages, page numbers appear in the top-right corner of the display.

Power Meters

The Power Meters menu option displays information and readings for each power meter. Use the arrow buttons to navigate through all power meters.

From all Power Meters pages, **X** (BACK) displays the Main Menu
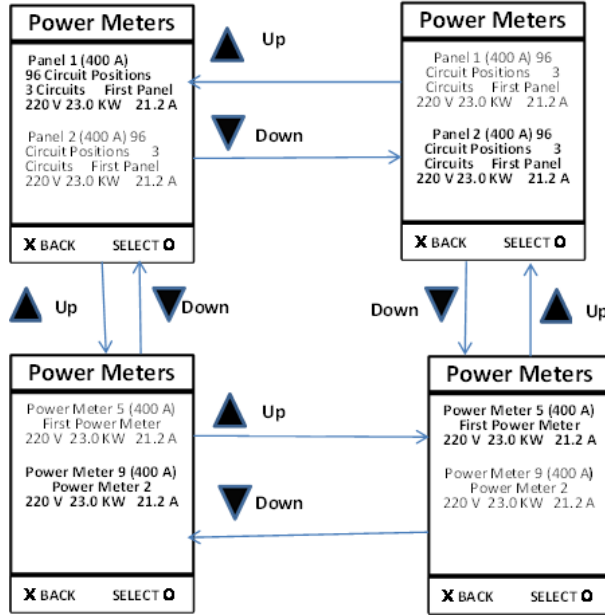
Panels

Navigate to a panel from the power meter details and press O (select) to display the panel details and readings.

From all Panel Details pages, **X** (BACK) displays Power Meters screen

Power Meters

Panel 1 (400 A)
96 Circuit Positions
3 Circuits   First Panel
220 V 23.0 KW   21.2 A

Panel 2 (400 A) 96
Circuit Positions   3
Circuits   First Panel
220 V 23.0 KW   21.2 A

X BACK   SELECT **O**

O (SELECT)

X (BACK)

Panel 1

Name: First Panel
Circuit Positions: 48
Layout: 2 columns
Numbering: odd/even
Breaker rating: 400 A
Meter Board: 2
Mains CT: 60 A
Neutral CT: not present
P.E. CT: not present

X BACK   SELECT **O**

Down   Up

X (BACK)   O (SELECT)

Panel 1

C: 20.1 A

C-A: 207 V

B-C: 208 V

C-N: 207 V

X BACK   SELECT **O**

Down   Up

Panel 1

4.29 KW

0.19 kvar

34720 Wh

X BACK   SELECT **O**

Down   Up

Panel 1

B: 12.9 A

B-C: 208 V

A-B: 206 V

B-N: 208 V

X BACK   SELECT **O**

Up

Down

Panel 1

A: 17.3 A

A-B: 206 V

C-A: 207 V

A-N: 206 V

X BACK   SELECT **O**

Raritan.
A brand of ☐legrand

Branch Circuits

Navigate to a branch circuit from the panel details and press O (select) to display the branch circuit details and readings.

From all Branch Circuits pages, **X** (BACK) displays the Panel Details page
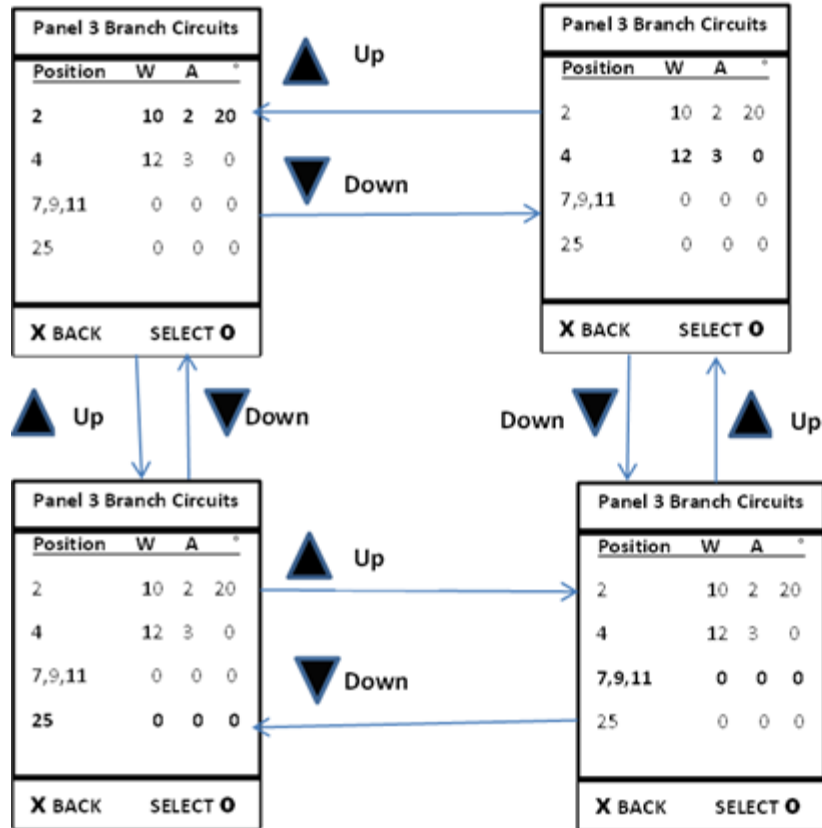
Branch Circuit Details

From all Branch Details pages, **X** (BACK) displays Panel Branch Circuits screen

Panel 3 Branch Circuits

Position	W	A	°
2	10	2	20
4	12	3	0
7,9,11	**0**	**0**	**0**
25	0	0	0

X BACK   DETAILS **O**

O (SELECT)

X (BACK)

Panel 3 Circuits 7,9,11 Details

Name: 3PC 14
Type: Three Phase
Circuit Rating: 30 A
CT Rating: 60 A
Positions: 7,9,11
CTs: 7,9,11
Phases: A,B,C

X BACK

O (SELECT)

X (BACK)

Down ▼   ▲ Up

Panel 3 Circuits 7,9,11 Details

Phase C (11) Sensors (CT 11)
Current: 20A
Phase Angle: 0
Active Power: 2 W
Reactive Power: 3 var
Apparent Power: 3 VA
Power factor: 0.67
Displacement Power Factor:
Active Energy: 2 Kwh

X BACK

Panel 3 Circuits 7,9,11 Details

Circuit Sensors

Current: 20A

Active Power: 5 W

Reactive Power: 3 var

Active Energy: 5 Wh

X BACK

Down ▼   ▲ Up

Down ▼   ▲ Up

Panel 3 Circuits 7,9,11 Details

Phase B (9) Sensors (CT 9)
Current: 20A
Phase Angle: 0
Active Power: 2 W
Reactive Power: 3 var
Apparent Power: 3 VA
Power factor: 0.67
Displacement Power Factor:
Active Energy: 2 Kwh

X BACK

▲ Up

Down ▼

Panel 3 Circuits 7,9,11 Details

Phase A (7) Sensors (CT 8)
Current: 20A
Phase Angle: 0
Active Power: 2 W
Reactive Power: 3 var
Apparent Power: 3 VA
Power factor: 0.67
Displacement Power Factor:
Active Energy: 2 Kwh

X BACK

Raritan
A brand of ☐legrand

Peripherals

If there are no Raritan environmental sensor packages connected to your BCM2, the LCD display shows the message "No managed devices" for the "Peripherals" menu command.

If you have enabled the front panel actuator control function, you can switch on or off a connected actuator using the LCD display. See *Miscellaneous* (on page 250).

▶ **To show environmental sensor or actuator information:**

1. Press ⒜/⌃ or ⒱/⌄ to select "Peripherals" in the Main Menu, and press ⦿/◯.

2. The display shows a list of environmental sensors/actuators similar to the following diagram.

   - If the desired sensor or actuator is not visible, press ⒜/⌃ or ⒱/⌄ to scroll up or down.

   - When the list exceeds one page, the currently-selected sensor/actuator's ID number and total of managed sensors/actuators are indicated in the top-right corner of the display.

   - If any sensor enters the warning, critical, or alarmed state, like 'Tamper Detector 1' shown below, it is highlighted in yellow or red. For color definitions, see *Yellow- or Red-Highlighted Sensors* (see "*The Yellow- or Red-Highlighted Sensors*" on page 66, on page 95).

The top and bottom bars also turn yellow or red. See *Operating the Dot-Matrix LCD Display* (on page 14).

Number	Description
❶	Sensor or actuator names.
❷	Sensor or actuator states as listed below. For further information, see *Sensor/Actuator States* (on page 97). ▪ n/a = unavailable ▪ Normal ▪ Alarmed ▪ Lower Critical = below lower critical ▪ Lower Warning = below lower warning ▪ Upper Warning = above upper warning ▪ Upper Critical = above upper critical ▪ On ▪ Off A numeric sensor shows both the reading and state. A state sensor or actuator shows the state only.

3. To view an environmental sensor or actuator's detailed information, press ⏶/⌃ or ⏷/⌄ to select that sensor or actuator, and press ⏺/◉. A screen similar to the following is shown.

Number	Description
❸	The ID number assigned to this sensor or actuator. ▪ A sensor shows "Peripheral Sensor x" (x is the ID number) ▪ An actuator shows "Peripheral Actuator x"
❹	Sensor or actuator name.
❺	The following information is listed. ▪ Serial number ▪ Chain position, which involves the following information: Port <N>: <N> is the number of the sensor port where this sensor or actuator is connected. This number is always 1 for BCM2. Chain Pos. <n>: <n> is the sensor or actuator's position in a sensor daisy chain. *Note: Only DX, DPX2 and DPX3 sensor packages provide the chain position information.* ▪ If this sensor or actuator is on a sensor package with multiple channels, such as DX-D2C6, its channel number is indicated as "Channel x", where x is a number.

Number	Description
❻	Depending on the sensor type, any of the following information is displayed: ▪ State of a state sensor: Normal or Alarmed. ▪ State of an actuator: On or Off. ▪ Reading of a numeric sensor.
❼	X, Y, and Z coordinates which you specify for this sensor or actuator. See *Individual Sensor/Actuator Pages* (on page 103).

▶ **To switch on or off an actuator:**

1. Follow the above steps 1 to 3 to select an actuator.
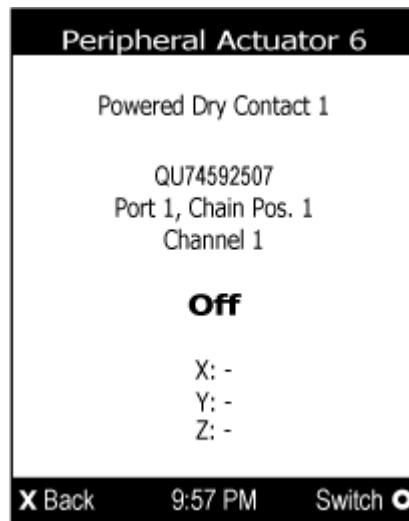
2. Press ⬤/◯ to turn on or off the actuator. A confirmation message similar to the following is shown.

Peripheral Actuator 6

Do you really want
to switch on
Powered Dry
Contact 1?

Yes

No

X Back   9:57 PM

3. Press ⬆/⌃ or ⬇/⌄ to select Yes or No, and then press ⬤/◯.

4. Verify that the actuator status shown on the LCD display has been changed.

Chapter 3 Connecting External Equipment (Optional)

More features are available if you connect Raritan's or third-party external equipment to your BCM2.

In This Chapter

Connecting Environmental Sensor Packages

The BCM2 supports all types of Raritan environmental sensor packages, including DPX, DPX2, DPX3 and DX sensor packages. For detailed information on each sensor package, refer to the Environmental Sensors Guide or Online Help on the Raritan website's *Support page* (*http://www.raritan.com/support/*).

An environmental sensor package may comprise sensors only or a combination of sensors and actuators.

The BCM2 can manage a maximum of 32 sensors and/or actuators. The supported maximum cabling distance is 98 feet (30 m), except for DPX sensor packages.

For information on connecting different types of sensor packages, see:

- *DPX Sensor Packages* (on page 27)
- *DPX2 Sensor Packages* (on page 33)
- *DPX3 Sensor Packages* (on page 35)
- *DX Sensor Packages* (on page 37)

DPX Sensor Packages

Most DPX sensor packages come with a factory-installed sensor cable, whose sensor connector is RJ-12.
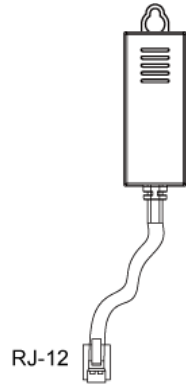
For the cabling length restrictions, see *Supported Maximum DPX Sensor Distances* (on page 32).

> Warning: For proper operation, wait for 15-30 seconds between each connection operation or each disconnection operation of environmental sensor packages.

► **To connect a DPX sensor package with a factory-installed sensor cable:**

• Plug the sensor cable's RJ-12 connector into the RJ-12 SENSOR port on the BCM2.

► **To connect a DPX differential air pressure sensor:**

1. Plug one end of a Raritan-provided phone cable into the IN port of a differential air pressure sensor.

2. Plug the other end of this phone cable into the RJ-12 SENSOR port on the BCM2.

3. If intended, connect one DPX sensor package to the OUT port of the differential air pressure sensor. It can be any DPX sensor package, such as a DPX-T3H1.
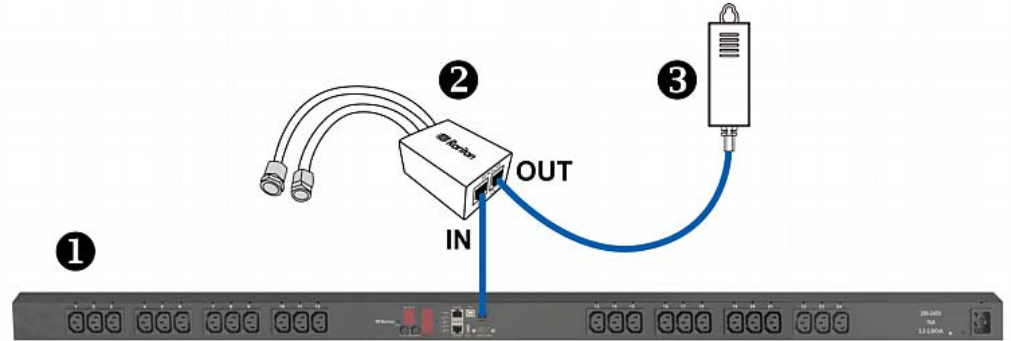
❶	The BCM2 device
❷	Raritan differential air pressure sensors
❸	One DPX sensor package (optional)

Using an Optional DPX-ENVHUB4 Sensor Hub

Optionally, you can connect a Raritan *DPX-ENVHUB4* sensor hub to the BCM2. This allows you to connect up to four DPX sensor packages to the BCM2 via the hub.

This sensor hub supports DPX sensor packages only. Do NOT connect DPX2, DPX3 or DX sensor packages to it.

DPX-ENVHUB4 sensor hubs CANNOT be cascaded. You can connect only one hub to each SENSOR port on the BCM2.

Tip: The Raritan sensor hub that supports ALL types of Raritan environmental sensor packages is DPX3-ENVHUB4. See **Using an Optional DPX3-ENVHUB4 Sensor Hub** *(on page 40).*

▶ **To connect DPX sensor packages via the DPX-ENVHUB4 hub:**

1. Connect the DPX-ENVHUB4 sensor hub to the BCM2.

   a. Plug one end of the Raritan-provided phone cable (4-wire, 6-pin, RJ-12) into the IN port (Port 1) of the hub.

   b. Plug the other end of the cable into the RJ-12 SENSOR port of the BCM2.

2. Connect DPX sensor packages to any of the four OUT ports on the hub.

This diagram illustrates a configuration with a sensor hub connected.
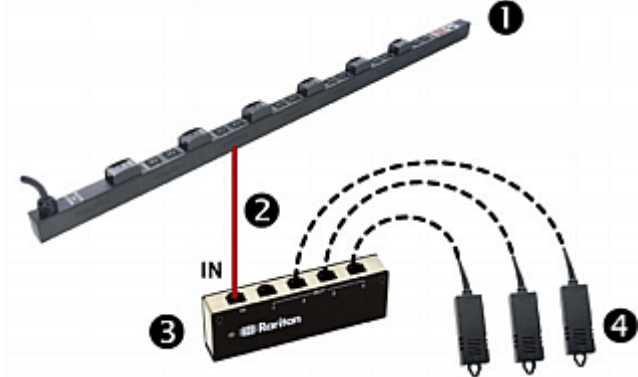
❶	The BCM2 device
❷	Raritan-provided phone cable
❸	DPX-ENVHUB4 sensor hub
❹	DPX sensor packages

Using an Optional DPX-ENVHUB2 cable

A Raritan *DPX-ENVHUB2* cable doubles the number of connected environmental sensors per SENSOR port.

This cable supports DPX sensor packages only. Do NOT connect DPX2, DPX3 or DX sensor packages to it.

▶ **To connect DPX sensor packages via the DPX-ENVHUB2 cable:**

1. Plug the connector of this cable directly into the BCM2 device's RJ-12 SENSOR port.
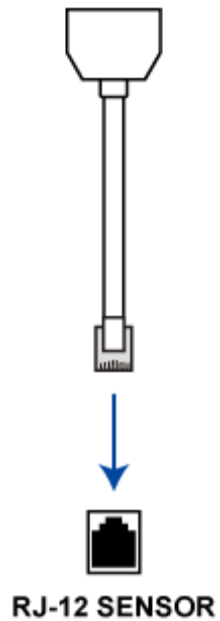
RJ-12 SENSOR

2. The cable has two RJ-12 sensor ports. Connect DPX sensor
    packages to the cable's sensor ports.
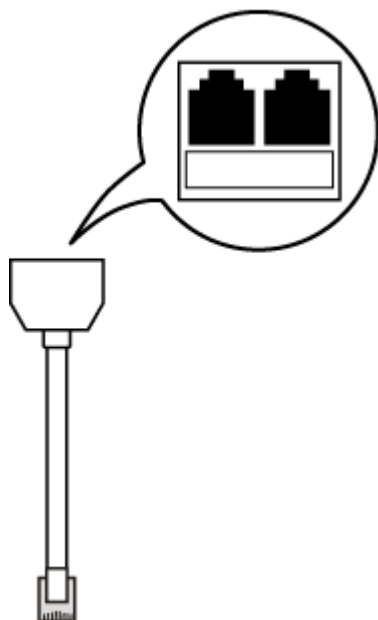
3. Repeat the above steps if there are additional SENSOR ports on your
    BCM2.

Supported Maximum DPX Sensor Distances

When connecting the following DPX sensor packages to the BCM2, you must follow two restrictions.

- DPX-CC2-TR
- DPX-T1
- DPX-T3H1
- DPX-AF1
- DPX-T1DP1

▶ **Sensor connection restrictions:**

- Connect a DPX sensor package to the BCM2 using the sensor cable pre-installed (or provided) by Raritan. You MUST NOT extend or modify the sensor cable's length by using any tool other than the Raritan's sensor hubs.
- If using a DPX-ENVHUB4 sensor hub, the cabling distance between the BCM2 and the sensor hub is up to 33' (10 m).

▶ **Maximum distance illustration:**

The following illustrates the maximum distance when connecting DPX sensor packages with a maximum 16' (5 m) sensor cable to a BCM2 via a sensor hub.

- The sum of a DPX-T3H1 sensor cable's length is 16' (5 m).

3 m   1 m   1 m

3 m + 1 m + 1 m = 5 m
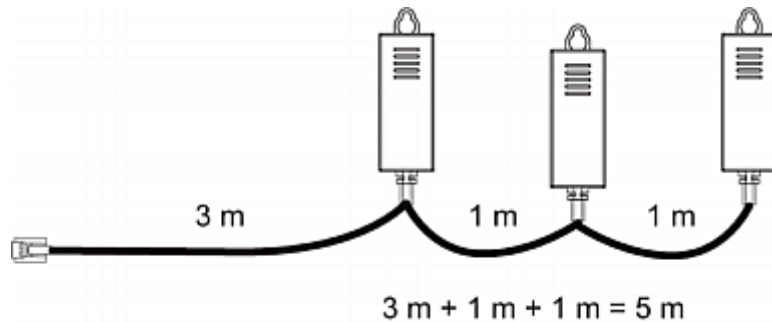
- The total cabling length between the BCM2 and one DPX-T3H1 is 49' (15 m) as illustrated below.

  Note that the length 16' (5 m) is the length of each DPX-T3H1 sensor cable, which is defined in the above diagram.

BCM2	→	33' (10 m) cable	→	1 sensor hub	→	16' (5 m) cable	→	Up to 4 DPX-T3H1 sensor packages

DPX2 Sensor Packages

A DPX2 sensor cable is shipped with a DPX2 sensor package. This cable is made up of one RJ-12 connector and one to three head connectors. You have to connect DPX2 sensor packages to the sensor cable.

For more information on DPX2 sensor packages, access the Environmental Sensors Guide or Online Help on Raritan website's *Support page* (*http://www.raritan.com/support/*).
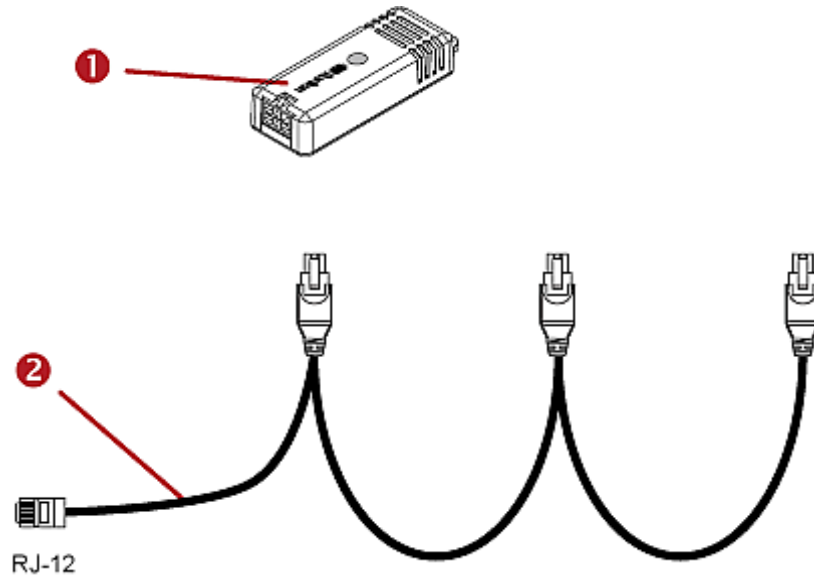
Item	
❶	DPX2 sensor package
❷	DPX2 sensor cable with one RJ-12 connector and three head connectors

The following procedure illustrates a DPX2 sensor cable with three head connectors. Your sensor cable may have fewer head connectors.

Warning: If there are free head connectors between a DPX2 sensor cable's RJ-12 connector and the final attached DPX2 sensor package, the sensor packages following the free head connector(s) on the same cable do NOT work properly. Therefore, always occupy all head connectors prior to the final sensor package with a DPX2 sensor package.

▶ **To connect DPX2 sensor packages to the BCM2:**

1. Connect a DPX2 sensor package to the first head connector of the DPX2 sensor cable.
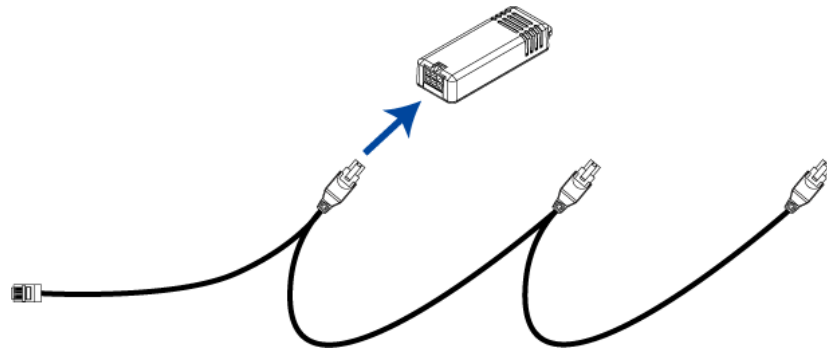
2. Connect remaining DPX2 sensor packages to the second and then the third head connector.
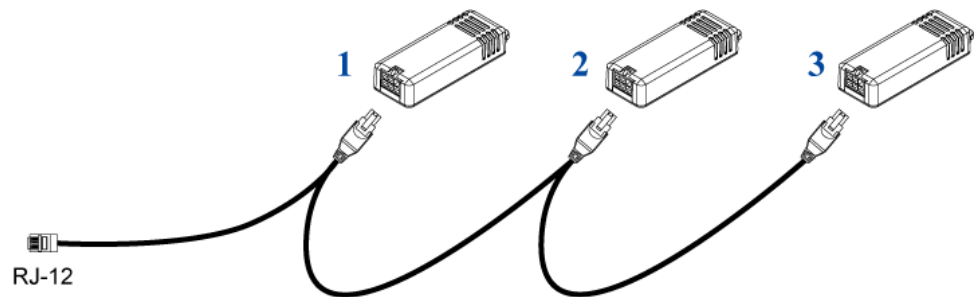
Tip: If the number of sensors you are connecting is less than the number of head connectors on your sensor cable, connect them to the first one or first two head connectors to ensure that there are NO free head connectors prior to the final DPX2 sensor package attached.

3. Plug the RJ-12 connector of the DPX2 sensor cable into the RJ-12 SENSOR port on the BCM2.

OR you can directly connect the DPX2 sensor package to a DX sensor chain without using any RJ-12 to RJ-45 adapter. See *Connecting a DPX2 Sensor Package to DX* (on page 39).

Note: If your BCM2 has "two" RJ-12 SENSOR ports, see Guidelines for BCM2 with Two Sensor Ports for sensor connection restrictions.

DPX3 Sensor Packages

A DPX3 sensor package features the following:

- Its connection interface is RJ-45.
- You can cascade a maximum of 12 DPX3 sensor packages.
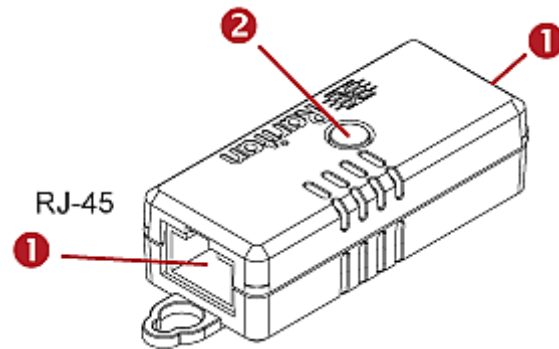
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DPX3 sensor package.
❷	LED for indicating the sensor status.

▶ **To connect DPX3 sensor packages to the BCM2:**

1. Connect an RJ-12 to RJ-45 adapter cable to the DPX3 sensor package.
   - Connect the adapter's RJ-45 connector to either RJ-45 port of the DPX3 sensor package.
2. If you want to cascade DPX3 sensor packages, get an additional standard network patch cable (CAT5e or higher) and then:
   a. Plug one end of the cable into the remaining RJ-45 port on the prior DPX3.
   b. Plug the other end into either RJ-45 port on an additional DPX3.

Repeat the same steps to cascade more DPX3 sensor packages.
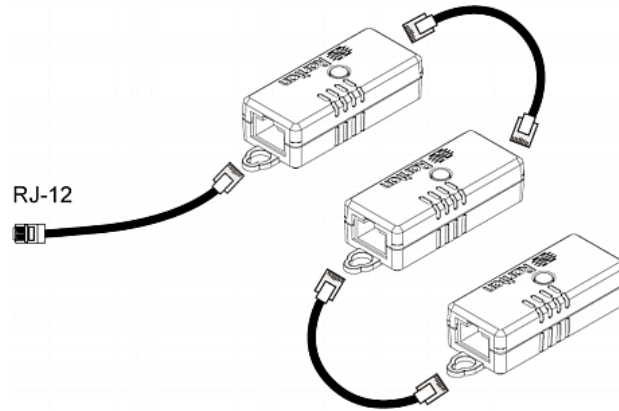
3. Connect the first DPX3 sensor package to the BCM2.
    ▪ Plug the adapter cable's RJ-12 connector into the RJ-12 SENSOR port on the BCM2.

Connecting a DPX2 Sensor Package to DPX3

You can connect only one DPX2 sensor package to the "end" of a DPX3 sensor chain. It is strongly recommended to use an RJ-12 to RJ-45 adapter for connecting the DPX2 to the final DPX3 in the chain.

The maximum number of DPX3 sensor packages in the chain must be less than 12 when a DPX2 sensor package is involved.

▶ **When connecting a DPX2 sensor package containing three DPX2 sensors:**

A maximum of nine DPX3 sensor packages can be cascaded because 12-3=9.
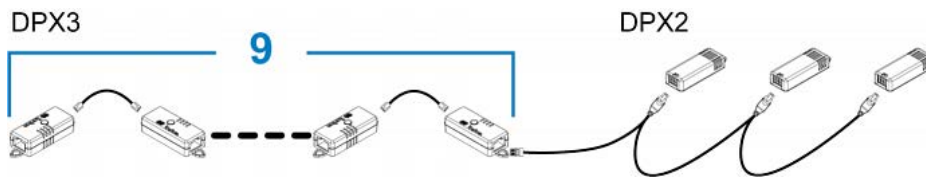
▶ **When connecting a DPX2 sensor package containing two DPX2 sensors:**

A maximum of ten DPX3 sensor packages can be cascaded because 12-2=10.
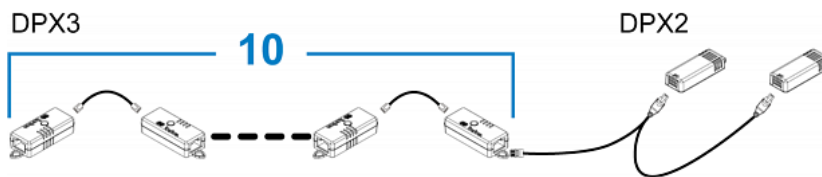
▶ **When connecting a DPX2 sensor package containing one DPX2 sensor:**

A maximum of eleven DPX3 sensor packages can be cascaded because 12-1=11.
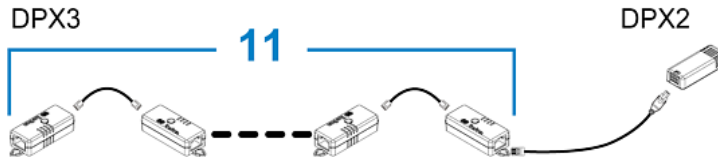
DX Sensor Packages

Most DX sensor packages contain terminals for connecting detectors or actuators. For information on connecting actuators or detectors to DX terminals, refer to the Environmental Sensors Guide or Online Help on Raritan website's *Support page* (*http://www.raritan.com/support/*).

You can cascade up to 12 DX sensor packages.

When cascading DX, remember that the BCM2 only supports a maximum of 32 sensors and/or actuators.

If there are more than 32 sensors and/or actuators connected, every sensor and/or actuator after the 32nd one is NOT managed by the BCM2.

For example, if you cascade 12 DX packages, and each package contains 3 functions (a function is a sensor or actuator), the BCM2 does NOT manage the last 4 functions because the total 36 (12*3=36) exceeds 32 by 4.

Tip: To manage the last 4 functions, you can release 4 "managed" sensors or actuators, and then manually bring the last 4 functions into management. See **Peripherals** *(on page 90).*
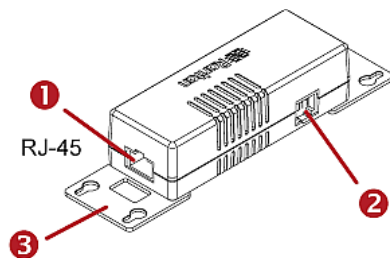
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DX sensor package.
❷	RJ-12 port, which is reserved for future use and now blocked.

Numbers	Components
❸	Removable rackmount brackets.

▶ **Connect DX to the BCM2:**

1. Connect an RJ-12 to RJ-45 adapter cable which is shipped with a DX sensor package to the DX.

   ▪ Connect the adapter's RJ-45 connector to either RJ-45 port of the DX.

2. If you want to cascade DX packages, get an additional standard network patch cable (CAT5e or higher) and then:

   a. Plug one end of the cable into the remaining RJ-45 port on the prior DX package.

   b. Plug the other end into either RJ-45 port on an additional DX package.

   Repeat the same steps to cascade more DX packages.
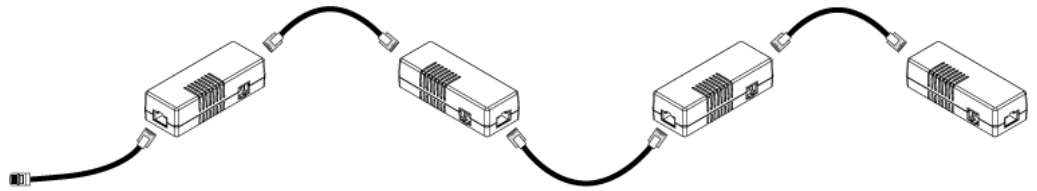
RJ-12

3. Connect the first DX sensor package to the BCM2.

   ▪ Plug the adapter cable's RJ-12 connector into the RJ-12 SENSOR port of the BCM2.

4. If needed, connect a DPX2 sensor package to the end of the DX chain. See *Connecting a DPX2 Sensor Package to DX* (on page 39).

Note: If your BCM2 has "two" RJ-12 SENSOR ports, see Guidelines for BCM2 with Two Sensor Ports for sensor connection restrictions.

Connecting a DPX2 Sensor Package to DX

You can connect only one DPX2 sensor package to the "end" of a DX sensor chain. It is strongly recommended to use an RJ-12 to RJ-45 adapter for connecting the DPX2 to the final DX in the chain.

The maximum number of DX sensor packages in the chain must be less than 12 when a DPX2 sensor package is involved.

▶ **When connecting a DPX2 sensor package containing three DPX2 sensors:**

A maximum of nine DX sensor packages can be cascaded because 12-3=9.
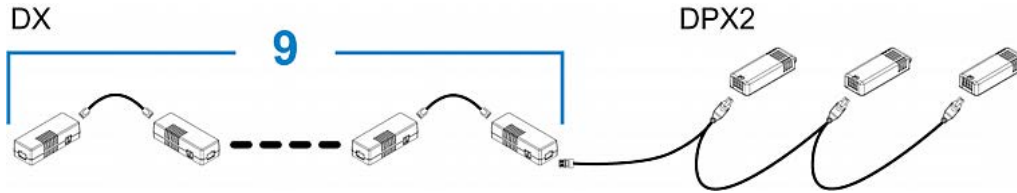
▶ **When connecting a DPX2 sensor package containing two DPX2 sensors:**

A maximum of ten DX sensor packages can be cascaded because 12-2=10.
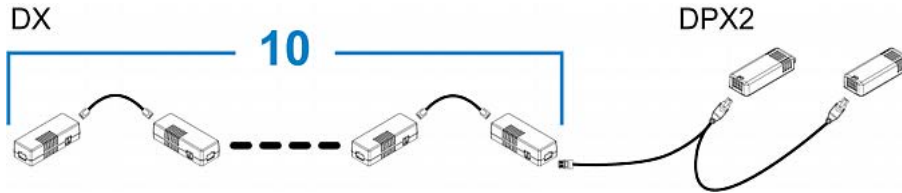
▶ **When connecting a DPX2 sensor package containing one DPX2 sensor:**

A maximum of eleven DX sensor packages can be cascaded because 12-1=11.
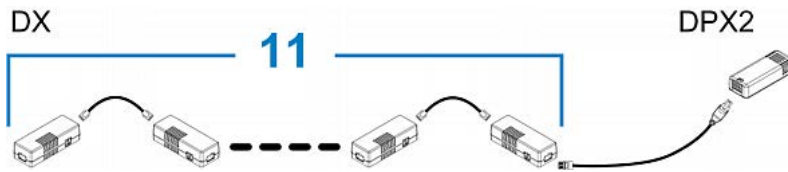
Using an Optional DPX3-ENVHUB4 Sensor Hub

A Raritan DPX3-ENVHUB4 sensor hub is physically and functionally similar to the DPX-ENVHUB4 sensor hub, which increases the number of sensor ports for the BCM2, except for the following differences:

- All ports on the DPX3-ENVHUB4 sensor hub are RJ-45 instead of RJ-12 as the DPX-ENVHUB4 sensor hub.
- The DPX3-ENVHUB4 sensor hub supports all Raritan environmental sensor packages, including DPX, DPX2, DPX3 and DX sensor packages.

To connect diverse types of sensor packages to this sensor hub, you must follow the combinations shown in the section titled *Mixing Diverse Sensor Types* (on page 41).

▶ **To connect DPX3 sensor packages via the DPX3-ENVHUB4 hub:**

1. Connect the DPX3-ENVHUB4 sensor hub to the BCM2 using an RJ-12 to RJ-45 adapter cable.

   a. Plug the RJ-45 connector of this cable into the IN port (Port 1) of the hub.

   b. Plug the RJ-12 connector of this cable into the RJ-12 SENSOR port of the BCM2.

2. Connect the Raritan sensor packages to any of the four OUT ports on the hub.

   - An RJ-12 to RJ-45 adapter is required for connecting a DPX or DPX2 sensor package to the hub.

   This diagram illustrates a configuration with a sensor hub connected.
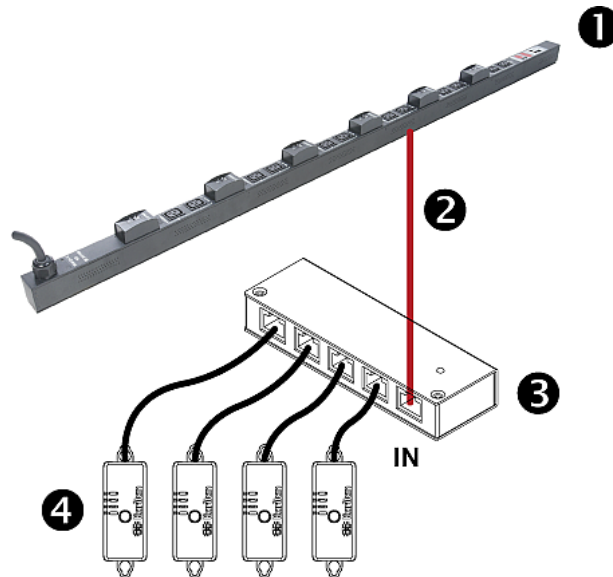
❶	The BCM2
❷	RJ-12 to RJ-45 adapter cable
❸	DPX3-ENVHUB4 sensor hub
❹	Any Raritan sensor packages

Mixing Diverse Sensor Types

You can mix DPX, DPX2, DPX3 and DX sensor packages on one BCM2 according to the following sensor combinations. In some scenarios, the DPX3-ENVHUB4 sensor hub is required.

The BCM2 does NOT support any other sensor-mixing combinations than those described in this section.

When mixing different sensor types, remember that the BCM2 supports a maximum of 32 sensors/actuators.

▶ **1 DX + 1 DPX:**

- An RJ-12 to RJ-45 adapter cable is required for connecting the DX sensor package to the BCM2.
- It is strongly recommended to use an RJ-12 to RJ-45 adapter to connect the DPX sensor package to the DX sensor package.
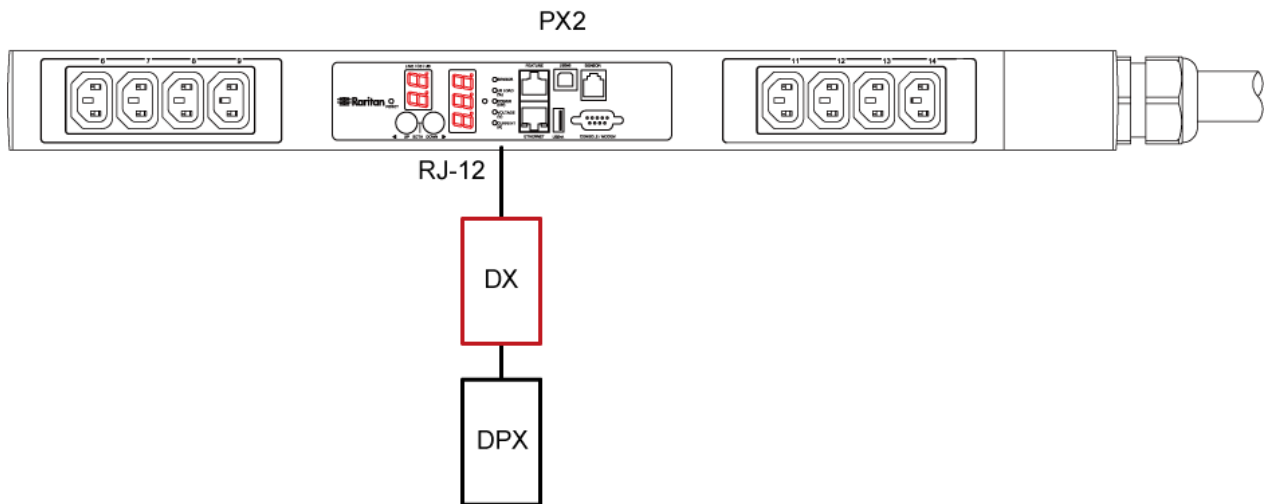
▶ **Diverse combinations via the DPX3-ENVHUB4 sensor hub:**

- You must use the **DPX3**-ENVHUB4 sensor hub instead of the old DPX-ENVHUB4 sensor hub. Each port on the hub supports any of the following:
  - A DX sensor package

- A chain of DX sensor packages
- A DPX3 sensor package
- A chain of DPX3 sensor packages
- A DPX2 sensor package
- A DPX sensor package

- An RJ-12 to RJ-45 adapter is recommended to connect a DPX or DPX2 sensor package to DPX3-ENVHUB4.
- In the following diagrams, the sensor package in "green" can be replaced by a DPX2 sensor package. The sensor package in "blue" can be one DPX2, DPX3 or DX sensor package.
- An RJ-12 to RJ-45 adapter cable MUST be used for connecting the DPX3-ENVHUB4 to the BCM2.

This section only illustrations the following three combinations, but actually there are tens of different combinations by using the DPX3-ENVHUB4 sensor hub.
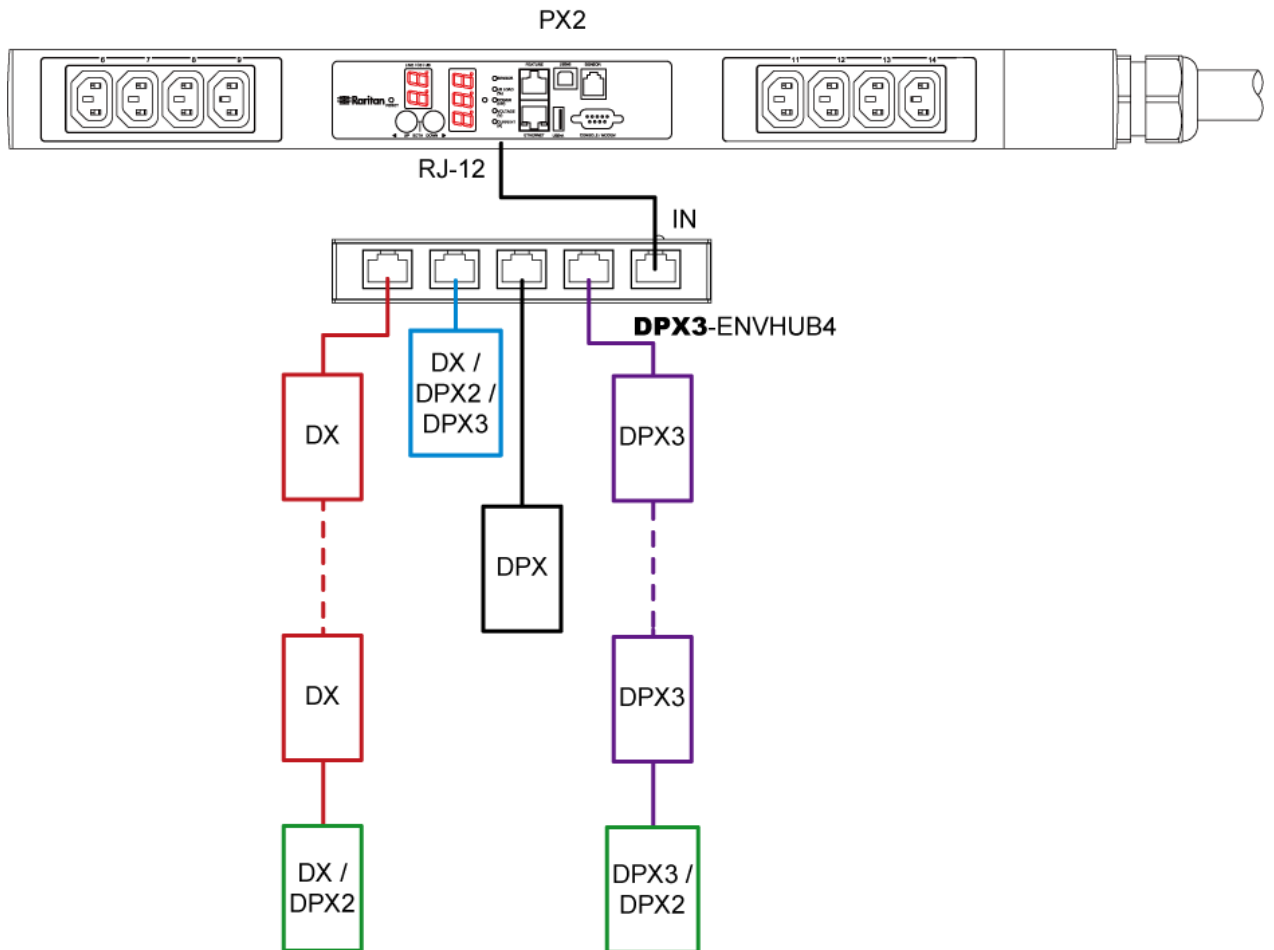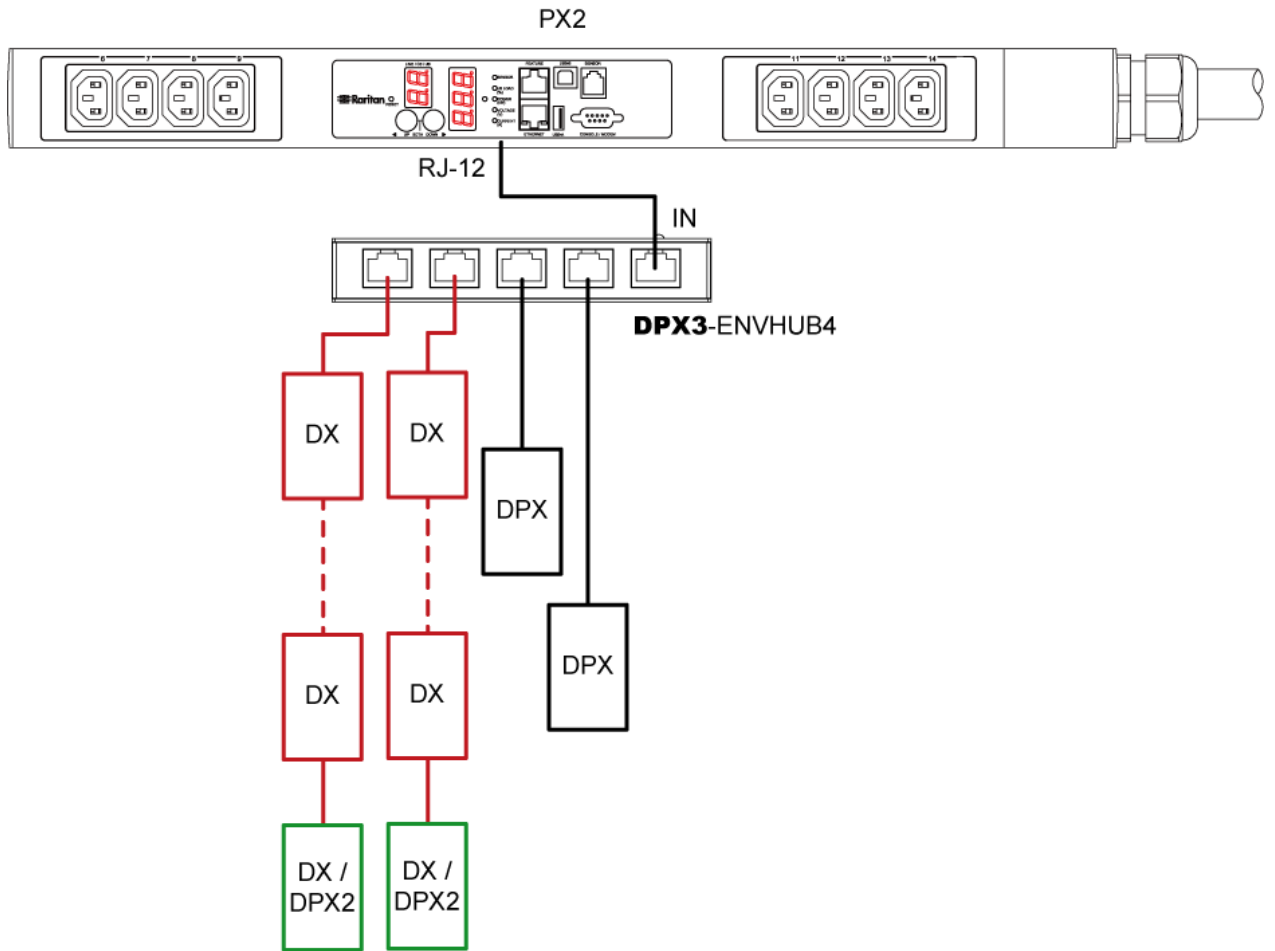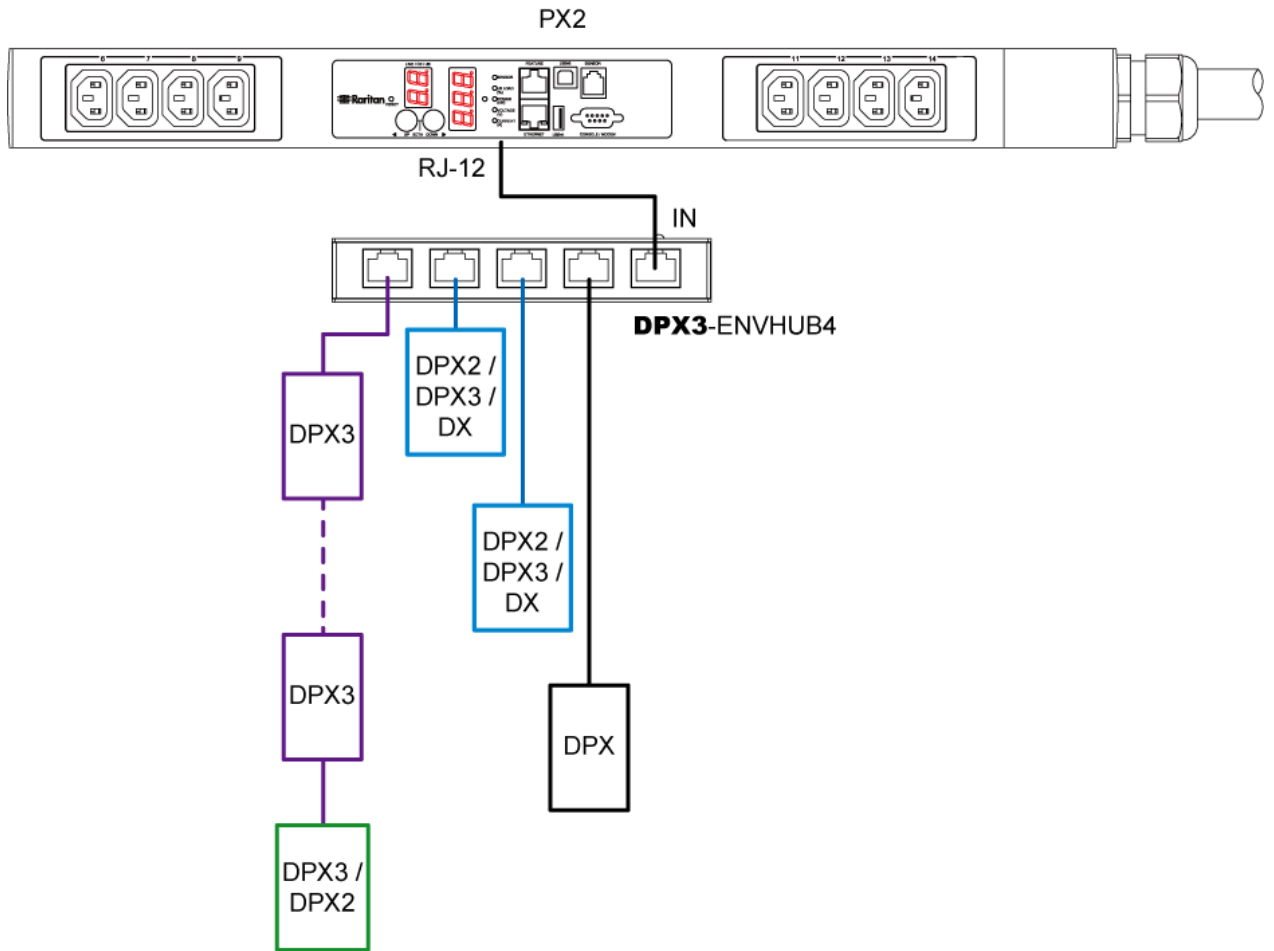
▶ **Mix DPX3 and DX in a sensor chain:**

Any DX sensor package in a chain can be replaced by a DPX3 sensor package, or vice versa. The total number of sensor packages in this chain cannot exceed 12.

For example, the following diagram shows a sensor chain comprising both DX and DPX3 sensor packages.

You can add a DPX2 sensor package to the end of such a sensor-mixing chain if intended. See *Connecting a DPX2 Sensor Package to DPX3* (on page 36) or *Connecting a DPX2 Sensor Package to DX* (on page 39).

Connecting Asset Management Sensors

> Note that only the PMC models of the BCM2 series have the FEATURE port. Therefore, only PMC models support the asset management feature.

You can remotely track the locations of up to 64 IT devices in the rack by connecting asset management strips (asset strips) to the BCM2 after IT devices are tagged electronically.

To use the asset management feature, you need the following items:

- *Raritan asset strips*: An asset strip transmits the asset management tag's ID and positioning information to the BCM2.
- *Raritan asset tags*: An asset management tag (asset tag) is adhered to an IT device. The asset tag uses an electronic ID to identify and locate the IT device.

Combining Regular Asset Strips

Each tag port on the regular asset strips corresponds to a rack unit and can be used to locate IT devices in a specific rack (or cabinet).

For each rack, you can attach asset strips up to 64U long, consisting of one MASTER and multiple SLAVE asset strips.

The difference between the master and slave asset strips is that the master asset strip has an RJ-45 connector while the slave does not.

The following diagram illustrates some asset strips. Note that Raritan provides more types of asset strips than the diagram.
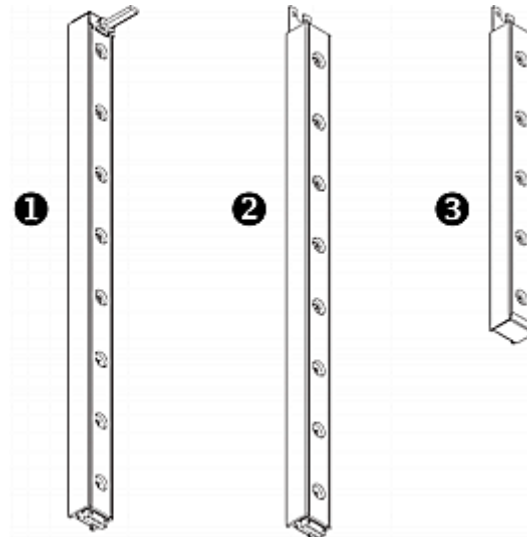
❶	8U MASTER asset strip with 8 tag ports
❷	8U SLAVE asset strip with 8 tag ports
❸	5U "ending" SLAVE asset strip with 5 tag ports

Note: Unlike general slave asset strips, which have one DIN connector respectively on either end, the ending slave asset strip has one DIN connector on only one end. An ending asset strip is installed at the end of the asset strip assembly.

▶ **To assemble asset strips:**

1. Connect a MASTER asset strip to an 8U SLAVE asset strip.
   - Plug the white male DIN connector of the slave strip into the white female DIN connector of the master strip.
   - Make sure that the U-shaped sheet metal adjacent to the male DIN connector is inserted into the rear slot of the master strip. Screw up the U-shaped sheet metal to reinforce the connection.
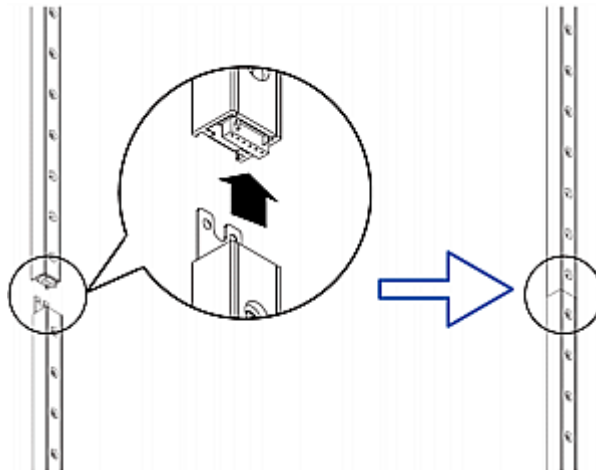
2. Connect another 8U slave strip to the one being attached to the master strip in the same manner as Step 1.

3. Repeat the above step to connect more slave strip. The length of the asset strip assembly can be up to 64U.
   - The final slave strip can be 8U or 5U, depending on the actual height of your rack.
   - Connect the "ending" asset strip as the final one in the assembly.

4. Vertically attach the asset strip assembly to the rack, next to the IT equipment, making each tag port horizontally align with a rack unit.

5. The asset strips are automatically attracted to the rack because of magnetic stripes on the back.

47

Note: The asset strip is implemented with a tilt sensor so it can be mounted upside down.

Connecting Regular Asset Sensors to the BCM2

Note that only the PMC models of the BCM2 series have the FEATURE port.

The cabling distance between an asset strip assembly and the BCM2 can be up to 10 meters.

You need both asset strips and asset tags for tracking IT devices.

Asset tags provide an ID number for each IT device. The asset tags are adhered to an IT device at one end and plugged in to an asset strip at the other.

The asset strip is connected to the BCM2, and the asset tag transmits the ID and positioning information to the asset strip.

The following diagram illustrates an asset tag. Note that there are two types of asset tags: non-programmable and programmable tags. The only difference is that programmable asset tags allow you to customize each tag's ID or barcode number while non-programmable ones have factory default ID or barcode numbers, which you cannot change.

A	Barcode (ID number), which is available on either end of the "non-programmable" asset tag
B	Tag connector
C	Adhesive area with the tape

Note: The barcode of each "non-programmable" asset tag is unique and is displayed in the BCM2 device's web interface for identification.

▶ **To connect regular asset strips to the BCM2 device:**

1. Affix the adhesive end of an asset tag to each IT device through the tag's tape.

2. Plug the connector of each asset tag into the corresponding tag port on the asset strip.

3. Connect the asset strip assembly to the BCM2 device, using a network patch cable (CAT5e or higher).

   a. Connect one end of the cable to the RJ-45 connector on the MASTER asset strip.

   b. Connect the other end of the cable to the FEATURE port on the BCM2 device.

   The BCM2 device supplies power to the connected asset strip assembly. All LEDs on the asset strip assembly may cycle through different colors during the power-on process if the asset strip's firmware is being upgraded by the BCM2. After the power-on or firmware upgrade process completes, the LEDs show solid colors. Note that the LED color of the tag ports with asset tags connected will be different from the LED color of the tag ports without asset tags connected.

Note: The BCM2 cannot detect how many rack units the connected asset sensor(s) has. You must provide the information to it manually. See Configuring the Asset Sensor.

Connecting Blade Extension Strips

For blade servers, which are contained in a single chassis, you can use a blade extension strip to track individual blade servers.

Raritan's blade extension strip functions similar to a Raritan asset strip but requires a tag connector cable for connecting it to a tag port on the regular or composite asset strip. A blade extension strip contains 4 to 16 tag ports.

The following diagrams illustrate a tag connector cable and a blade extension strip with 16 tag ports.

Tag connector cable
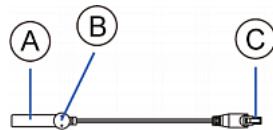
A	Barcode (ID number) for the tag connector cable
B	Tag connector
C	Cable connector for connecting the blade extension strip

Note: A tag connector cable has a unique barcode, which is displayed in the BCM2 device's web interface for identifying each blade extension strip where it is connected.

Blade extension strip with 16 tag ports
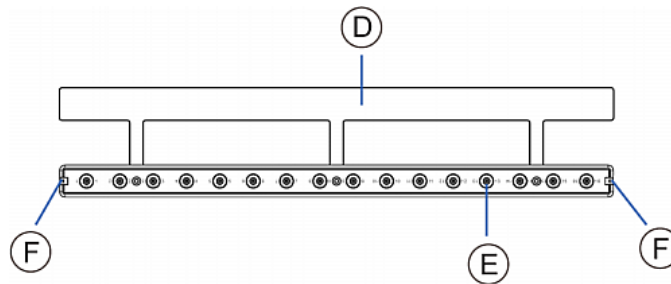
D	Mylar section with the adhesive tape
E	Tag ports
F	Cable socket(s) for connecting the tag connector cable

Note: Each tag port on the blade extension strip is labeled a number, which is displayed as the slot number in the BCM2 device's web interface.

▶ **To install a blade extension strip:**

1. Connect the tag connector cable to the blade extension strip.

   ▪ Plug the cable's connector into the socket at either end of the blade extension strip.
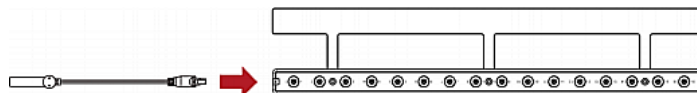
2. Move the blade extension strip toward the bottom of the blade chassis until its mylar section is fully under the chassis, and verify that the blade extension strip does not fall off easily. If necessary, you may use the adhesive tape in the back of the mylar section to help fix the strip in place.
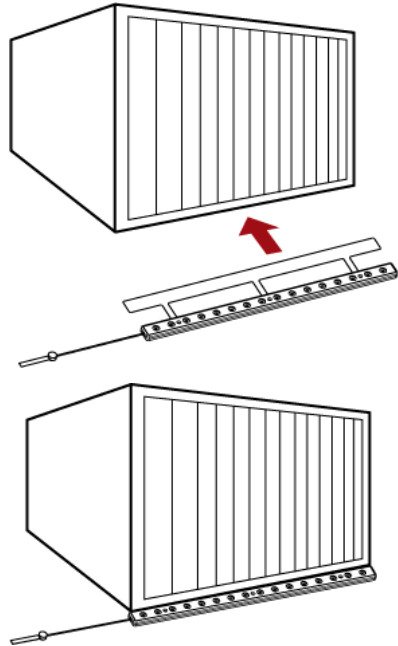
3. Connect one end of an asset tag to a blade server and the other end to the blade extension strip.

   a. Affix the adhesive part of the asset tag to one side of a blade server through the tag's tape.

   b. Plug the tag connector of the asset tag into a tag port on the blade extension strip.
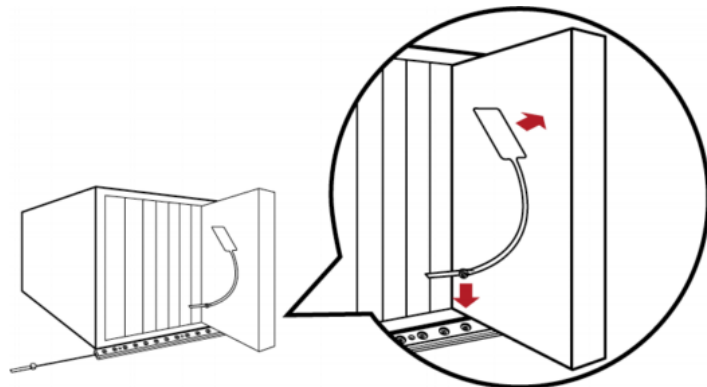
4. Repeat the above step until all blade servers in the chassis are connected to the blade extension strip via asset tags.

5. Plug the tag connector of the blade extension strip into the closest tag port of the regular or composite asset strip on the rack.
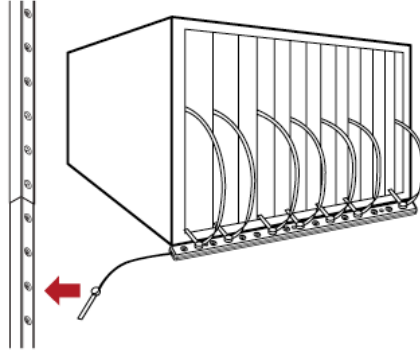
6. Repeat the above steps to connect additional blade extension strips. Up to 128 asset tags on blade extension strips are supported per FEATURE port.

Note: If you need to temporarily disconnect the blade extension strip from the asset strip, wait at least 1 second before re-connecting it back, or the BCM2 device may not detect it.

Connecting Composite Asset Sensors to the BCM2

A composite asset strip is named AMS-Mx-Z, where x is a number, such as AMS-M2-Z or AMS-M3-Z. It is a type of asset strip that functions the same as regular MASTER asset strips except for the following differences:

*   It has two RJ-45 connectors.
*   Multiple composite asset strips can be daisy chained.
*   It contains less tag ports than regular asset strips.

    For example, AMS-M2-Z contains two tag ports, and AMS-M3-Z contains three tag ports only.

The composite asset strip is especially useful for tracking large devices such as SAN boxes in the cabinet.

The following diagram illustrates AMS-M3-Z.
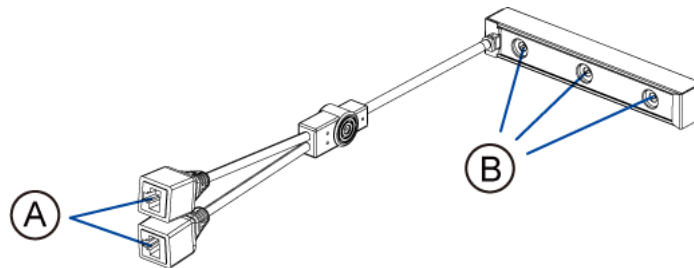
A	Two RJ-45 connectors
B	Tag ports

▶ **To connect composite asset strips to the BCM2 device:**

1. Connect a composite asset strip to the BCM2 device via a standard network patch cable (CAT5e or higher).

   a. Connect one end of the cable to the RJ-45 port labeled "Input" on the composite asset strip.

   b. Connect the other end of the cable to the FEATURE port on the BCM2 device.

2. Affix an asset tag to the IT device. Then connect this asset tag to the composite asset strip by plugging the tag connector into the tag port on the composite asset strip. For details, see *Connecting Regular Asset Strips to the BCM2* (see "*Connecting Regular Asset Sensors to the BCM2*" on page 48).

3. If necessary, daisy chain additional composite asset strips to track more IT devices.

   a. Get a standard network patch cable that is within 2 meters.

   b. Connect one end of the network cable to the RJ-45 connector labeled "Output" on the previous composite asset strip.

   c. Connect the other end of the cable to the RJ-45 connector labeled "Input" on the subsequent composite asset strip.

   d. Repeat the above steps to connect more composite asset strips. See *Daisy-Chain Limitations of Composite Asset Strips* (on page 53) for the maximum number of composite asset strips supported per chain.

It is highly recommended using the cable ties to help hold the weight of all connecting cables.

Daisy-Chain Limitations of Composite Asset Strips

There are some limitations when daisy chaining composite asset strips "AMS-Mx-Z," where x is a number.

• The maximum cable length between composite asset strips is 2 meters, but the total cable length cannot exceed 10 meters.

• The maximum number of composite asset strips that can be daisy chained depend on the Raritan product you purchased.

Raritan devices	Maximum strips per chain
EMX2-111,	Up to 4 composite asset strips

Raritan devices	Maximum strips per chain
PX2 PDUs, BCM1 (NOT BCM2 series)	are supported.
EMX2-888, PX3 PDUs, PX3TS transfer switches PMC (BCM2 series)	Up to 6 composite asset strips are supported.

Important: Different types of composite asset strips can be mixed in a chain as of release 3.3.0.

Connecting a GSM Modem

The following Cinterion® GSM modems can be connected to the BCM2 in order to send SMS messages containing event information.

- MC52iT
- MC55iT
- EHS6

See *Available Actions* (on page 207) for more information on SMS messages.

Note: BCM2 cannot receive SMS messages.

▶ **To connect the GSM modem:**

1. Connect the GSM modem to the serial port labeled CONSOLE / MODEM on the BCM2.

2. Configure the GSM modem as needed. See the supporting GSM modem help for information on configuring the GSM modem.

3. Configure the GSM modem settings in the BCM2 to specify the modem's SIM PIN number and the recipient phone number. See *Configuring the Serial Port* (on page 243).

Connecting an Analog Modem

The BCM2 supports remote dial-in communications to access the CLI through an analog modem. This dial-in feature provides an additional alternative to access the BCM2 when the LAN access is not available. To dial in to the BCM2, the remote computer must have a modem connected and dial the correct phone number.

Below are the analog modems that the BCM2 supports for sure:

- NETCOMM IG6000 Industrial Grade SmartModem
- US Robotics 56K modem

The BCM2 may also support other analog modems which Raritan did not test.

Note that the BCM2 does NOT support dial-out or dial-back operations via the modem.

▶ **To connect an analog modem:**

1. Plug a telephone cord into the phone jack of the supported modem.
2. Plug the modem's RS-232 cable into the serial port labeled CONSOLE / MODEM on the BCM2.

You need to enable the modem dial-in support to take advantage of this feature, see *Configuring the Serial Port* (on page 243).

Connecting an External Beeper

The BCM2 supports the use of an external beeper for audio alarms.

External beepers that are supported include but may not be limited to the following:

- Mallory Sonalert MODEL SNP2R

After having an external beeper connected, you can create event rules for the BCM2 to switch on or off the external beeper when specific events occur. See *Event Rules and Actions* (on page 190).

▶ **To connect an external beeper:**

1. Connect a standard network patch cable to the FEATURE port of the BCM2.
2. Plug the other end of the cable into the external beeper's RJ-45 socket.

   The beeper can be located at a distance up to 330 feet (100 m) away from the BCM2.

Cascading the BCM2 via USB

You can cascade a maximum of eight Raritan devices, using USB cables. All devices in the USB-cascading chain share the Ethernet connectivity. Different Raritan models can be cascaded as long as they are running an appropriate firmware.

The first device in the chain is the master device and all the other are slave devices.

Only the master device is physically connected to the LAN -- wired or wireless.

Each device in the chain is accessible over the network, with the bridging or port-forwarding cascading mode activated on the master device. See *Setting the Cascading Mode* (on page 149).

The master device's LAN connection method varies based on the cascading mode.

- The bridging mode supports the *wired* networking only.
- The port forwarding mode supports both the *wired* and *wireless* networking.

For more information on the USB-cascading configuration, see the *Cascading Guide*, which is available from Raritan website's *Support page* (*http://www.raritan.com/support/*).

▶ **To cascade the BCM2 devices via USB:**

1. Select one of the devices as the master device.
   - When the port forwarding mode over wireless LAN is intended, the master device must be a Raritan product with two USB-A ports, such as PX3, EMX2-888, PX3TS or BCM2.

2. Connect the master device to the LAN.
   - Bridging mode: Use a standard network patch cable (CAT5e or higher).
   - Port forwarding mode: Use a standard network patch cable or a Raritan USB WIFI wireless LAN adapter.

     For information on the Raritan USB WIFI adapter, see *USB Wireless LAN Adapters* (on page 58).

3. Connect the USB-A port of the master device to the USB-B port of an additional BCM2 via a USB cable. This additional device is Slave 1.

4. Connect Slave 1's USB-A port to the USB-B port of an additional BCM2 via another USB cable. The second additional device is Slave 2.

5. Repeat the same step to connect more slave devices. You may connect up to 7 slave devices.

▪ Do NOT connect any slave device to the LAN. That is, there is no connection of a standard network cable or USB wireless LAN adapter to the slave devices.

Note: The master/slave devices shown in the following diagram may not look the same as BCM2, but the USB-cascading connection method is the same.
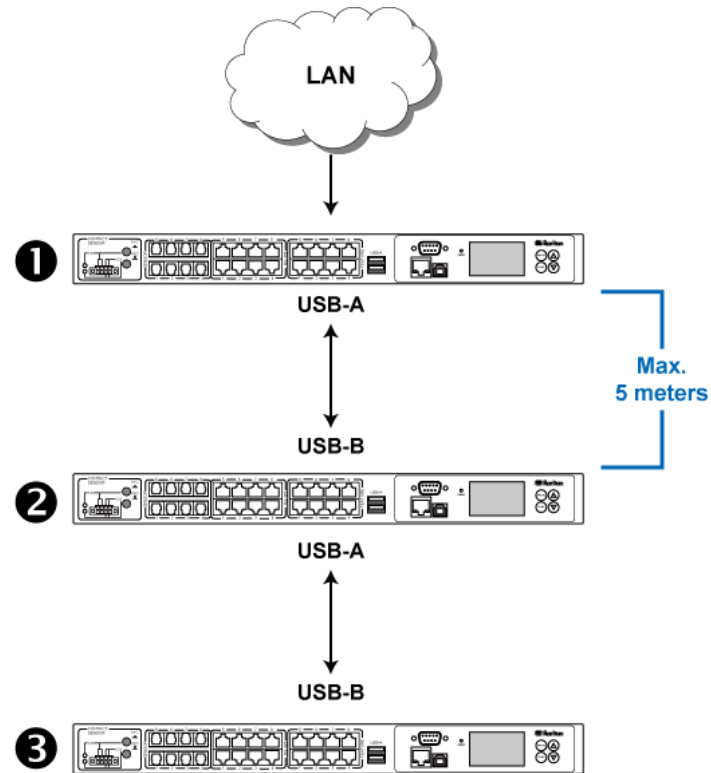
Number	Device role
1	Master device
2	Slave 1
3	Slave 2

1. Log in to the master device to configure the cascading mode. See *Setting the Cascading Mode* (on page 149) or *Configuring the Cascading Mode* (on page 340).

2. Configure the master and/or each slave device's networking settings.

▪ Bridging mode: You need to configure each cascaded device's network settings respectively.

▪ Port forwarding mode: Only the master device's network settings must be configured.

Note: To remotely identify the master and slave devices in the USB-cascading configuration, see Identifying Cascaded Devices.

▶ **Tip:**

The cascading configuration can be a combination of diverse Raritan products that support the cascading feature, including PX2, PX3, PX3TS, EMX, and BCM.

Wireless Network Connection

If intended, you can connect your BCM2 to a wireless network instead of a wired network.

▶ **To make a wireless connection:**

Do one of the following:

▪ Plug a supported USB wireless LAN adapter into the USB-A port on your BCM2.

▪ Connect a USB hub to the USB-A port on the BCM2. Then plug the supported USB wireless LAN adapter into the appropriate USB port on the hub.

See *USB Wireless LAN Adapters* (on page 58) for a list of supported wireless LAN adapters.

USB Wireless LAN Adapters

The BCM2 supports the following USB Wi-Fi LAN adapters.

Wi-Fi LAN adapters	Supported 802.11 protocols
SparkLAN WUBR-508N	A/B/G/N
Proxim Orinoco 8494	A/B/G
Zyxel NWD271N	B/G
Edimax EW-7722UnD	A/B/G/N
TP-Link TL-WDN3200 v1	A/B/G/N
Raritan USB WIFI	A/B/G/N

Note: To use the Edimax EW-7722UnD or Raritan USB WIFI wireless LAN adapter to connect to an 802.11n *wireless network, the handshake timeout setting must be changed to 500 or greater, or the wireless connection will fail.*

Supported Wireless LAN Configuration

If wireless networking is preferred, ensure that the wireless LAN configuration of your BCM2 matches the access point. The following is the wireless LAN configuration that the BCM2 supports.

- Network type: 802.11 A/B/G/N
- Protocol: WPA2 (RSN)
- Key management: WPA-PSK, or WPA-EAP with PEAP and MSCHAPv2 authentication
- Encryption: CCMP (AES)

Important: Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the BCM2. See *USB Wireless LAN Adapters* **(on page 58).**

Chapter 4 Using the Web Interface

Use the web interface of the BCM2 for configuration and administration. You must enable JavaScript in the web browser for proper operation.

▶ **Default login:**

- Username: admin
- Password: raritan
- You are prompted to change the defaults at your first login.

▶ **To login to the web interface:**

1. In a supported browser, go to the IP address of the PMC (BCM2).
2. Login and accept security warnings.

In This Chapter

Supported Web Browsers

- Internet Explorer® 11
- Windows Edge
- Firefox® 25 and later
- Safari® (Mac)
- Google® Chrome® 52 and later
- Android 4.2 and later
- iOS 7.0 and later

Note: Depending on the browser you use, spin controls similar to
may or may not appear in the numeric input fields. Clicking these adjusts numeric values by 1.

Changing Your Password

You must have the Change Own Password permission to change your own password. See *Creating Roles* (see "*Creating a Role*" on page 132, on page 128).

You must have Administrator Privileges to change other users' passwords. See *Editing or Deleting Users* (on page 127).

▶ **Password change request on first login:**

On *first login*, if you have both the Change Local User Management and Change Security Settings permissions, you can choose to either change your password or ignore it.

- *Not Now* ignores the request for this time only.
- *Do not ask again* ignores the request permanently. If you select this checkbox, then click *Not Now*.
- Or enter the new password and click Ok.

  Users without permissions listed must change password.

  Note: This password change request also appears if the 'force password change' is enabled in the user account setting. See **Creating Users** *(on page 123).*

▶ **To change your password via the Change Password command:**

1. Choose User Management > Change Password.
2. First type the current password, and then the new password twice. Passwords are case sensitive.
   - A password comprises 4 to 64 characters.

Introduction to the Web Interface

The web interface consists of four areas as shown below.

▶ **Operation:**

1. Click any menu or submenu item in the area of ❶.
2. That item's data/setup page is then opened in the area of ❷.
3. Now you can view or configure settings on the opened page.

To return to the main menu and the Dashboard page, click **Raritan.** on the top-left corner.

Number	Web interface element
❶	Menu
❷	Data/setup page of the selected menu item
❸	▪ Left side: - BCM2 device name *Note: To customize the device name, see .* ▪ Right side: - Your login name, which you can click to view your user account settings - Logout button
❹	From top to bottom -- ▪ Your BCM2 model ▪ Current firmware version ▪ **Online Documentation**: link to the BCM2 online help. - See Browsing through the Online Help. ▪ **Raritan Support**: link to the Raritan Technical Support webpage. ▪ Date and time of your user account's last login - Click **Last Login** to view your login history. ▪ BCM2 system time - Click **Device Time** to open the Date/Time setup page.

Menu

Depending on your model and hardware configuration, your menu may show some or all items.
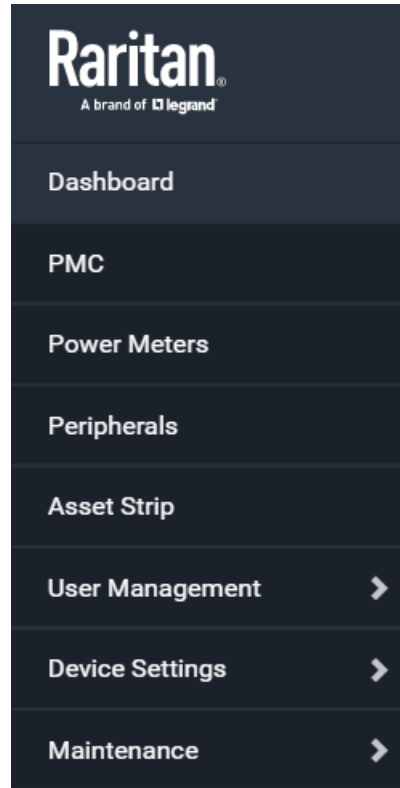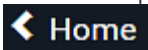
Menu	Information shown
Dashboard	Summary of the BCM2 status, including a list of alerted sensors and alar if any. See *Viewing the Dashboard* (on page 67).
PMC	Device data and settings, such as the device name and MAC address. See PMC.
Power Meters	Power meters and panels data and settings. See Power Meters.
Peripherals	Status and settings of Raritan environmental sensor packages, if connec See *Peripherals* (on page 90).

Menu	Information shown
Feature Port The name 'Feature Port(s)' will be replaced with one of the device names listed to the right	Status and settings of the device connected to the Feature port(s), which be one of the following. ▪ Asset Strip ▪ External Beeper ▪ LHX 20 ▪ SHX 30 ▪ LHX 40 ▪ Power CIM See *Feature Port* (on page 108).
Webcam, Webcam Snapshots	The webcam-related menu items appear only when there are webcam(s) connected to the BCM2. Webcam live snapshots/video and webcam settings. See *Webcam Management* (on page 265).
User Management	Data and settings of user accounts and groups, such as password chang See *User Management* (on page 122).
Device Settings	Device-related settings, including network, security, system time, event rules and more. See *Device Settings* (on page 134).
Maintenance	Device information and maintenance commands, such as firmware upgr device backup and reset. See *Maintenance* (on page 251).

If a menu item contains the submenu, the submenu is shown after clicking that item.

▶ **To return to the previous menu list, do any below:**

- Click the topmost link with the symbol **>**. For example, click **< Home**.

- Press Backspace on the keyboard.

OR click on the top-left corner to return to the main menu.

The Yellow- or Red-Highlighted Sensors

When a numeric sensor's reading enters the warning or critical range, the background color of that sensor's row turns to yellow or red for alerting you.

For a discrete (on/off) sensor, the row changes the background color when the sensor enters the abnormal state.

See the table for the meaning of each color:

Color	State
White	The background is white in one of the following scenarios: • For a numeric sensor, no thresholds have been enabled. • If any thresholds have been enabled for a numeric sensor, the sensor reading is within the normal range, which is between the lower and upper warning thresholds. • For a discrete (on/off) sensor, the sensor state is normal. • The sensor is unavailable or unmanaged.
Yellow	The reading drops below the lower warning threshold or rises above the upper warning threshold.

| Red | The meaning of the red color varies depending on the sensor type:
• For a numeric sensor, this color indicates the reading drops below the lower critical threshold or rises above the upper critical threshold.
▪ For a discrete (on/off) sensor, this color indicates the sensor is in the "alarmed" state. |

Raritan.
A brand of ☐ legrand

To find the exact meaning of the alert, read the information shown in the State (or Status) column:

- below lower critical: The numeric sensor's reading drops below the lower critical threshold.
- below lower warning: The numeric sensor's reading drops below the lower warning threshold.
- above upper critical: The numeric sensor's reading reaches or exceeds the upper critical threshold.
- above upper warning: The numeric sensor's reading reaches or exceeds the upper warning threshold.
- alarmed: The discrete sensor is NOT in the normal state.

For information on the thresholds, see *Setting Power Thresholds* (on page 82).

Viewing the Dashboard

When you log in to the web interface, the Dashboard page is displayed by default. This page provides an overview of the BCM2 device's status.
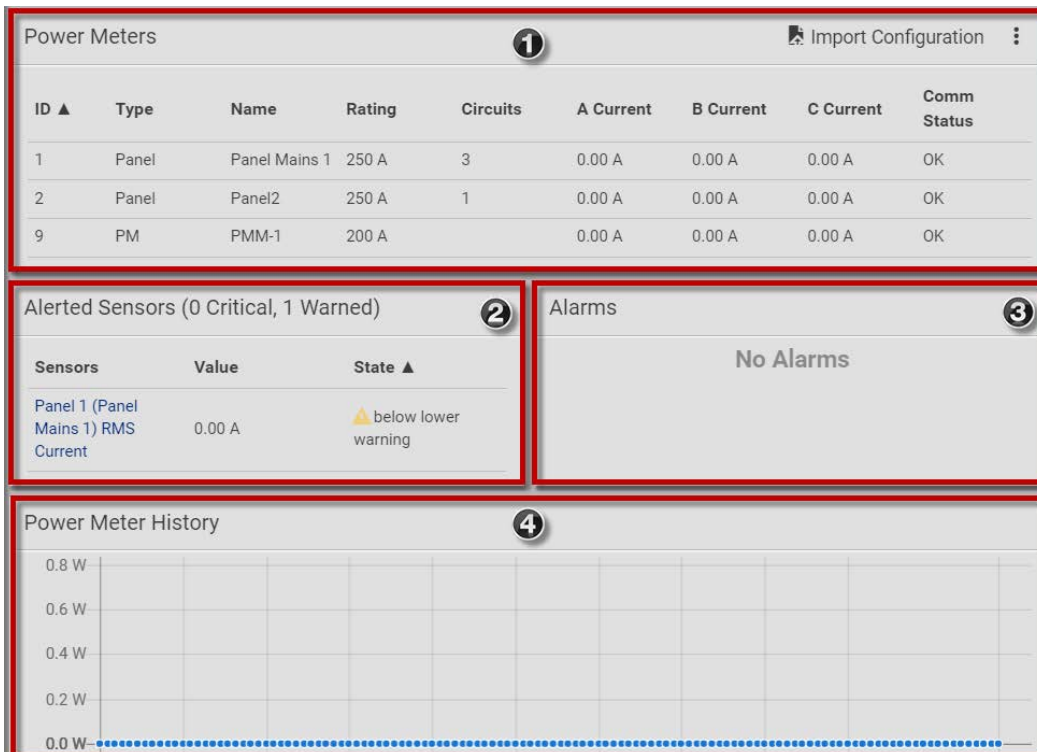
1	Configured power meters with basic details and current readings for each phase . See *Dashboard - Power Meters* (on page 68).
2	Enabled thresholds show alerts in red and yellow. See *Dashboard - Alerted Sensors* (on page 69)
3	Alarms that need attention. See *Dashboard - Alarms* (on page 70).
4	Chart of recent data. See *Dashboard - Power Meter History* (on page 72).

Dashboard - Power Meters

The Power Meters section of the Dashboard shows all configured power meters and panels, with some details for each.

1	ID: The PMM rotary switch setting for the power meter.
2	Type: Panel or PM Name: The configured name Rating: The configured circuit rating.
3	Circuits: The number of configured circuits
4	A Current/B Current/C Current: The current reading in Amps for each phase.

Dashboard - Alerted Sensors

When any internal sensors or environmental sensor packages connected to the BCM2 enter an abnormal state, the Alerted Sensors section in the Dashboard show them for alerting users. This section also lists tripped circuit breakers or blown fuses, if available.

To view detailed information or configure each alerted sensor, you can click each sensor's name to go to individual sensor pages. See *Individual Sensor/Actuator Pages* (on page 103).

If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

Alerted Sensors (1 Critical, 1 Warned)		
Sensors	**Value**	**State ▲**
Temperature 3	20.7 °C	⚠ above upper critical
Temperature 1	19.8 °C	⚠ above upper warning

▶ **Summary in the section title:**

Information in parentheses adjacent to the title is the total number of alerted sensors.

For example:

- **1 Critical**: 1 sensor enters the critical or alarmed state.

  - Numeric sensors enter the critical state.

  - State sensors enter the alarmed state.

- **1 Warned**: 1 'numeric' sensor enters the warning state.

▶ **List of alerted sensors:**

Two icons are used to indicate various sensor states.

Icons	Sensor states
⚠️	For numeric sensors: ▪ above upper warning ▪ below lower warning
🔺	For numeric sensors: ▪ above upper critical ▪ below lower critical
	For state sensors: ▪ alarmed state

For details, see *Sensor/Actuator States* (on page 97).

Dashboard - Alarms

If configuring any event rules which require users to take the acknowledgment action, the Alarms section will list any event which no one acknowledges yet since event occurrence.

Note: For information on event rules, see **Event Rules and Actions** *(on page 190).*

Only users with the Acknowledge Alarms permission can manually acknowledge an alarm.

▶ **To acknowledge an alarm:**

- Click Acknowledge, and that alarm then disappears from the Alarms section.

This table explains each column of the alarms list.

Field	Description
Name	The customized name of the Alarm action.
Reason	The first event that triggers the alert.
First Appearance	The date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	The date and time when the event indicated in the Reason column occurred for the last time.
Count	The number of times the event indicated in the Reason column has occurred.
More Alerts	This field appears only when there are more than one type of events triggering this alert. If there are other types of events (that is, other reasons) triggering the same alert, the total number of additional reasons is displayed. You can click it to view a list of all events triggering this alert.

Dashboard - Power Meter History

The history graph for the power meter helps you observe whether there were abnormal events within the past range of time. The default is to show the active power data.
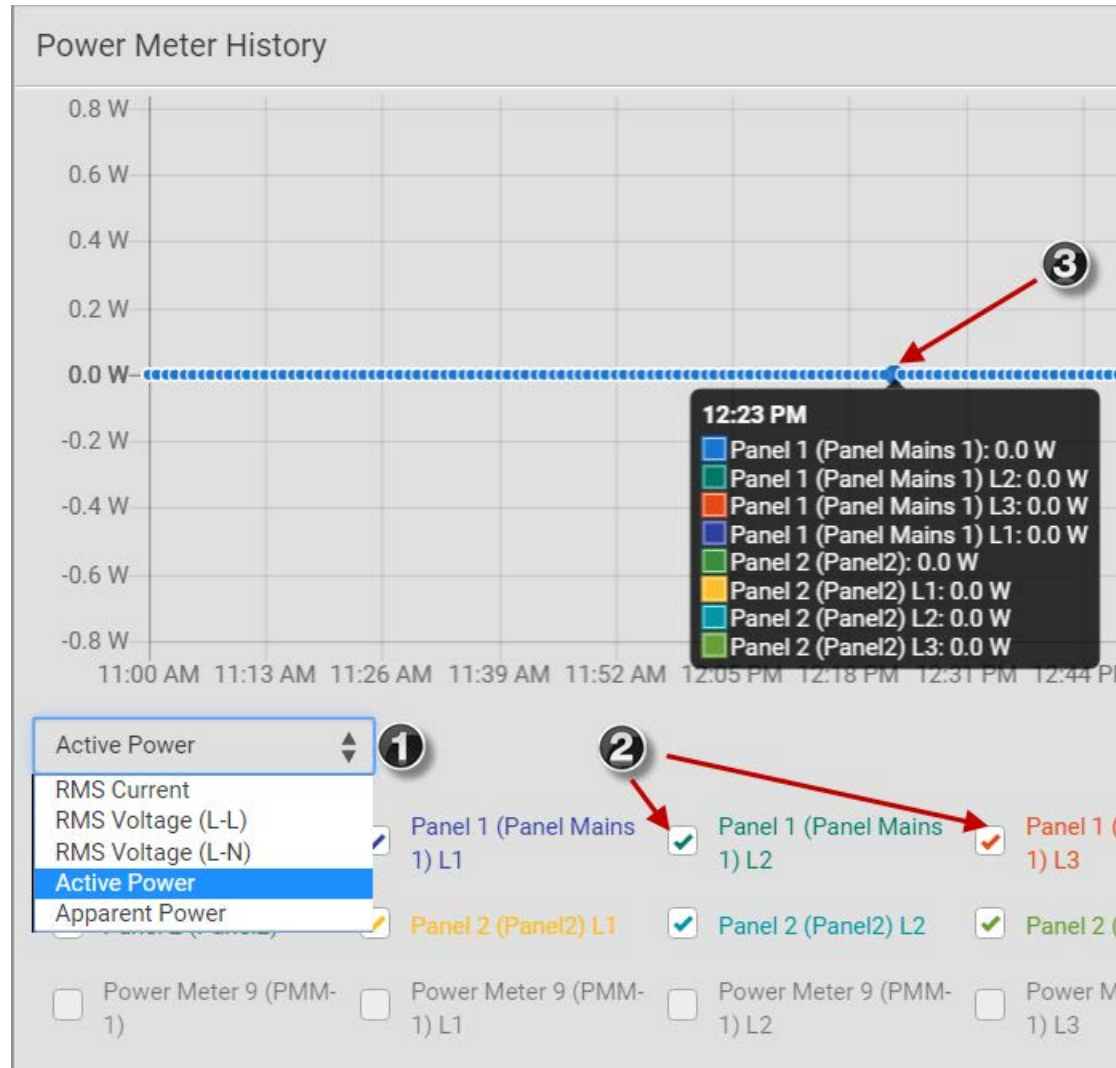
1	Select a different data type by clicking the selector below the diagram.
	▪ RMS Current
	▪ RMS Voltage Line to Line
	▪ RMS Voltage Line to Neutral
	▪ Active power
	▪ Apparent power

2	Select the checkbox for the lines you want to add to the diagram. Each line is assigned a custom color.
3	Hover the mouse over the graph line to view details for the minute. Each line color is coordinated in the details.

PMC Power Metering Controller

Click PMC in the Menu to open the Power Metering Controller page.

You can view details on the PMC:

- Firmware Version
- Serial Number
- MAC Address
- Internal beeper state

▶ **To edit PMC settings:**

- Click the Edit Settings link. The following settings can be changed.
1. Name: The name of the PMC appears in the top bar of the web interface.
2. Peripheral Device Z Coordinate Format: Select Rack Units or Free Form.

- If set to Rack Units, the Z coordinate field in the peripheral device settings only allows to enter numerical values. If set to Free-form, any input is allowed. The label of the input field on the peripheral device settings page will indicate which format is expected.

3. Peripheral Device Auto Management: Select the checkbox to enable. Selects whether newly plugged peripheral devices are automatically assigned to an empty slot (if any is available).

4. Altitude: Set the altitude in meters for the differential air pressure sensor.

5. Click Save.

Power Meters

To view or manage the connected panels and power meters, click Power Meters in the menu.

The Power Meters page contains all configured power meters and panels, allows you to scan for unconfigured meters, and gives access to all configuration possibilities.

For help with configuring power meters and panels, see **Configuring Power Meters and Branch Circuit Monitors** *(on page 7).*

Viewing the Power Meter Data

To view power meter data, go to the Power Meters page and click to select a power meter. You can also select a power meter from the dashboard.

The Power Meter details page opens with a list of sensor data and readings.

1	Sensor list
2	Readings in total for the power meter.
3	Readings for each phase.
4	If thresholds have been configured for a sensor, and a reading meets a threshold, the data is highlighted red or yellow.
5	Value contains the reading for the sensor.

6	State indicates if readings are normal, warning or critical.
7	Click actions menu for more options.

Power Meter Management

This section introduces the operations for a power meter module. For information on the power meter's sensor data, see *Viewing the Power Meter Data* (on page 75).

▶ **To access power meter management options:**

- Click Power Meters in the menu, then select a power meter. In the power meter details page, click the actions icon in the top right corner.

The following options are available:

- Edit Thresholds: See *Configure Thresholds* (on page 82).
- Configure: You can edit some details of the power meter configuration. See *Configure Power Meter* (on page 9).
- Reset Active Energy: See below.
- Delete: Click Delete to delete this power meter.
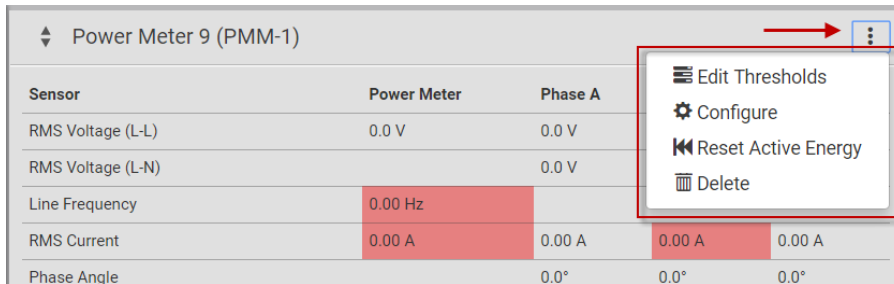
▶ **To reset active energy:**

Click Reset Active energy to reset the power meter's active energy to 0 (zero) Wh. Only users with the "Change PMC, PMB & PMM Configuration" permission can reset active energy readings.

Tip: To reset all active energy readings simultaneously, see Resetting All Active Energy. To reset a branch circuit's active energy, see **Panel Branch Circuits Operations** *(on page 81). To reset a panel's active energy, see* **Panel Mains Circuit Management** *(on page 80).*

Enable Modbus Access

For details on Modbus, see Configuring Modbus TCP and/or RTU.

▶ **To enable Modbus access:**

1. Select the power meter or panel in the Power Meters page.

2. Click the actions icon to open the options, then choose Configure.

3. Select the Enable Modbus Access checkbox, and assign a "unique" Modbus address to the power meter.

   ▪ This Modbus address must be different from that of the main controller, any panel or power meter module connected to this BCM2, or the BCM2 does NOT allow you to save this dialog.

   ▪ If Modbus/RTU is enabled, make sure this Modbus address is also different from those of other devices on the same Modbus RTU bus.

4. Click OK to save.

Viewing the Panel Data

To view panel data, including mains circuit and branch circuits, go to the Power Meters page and click to select a panel. You can also select a panel from the dashboard.

ID ▲	Type	Name	Rating	Circuits
1	Panel	Panel Mains 1	250 A	3
2	Panel	Panel2	250 A	1
3	Panel	Rack3	250 A	0
9	PM	PMM-1	200 A	

The Panel details page opens with a list of sensor data and readings at the top, and a list of Panel Branch Circuits at the bottom.

①	A short list of readings is available by default.
②	To add more readings, click Select Readings, then choose the sensors to add. See graphic for menu details.
	Click actions menu for more options. See *Panel Mains Circuit Management* (on page 80).

3	Readings in total for the panel.
	If thresholds have been configured for a sensor, and a reading meets a threshold, the data is highlighted red or yellow.
4	Readings for each phase.
5	Value contains the reading for the sensor.
6	State indicates if readings are normal, warning or critical.
7	Branch circuit details and readings.
8	Click a branch circuit to show the menu: Circuit Details to open a new page. Or, delete a circuit.

▶ **Panel Branch Circuit Details page:**

Click a configured circuit, then choose Circuit Details to open a new page with panel branch circuits details. Similar to the panel details, the circuit details displays readings at the circuit level.

Note: Branch circuit RMS voltage is the minimum *of Line-Line or Line-Neutral RMS voltage readings. NO alerts will be available for a branch circuit's RMS voltage even when voltage thresholds are set for it.*

1	Panel name and circuit name. Click the arrows to scroll through the configured branch circuits.
2	Click actions menu for more options. See *Panel Branch Circuits Operations* (on page 81).
3	Sensor list. This list may be filtered by the Select Readings settings in the Panel Mains Circuit page.

④	Total readings for the whole circuit.
⑤	Readings for each phase. Each phase is labeled with the CT number.
⑥	Value contains the reading for the sensor.
⑦	State indicates if readings are normal, warning or critical.

Panel Mains Circuit Management

This section introduces the operations for a panel. For information on the panel's sensor data, see *Viewing the Panel Data* (on page 77).

▶ **To access panel management options:**

Click Power Meters in the menu, then select a panel. In the panel details page, click the actions icon in the top right corner.

The following options are available:

- Edit Thresholds: See *Configure Thresholds* (on page 82).
- Configure: You can edit some details of the panel configuration. See *Configure Panel Mains Circuit* (on page 10).
- Export Readings as CSV: See *Export Readings as CSV* (on page 88)
- Reset Active Energy: See below.
- Delete: Click Delete to delete this power meter.

▶ **To reset Active Energy:**

Click Reset Active Energy to reset this panel's active energy reading to 0 (zero) Wh. Only users with the "Change PMC, PMB & PMM Configuration" permission can reset active energy readings.

Tip: To reset all active energy readings simultaneously, see Resetting All Active Energy. To reset a branch circuit's active energy, see **Panel Branch Circuits Operations** *(on page 81). To reset a Power Meter's active energy, see* **Power Meter Management** *(on page 76).*

Panel Branch Circuits Operations

This section introduces the operations for the Panel Branch Circuits section.

To manage branch circuits, click the desired branch circuit to open a menu.

▶ **Circuit Details:**

A circuit page showing the circuit readings and detailed information opens. Click the actions menu at top right corner. The following options are available:

- Edit Thresholds: See *Configure Thresholds* (on page 82).
- Configure Circuit: Click to open the circuit's setup dialog. See *Configure Panel Branch Circuits* (on page 11).
- Reset Active Energy: This button resets this circuit's active energy to 0 (zero) Wh. Only users with the "Change PMC, PMB & PMM Configuration" permission can reset active energy readings.
- Delete: Click to delete this circuit.

Tip: To reset all active energy readings simultaneously, see Resetting All Active Energy. To reset a panel's active energy, see **Panel Mains Circuit Management** *(on page 80). To reset a power meter's active energy, see* **Power Meter Management** *(on page 76).*

Note: NO alerts will be available for a branch circuit's RMS voltage even though you have set the voltage thresholds for it.

Setting Power Thresholds

Setting and enabling the thresholds causes the BCM2 to generate alert notifications when it detects that any component's power state crosses the thresholds. See *The Yellow- or Red-Highlighted Sensors* (on page 66, "*Yellow- or Red-Highlighted Sensors*" on page 95).

There are four thresholds for each sensor: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

- Upper and Lower Warning thresholds indicate the sensor reading enters the warning level.
- Upper and Lower Critical thresholds indicate the sensor reading enters the critical level.

To avoid generating a large amount of alert events, you can set the assertion timeout and deassertion hysteresis.

Note: After setting the thresholds, remember to configure event rules. See **Event Rules and Actions** *(on page 190).*

Configure Thresholds

| ① | In the Power Meters page, click the panel or power meter. | |

The details page opens.

② In the details page, click the actions icon, then choose Edit Thresholds.
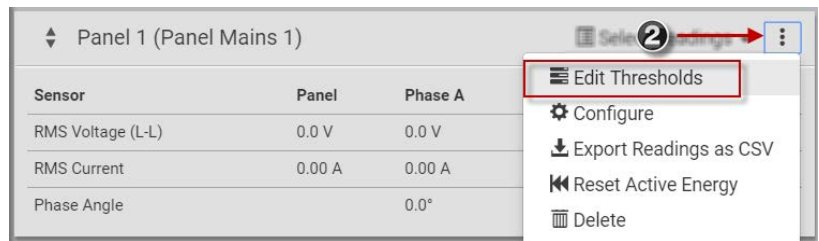
③ The sensor list displays.

Click a sensor to open the Edit Threshold dialog.
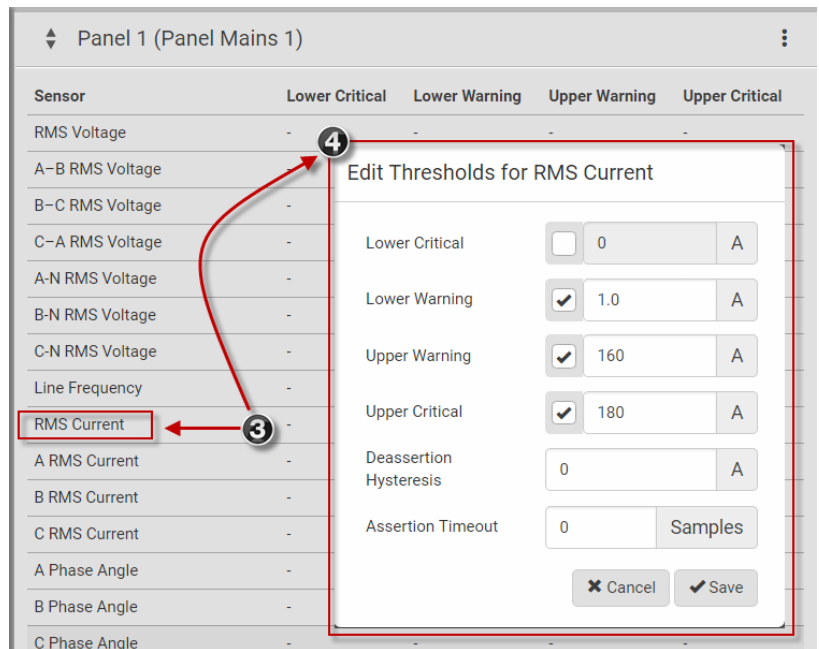
④ Select the checkbox for the level, and enter the threshold current in amps. Click OK.

This example shows RMS Current thresholds set for upper warning and critical levels for the circuit max current rating, and a lower warning set for 1 amp.

"To Assert" and Assertion Timeout

If multiple sensor states are available for a specific sensor, the BCM2 asserts a state for it whenever a bad state change occurs.

▶ **To assert a state:**

To assert a state is to announce a new, "worse" state.

Below are bad state changes that cause the BCM2 to assert.
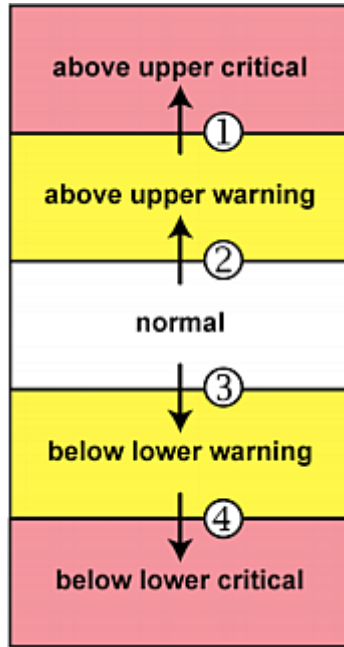
1. above upper warning --> above upper critical
2. normal --> above upper warning
3. normal --> below lower warning
4. below lower warning --> below lower critical

▶ **Assertion Timeout:**

84

In the threshold settings, the Assertion Timeout field postpones or even cancels the "assertion" action. It determines how long a sensor must be in the "worse" new state before the BCM2 triggers the "assertion" action. If that sensor changes its state again within the specified wait time, the BCM2 does NOT assert the worse state.

To disable the assertion timeout, set it to 0 (zero).

Note: For most sensors, the measurement unit in the "Assertion Timeout" field is sample. Sensors are measured every second, so the timing of a sample is equal to a second. BCM2 is an exception to this, with a sample of 3 seconds.

▶ How "Assertion Timeout" is helpful:

If you have created an event rule that instructs the BCM2 to send notifications for assertion events, setting the "Assertion Timeout" is helpful for eliminating a number of notifications that you may receive in case the sensor's readings fluctuate around a certain threshold.

"To De-assert" and Deassertion Hysteresis

After the BCM2 asserts a worse state for a sensor, it may de-assert that state later on if the readings improve.

▶ **To de-assert a state:**

To de-assert a state is to announce the end of the previously-asserted worse state.

Below are good state changes that cause the BCM2 to de-assert the previous state.
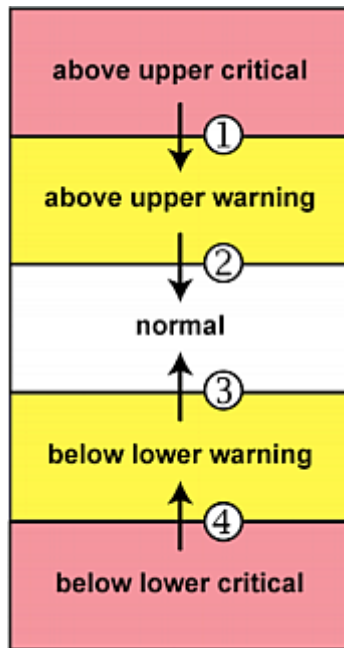
1. above upper critical --> above upper warning
2. above upper warning --> normal
3. below lower warning --> normal
4. below lower critical --> below lower warning

▶ **Deassertion Hysteresis:**

In the threshold settings, the Deassertion Hysteresis field determines a new level to trigger the "deassertion" action.

This function is similar to a thermostat, which instructs the air conditioner to turn on the cooling system when the temperature exceeds a pre-determined level. "Deassertion Hysteresis" instructs the BCM2 to de-assert the worse state for a sensor only when that sensor's reading reaches the pre-determined "deassertion" level.

For upper thresholds, this "deassertion" level is a decrease against each threshold. For lower thresholds, this level is an increase to each threshold. The absolute value of the decrease/increase is exactly the hysteresis value.

For example, if Deassertion Hysteresis = 2, then:

- Upper Critical = 33, so its "deassertion" level = 33 - 2 = 31.
- Upper Warning = 25, so its "deassertion" level = 25 - 2 = 23.
- Lower Critical = 10, so its "deassertion" level = 10 + 2 = 12.
- Lower Warning = 18, so its "deassertion" level = 18 + 2 = 20.

To use each threshold as the "deassertion" level instead of determining a new level, set the Deassertion Hysteresis to 0 (zero).

▶ How "Deassertion Hysteresis" is helpful:

If you have created an event rule that instructs the BCM2 to send notifications for deassertion events, setting the "Deassertion Hysteresis" is helpful for eliminating a number of notifications that you may receive in case a sensor's readings fluctuate around a certain threshold.

Export Readings as CSV

Export instantaneous readings from the power meter controller as a CSV file. The export file may be helpful to diagnose issues.

You can export readings from each configured power meter and panel.

▶ **Power meter includes the following readings:**

- ID
- Name
- Line to Line Voltages
- L1-L2, L2-L3, L3-L1
- Line to Neutral voltages
- L1-N
- L2-N
- L3-N
- Frequency
- L1 Current, L2 Current, L3 Current
- L1 Active   Power, L2 Active Power, L3 Active Power
- L1 Reactive   Power, L2 Reactive Power, L3 Reactive Power
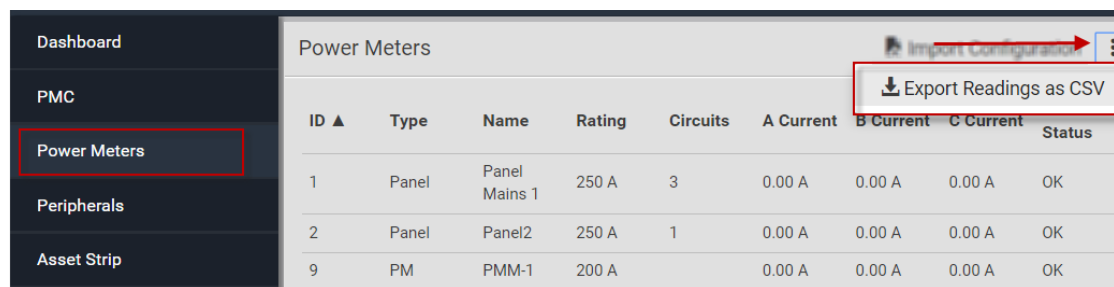
▶ **Panel includes the following readings:**

- Mains Sensors
    - Line to Line Voltages
        - L1-L2, L2-L3, L3-L1
- Line to Neutral voltages
    - L1-N
    - L2-N
    - L3-N
- Frequency
- L1 Current, L2 Current, L3 Current
- L1 Active   Power, L2 Active Power, L3 Active Power
- L1 Reactive   Power, L2 Reactive Power, L3 Reactive Power
- For each configured circuit
    - Name
    - For each circuit pole

- Position
- Phase
- CT Number
- Current
- Active Power
- Reactive Power

▶ **To export readings as CSV:**

1. Click Power Meters in the Menu.
2. Click the actions icon, then choose Export Readings as CSV.

Dashboard	Power Meters						Import Configuration	⋮
PMC							⬇ Export Readings as CSV	
Power Meters	ID ▲	Type	Name	Rating	Circuits	A Current	B Current	C Current	Status
Peripherals	1	Panel	Panel Mains 1	250 A	3	0.00 A	0.00 A	0.00 A	OK
Asset Strip	2	Panel	Panel2	250 A	1	0.00 A	0.00 A	0.00 A	OK
	9	PM	PMM-1	200 A		0.00 A	0.00 A	0.00 A	OK

Peripherals

If there are Raritan environmental sensor packages connected to the BCM2, they are listed on the Peripherals page. See *Connecting Environmental Sensor Packages* (on page 26).

An environmental sensor package comprises one or some of the following sensors/actuators:

- Numeric sensors: Detectors that show both readings and states, such as temperature sensors.
- State sensors: Detectors that show states only, such as contact closure sensors.
- Actuators: An actuator controls a system or mechanism so it shows states only.

The BCM2 communicates with *managed* sensors/actuators only and retrieves their data. It does not communicate with unmanaged ones. See *Managed vs Unmanaged Sensors/Actuators* (on page 96).

When the number of "managed" sensors/actuators has not reached the maximum, the BCM2 automatically brings newly-detected sensors/actuators under management by default.

One BCM2 can manage a maximum of 32 sensors/actuators.

Note: To disable the automatic management function, go to . You need to manually manage a sensor/actuator only when it is not under management.

When any sensor/actuator is no longer needed, you can unmanage/release it.

Open the Peripherals page by clicking Peripherals in the Menu. Then you can:

- **Perform actions on multiple sensors/actuators by using the control/action icons on the top-right corner.**

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1	
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3	
3	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4	
5	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	
6	On/Off 5		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 5	

Peripheral Devices

- Go to an individual sensor's or actuator's data/setup page by clicking its name.

Peripheral Devices

# ▲	Name
1	On/Off 1
2	On/Off 2
3	Temperature 1
4	Absolute Humidity 1
5	Relative Humidity 1

If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

▶ **Sensor/actuator overview on this page:**

If any sensor enters the alarmed state, it is highlighted in yellow or red. See *Yellow- or Red-Highlighted Sensors* (see "*The Yellow- or Red-Highlighted Sensors*" on page 66, on page 95). An actuator is never highlighted.

Column	Description
Name	By default the BCM2 assigns a name comprising the following two elements to a newly-managed sensor/actuator. ▪ Sensor/actuator type, such as "Temperature" or "Dry Contact." ▪ Sequential number of the same sensor/actuator type, like 1, 2, 3 and so on. You can customize the name. See *Individual Sensor/Actuator Pages* (on page 103).
Reading	Only managed 'numeric' sensors show this data, such as temperature and humidity sensors.
State	The data is available for all sensors and actuators. See *Sensor/Actuator States* (on page 97).
Type	Sensor or actuator type.

Column	Description
Serial Number	This is the serial number printed on the sensor package's label. It helps to identify your Raritan sensors/actuators. See *Finding the Sensor's Serial Number* (on page 99).
Position	The data indicates where this sensor or actuator is located in the sensor chain. See *Identifying the Sensor Position and Channel* (on page 100).
Actuator	Indicates whether this sensor package is an actuator or not. If yes, the symbol ✔ is shown.

▶ **To release or manage sensors/actuators:**

When the total of managed sensors/actuators reaches the maximum (32), you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace any managed ones. To replace a managed sensor/actuator, see *Managing One Sensor or Actuator* (on page 101). To release any one, follow this procedure.

1. Click ☑ to make checkboxes appear in front of sensors/actuators.

   Tip: To perform the desired action on only one sensor/actuator, simply click that sensor/actuator without making the checkboxes appear.

2. Select multiple sensors/actuators.
   - To release sensors/actuators, you must only select "managed" ones. See *Sensor/Actuator States* (on page 97).
   - To manage sensors/actuators, you must only select "unmanaged" ones.
   - To select ALL sensors/actuators, select the topmost checkbox in the header row.

3. To release selected ones, click ⚙ > Release.

   To manage them, click ⚙ > Manage.

- The management action triggers a "Manage peripheral device" dialog. Simply click Manage if you are managing *multiple* sensors/actuators.

Manage peripheral device

- Automatically assign a sensor number
- Manually select a sensor number

Sensor 1 (QLLemu0001)

[Cancel] [Manage]

- If you are managing only *one* sensor/actuator, you can choose to assign an ID number by selecting "Manually select a sensor number." See *Managing One Sensor or Actuator* (on page 101).

4. Now released sensors/actuators become "unmanaged."

Managed ones show one of the managed states.

▶ **To configure default threshold settings:**

Note that any changes made to default threshold settings not only re-determine the initial threshold values applying to newly-added sensors but also the threshold values of the already-managed sensors where default thresholds are being used. See *Individual Sensor/Actuator Pages* (on page 103).

1. Click ⚙ > Default Threshold Setup.

2. **Click the desired sensor type** (required), and then click Edit Thresholds.

Peripherals Default Thresholds				
				Edit Thresholds
Sensor Type	**Lower Critical**	**Lower Warning**	**Upper Warning**	**Upper Critical**
Absolute Humidity	2 g/m³	4 g/m³	20 g/m³	22 g/m³
Air Flow	0.4 m/s	0.8 m/s	2.6 m/s	3.2 m/s
Air Pressure	---	---	80 Pa	100 Pa
Relative Humidity	10 %	15 %	85 %	90 %
Temperature	10 °C	15 °C	30 °C	35 °C
Vibration	---	---	0.05 g	0.1 g

3. Make changes as needed.

   ▪ To enable any threshold, select the corresponding checkbox.

   ▪ Type a new value in the accompanying text box.

   For concepts of thresholds, deassertion hysteresis and assertion timeout, see Sensor Threshold Settings.

4. Click Save.
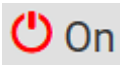
Tip: To customize the threshold settings on a per-sensor basis, go to **Individual Sensor/Actuator Pages** *(on page 103).*

▶ **To turn on or off any actuator(s):**

1. Select one or multiple actuators which are *in the same status* - on or off.

   ▪ To select multiple actuators, click [icon] to make checkboxes appear and then select desired actuators.

2. Click the desired button.

   [On button]: Turn ON.

   [Off button]: Turn OFF.

3. Confirm the operation when prompted.

Tip: If intending to control the actuator via the front panel, see **Front Panel Settings** *(on page 242).*

Yellow- or Red-Highlighted Sensors

The BCM2 highlights those sensors that enter the abnormal state with a yellow or red color. Note that numeric sensors can change colors only after you have enabled their thresholds.

Tip: When an actuator is turned ON, it is also highlighted in red for drawing attention.

For concepts of thresholds, deassertion hysteresis and assertion timeout, see Sensor Threshold Settings.

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	25.0 °C	above upper critical	Temperature	AEH2A51454	Port 1	
2	Absolute Humidity 1	10.8 g/m³	normal	Absolute Humidity	AEI1750551	Port 4	
3	Absolute Humidity 2	11.0 g/m³	above upper warning	Absolute Humidity	AEI2850240	Port 4	
4	Temperature 2	25.8 °C	above upper critical	Temperature	AEI2A50775	Port 1	
5	Relative Humidity 1	44 %	normal	Humidity	AEI2A50775	Port 1	

In the following table, "R" represents any numeric sensor's reading. The symbol <= means "smaller than" or "equal to."

Sensor status	Color	States shown in the interface	Description
Unknown	⬜	unavailable	Sensor state or readings cannot be detected.
		unmanaged	Sensors are not being managed. See *Managed vs Unmanaged Sensors/Actuators* (on page 96).
Normal	⬜	normal	▪ Numeric or state sensors are within the normal range. -- OR -- ▪ No thresholds have been enabled for numeric sensors.
Warning	🟨	above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
		below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
Critical	🟥	above upper critical	Upper Critical threshold < "R"
		below lower critical	"R" < Lower Critical threshold

Sensor status	Color	States shown in the interface	Description
Alarmed		alarmed	State sensors enter the abnormal state.
OCP alarm		Open	▪ Circuit breaker trips. -- OR -- ▪ Fuse blown.

If you have connected a Schroff® LHX/SHX heat exchanger, when any sensor implemented on that device fails, it is also highlighted in red.

Managed vs Unmanaged Sensors/Actuators

To manually manage or unmanage/release a sensor or actuator, see *Peripherals* (on page 90).

▶ **Managed sensors/actuators:**

- The BCM2 communicates with managed sensors/actuators and retrieves their data.
- Managed sensors/actuators are always listed on the Peripheral Devices page no matter they are physically connected or not.
- They have an ID number as illustrated below.

- They show one of the managed states. See *Sensor/Actuator States* (on page 97).
- For managed 'numeric' sensors, their readings are retrieved and displayed. If any numeric sensor is disconnected or its reading cannot be retrieved, it shows "unavailable" for its reading.

▶ **Unmanaged sensors/actuators:**

- The BCM2 neither communicates with unmanaged sensors/actuators nor retrieves their data.
- Unmanaged sensors/actuators are listed only when they are physically connected to the BCM2. They disappear when they are no longer connected.
- They do *not* have an ID number.
- They show the "unmanaged" state.

Sensor/Actuator States

An environmental sensor or actuator shows its real-time state after being managed.

Available sensor states depend on the sensor type -- numeric or state sensors. For example, a contact closure sensor is a state sensor so it switches between three states only -- *unavailable*, *alarmed* and *normal*.

Sensors will be highlighted in yellow or red when they enter abnormal states. See *Yellow- or Red-Highlighted Sensors* (see "*The Yellow- or Red-Highlighted Sensors*" on page 66, on page 95).

An actuator's state is marked in red when it is turned on.

▶ **Managed sensor states:**

In the following table, "R" represents any numeric sensor's reading. The symbol <= means "smaller than" or "equal to."

State	Description
normal	▪ For numeric sensors, it means the readings are within the normal range. ▪ For state sensors, it means they enter the normal state.
below lower critical	"R" < Lower Critical threshold
below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold

State	Description
above upper critical	Upper Critical threshold < "R"
alarmed	The state sensor enters the abnormal state.
unavailable	▪ The communication with the managed sensor is lost. -- OR -- ▪ DPX2, DPX3 or DX sensor packages are upgrading their sensor firmware.

Note that for a contact closure sensor, the normal state depends on the normal setting you have configured. Refer to the Environmental Sensors Guide or Online Help for detailed information, which is available on Raritan's *Support page* (*http://www.raritan.com/support/*).

▶ **Managed actuator states:**

State	Description
on	The actuator is turned on.
off	The actuator is turned off.
unavailable	▪ The communication with the managed actuator is lost. -- OR -- ▪ DX sensor packages are upgrading their sensor firmware.

▶ **Unmanaged sensor/actuator states:**

State	Description
unmanaged	Sensors or actuators are physically connected to the BCM2 but not managed yet.

Note: Unmanaged sensors or actuators will disappear from the web interface after they are no longer physically connected to the BCM2. To manage a sensor/actuator, go to **Peripherals** *(on page 90).*

Finding the Sensor's Serial Number

A DPX environmental sensor package includes a serial number tag on the sensor cable.

A DPX2, DPX3 or DX sensor package has a serial number tag attached to its rear side.

The serial number for each sensor or actuator appears listed in the web interface after each sensor or actuator is detected by the BCM2. Match the serial number from the tag to those listed in the sensor table.

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1	
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3	
3	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4	
5	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	

Identifying the Sensor Position and Channel

Raritan has developed four types of environmental sensor packages - DPX, DPX2, DPX3 and DX series. Only DPX2, DPX3 and DX sensor packages can be daisy chained.

The BCM2 can indicate where each sensor or actuator is connected on the Peripheral Devices page.

- DPX series only shows the sensor port number only.

  For example, *Port 1*.

- DPX2, DPX3 and DX series show both the sensor port number and its position in a sensor chain.

  For example, *Port 1, Chain Position 2*.

- If a Raritan DPX3-ENVHUB4 sensor hub is involved, the hub port information is also indicated for DPX2, DPX3 and DX series, but NOT indicated for DPX series.

  For example, *Hub Port 3*.

- If a sensor/actuator contains channels, such as a contact closure or dry contact sensor, the channel information is included in the position information.

  For example, *Channel 1*.

▶ **Sensor/actuator position examples:**

Example	Physical position
Port 1	Connected to the sensor port #1.
Port 1, Channel 2	▪ Connected to the sensor port #1. ▪ The sensor/actuator is the 2nd channel of the sensor package.
Port 1, Chain Position 4	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 4th sensor package of the sensor chain.
Port 1, Chain Position 3, Channel 2	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 3rd sensor package of the sensor chain. ▪ It is the 2nd channel of the sensor package.
Port 1, Chain Position 1, Hub Port 2, Chain Position 3	▪ Connected to the sensor port #1. ▪ Connected to the 2nd port of the DPX3-ENVHUB4 sensor hub, which shows the following two pieces of information: 　▪ The hub's position in the sensor chain -- "Chain Position 1" 　▪ The hub port where this particular sensor package is connected -- "Hub Port 2" ▪ The sensor/actuator is located in the 3rd sensor package of the sensor chain connected to the hub's port 2.

Managing One Sensor or Actuator
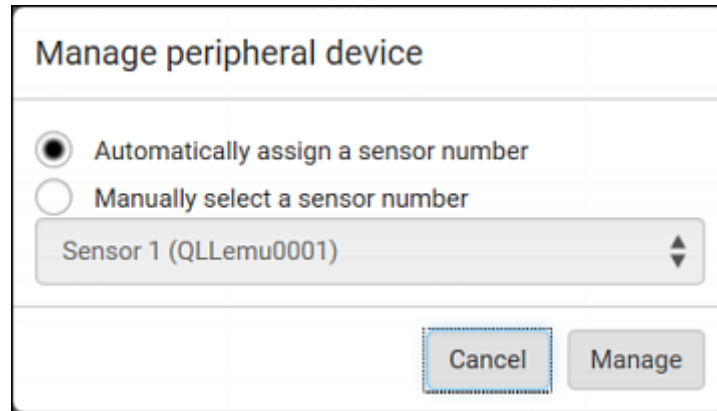
If you are managing only one sensor or actuator, you can assign the desired ID number to it. Note that you cannot assign ID numbers when you are managing multiple sensors/actuators at a time.

Tip: When the total of managed sensors/actuators reaches the maximum (32), you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace any managed ones. To replace a managed one, assign an ID number to it by following this procedure. To release any one, see **Peripherals** *(on page 90).*

▶ **To manage only one sensor/actuator:**

1. From the list of "unmanaged" sensors/actuators, click the one you want to manage.

2. The "Manage peripheral device" dialog appears.

Manage peripheral device

- ● Automatically assign a sensor number
- ○ Manually select a sensor number

Sensor 1 (QLLemu0001)

Cancel   Manage

- To let the BCM2 randomly assign an ID number to it, select "Automatically assign a sensor number."

  This method does not release any managed sensor or actuator.

- To assign the desired ID number to it, select "Manually select a sensor number." Then click [▲▼] to select an ID number.

  This method may release a managed sensor/actuator if the number you selected has been assigned to a specific sensor/actuator.

Tip: The information in parentheses following each ID number indicates whether the number has been assigned to a sensor or actuator. If it has been assigned to a sensor or actuator, it shows its serial number. Otherwise, it shows the word "unused."

3. Click Manage.

▶ **Special note for a Raritan humidity sensor:**

A Raritan humidity sensor is able to provide two measurements - relative and absolute humidity values.

- A relative humidity value is measured in percentage (%).
- An absolute humidity value is measured in grams per cubic meter (g/m^3).

Raritan.
A brand of legrand

However, only relative humidity sensors are "automatically" managed if the automatic management function is enabled. You must "manually" manage absolute humidity sensors as needed.

Note that relative and absolute values of the same humidity sensor do NOT share the same ID number though they share the same serial number and position.

Individual Sensor/Actuator Pages

A sensor's or actuator's data/setup page is opened after clicking any sensor or actuator name on the Peripheral Devices page. See *Peripherals* (on page 90).

Note that only a numeric sensor has threshold settings, while a state sensor or actuator has no thresholds.

Threshold settings, if enabled, help you identify whether any numeric sensor enters the warning or critical level. See *Yellow- or Red-Highlighted Sensors* (see "*The Yellow- or Red-Highlighted Sensors*" on page 66, on page 95). In addition, you can have the BCM2 automatically generate alert notifications for any warning or critical status. See *Event Rules and Actions* (on page 190).

▶ **To configure a numeric sensor's threshold settings:**

1. Click Edit Thresholds.

2. Select or deselect Use Default Thresholds according to your needs.

Sensor		
		Edit Thresholds
Use Default Thresholds	☑	
Lower Critical	☑	10 °C
Lower Warning	☑	15 °C
Upper Warning	☑	57 °C
Upper Critical	☑	68 °C
Deassertion Hysteresis		1 °C
Assertion Timeout		0 Samples
	✖ Cancel	✔ Save

- To have this sensor follow the default threshold settings configured for its sensor type, select the Use Default Thresholds checkbox.

  The default threshold settings are configured on the page of *Peripherals* (on page 90).

- To customize the threshold settings for this particular sensor, deselect the Use Default Thresholds checkbox, and then modify the threshold fields below it.

Note: For concepts of thresholds, deassertion hysteresis and assertion timeout, see Sensor Threshold Settings.

3. Click Save.

▶ **To set up a sensor's or actuator's physical location and additional settings:**

1. Click Edit Settings.

Settings	
	Edit Settings
Name	Temperature 1
Description	
Location (X)	
Location (Y)	
Location (Z: Rack Units)	

2. Make changes to available fields, and then click Save.

Fields	Description
Binary Sensor Subtype	This field is available for a contact closure sensor only. Determine the sensor type of your contact closure detector. ▪ *Contact Closure* detects the door lock or door open/closed status. ▪ *Smoke Detection* detects the appearance of smoke. ▪ *Water Detection* detects the appearance of water on the floor. ▪ *Vibration* detects the vibration of the floor.
Name	A name for the sensor or actuator.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's or actuator's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See *Sensor/Actuator Location Example* (on page 107). If the term "Rack Units" appears in parentheses in the Z location, you must type an integer number. Note that the Z coordinate's format is determined on the page of .
Alarmed to Normal Delay	This field is available for the DX-PIR presence detector only. It determines the wait time before the BCM2 announces that the presence detector is back to normal after it actually returns to normal. Adjust the value in seconds.

▶ **To view a numeric sensor's readings waveform:**

This sensor's data within the past tens of minutes is shown in the waveform diagram. Note that only a numeric sensor has this diagram. State sensors and actuators do not show such data.
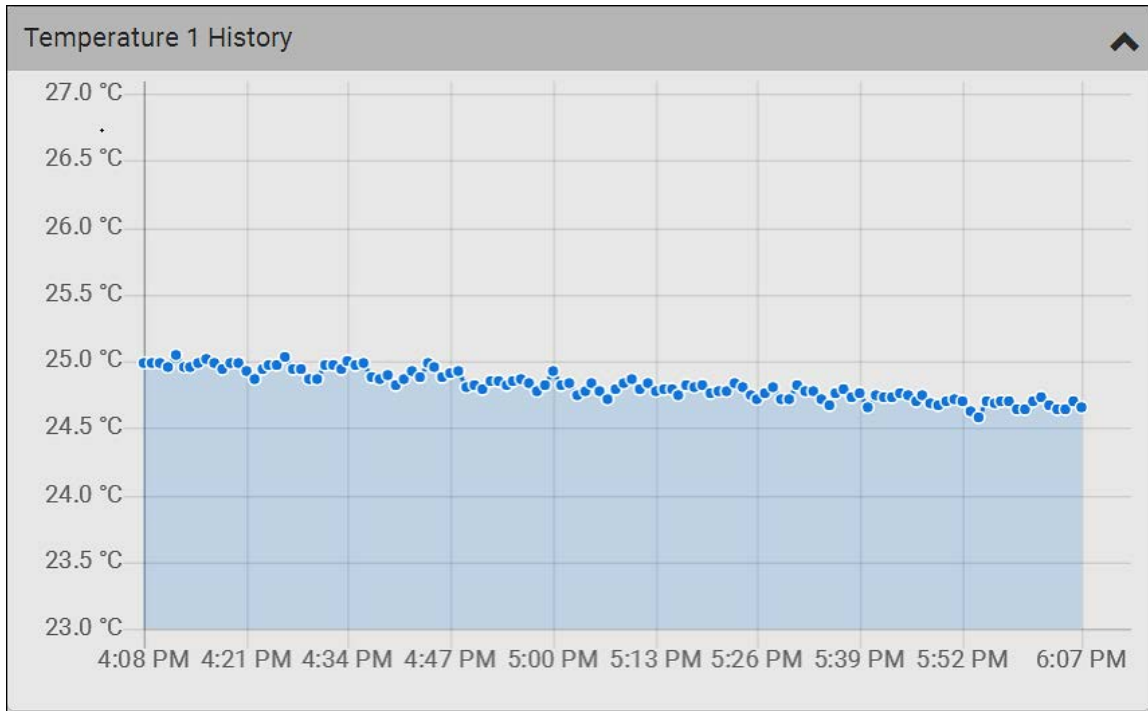
▶ **To turn on or off an actuator:**

1. Click the desired control button.

: Turn ON.

: Turn OFF.

2. Confirm the operation on the confirmation message. An actuator's state is marked in red when it is turned on.

▶ **Other operations:**

You can go to another sensor's or actuators's data/setup page by clicking the selector [⬍] on the top-left corner.

Details	
Peripheral Device ID	1
Position	Port 1
Serial Number	AEH2A51454
Type	Temperature

Sensor/Actuator Location Example

Use the X, Y and Z coordinates to describe each sensor's or actuator's physical location in the data center. See *Individual Sensor/Actuator Pages* (on page 103).

The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. Therefore, you can use non-measurement values.

▶ **Example:**

X = Brown Cabinet Row

Y = Third Rack

Z = Top of Cabinet

▶ **Values of the X, Y and Z coordinates:**

- X and Y: They can be any alphanumeric values comprising 0 to 24 characters.
- Z: When the Z coordinate format is set to *Rack Units*, it can be any number ranging from 0 to 60. When its format is set to *Free-Form*, it can be any alphanumeric value comprising 0 to 24 characters. See .

Feature Port

The FEATURE port supports connection to the following devices.

Device	Description
Asset Strip	Raritan asset strips
External Beeper	An external beeper with the RJ-45 socket.
LHX 20	Schroff® LHX-20 heat exchanger.
SHX 30	Schroff® SHX-30 heat exchanger.
LHX 40	Schroff® LHX-40 heat exchanger.
Power CIM	This type represents one of the following Raritan products: ▪ Raritan power CIM, D2CIM-PWR. This CIM is used to connect the BCM2 to the Raritan digital KVM switch -- Dominion KX II / III. ▪ Dominion KSX II ▪ Dominion SX or SX II

When the BCM2 detects the connection of any listed device, it replaces 'Feature Port' in the menu with that device's name and shows that device's data/settings instead. See *Asset Strip* (on page 110), *External Beeper* (on page 118), *Schroff LHX/SHX* (on page 119) and *Power CIM* (on page 122).

When no devices are detected, the BCM2 displays the name 'Feature Port" and the Feature Port page shows the message "No device is currently connected."

Open the Feature Port page by clicking it in the Menu. From this page, you can enable or disable this port's detection capability, or force it to show a specific device's data/settings even though no device is detected.

Note: You must enable the LHX/SHX support for the BCM2 to detect the presence of a supported Schroff® LHX/SHX heat exchanger. See **Miscellaneous** *(on page 250).*

▶ **To configure the feature port:**

1. Click ⚙ on the top-right corner. The Feature Port Setup dialog appears.

> **Feature Port Setup**
>
> Port: 1
> Device Type: Asset Strip
> Detection Mode:
>
> | Auto | ⬍ |
> |------|---|
>
> Cancel   Save

2. Click the Detection Mode field, and select one mode.

Mode	Description
Auto	Enable the port to automatically detect the device connection.
Disabled	Disable the port's detection capability.

Mode	Description
Asset Strip, Raritan asset strips, LHX 20, SHX 30, LHX 40, Power CIM	Force the BCM2 to show the selected device's data/setup page regardless of the physical connection status.

Note: 'LHX 20', 'SHX 30', and 'LHX 40' are not available when the support of LHX/SHX heat exchangers is disabled. See **Miscellaneous** *(on page 250).*

Asset Strip

After connecting and detecting Raritan asset management strips (asset strips), the BCM2 shows 'Asset Strip' in place of 'Feature Port' in the menu.

Note: For connection instructions, see **Connecting Asset Management Strips** *(see "***Connecting Asset Management Sensors***" on page 46).*

To open the Asset Strip page, click it in the Menu. On this page, you can configure the rack units of asset strips and asset tags. A rack unit refers to a tag port on the asset strips. The "Change Asset Strip Configuration" permission is required.

For the functionality of this icon ⚙ on the top-right corner, see *Feature Port* (on page 108).

▶ **To configure asset strip and rack unit settings:**

1. Click Edit Settings.

Settings	⌃
	Edit Settings
Name	
Number of Rack Units	48
Numbering Mode	Bottom-Up
Numbering Offset	1
Orientation	Bottom Connector

2. Make changes to the settings by directly typing a new value, or clicking that field to select a different option.

Field	Description
Name	Name for this asset strip assembly.
Number of Rack Units	Total of available tag ports on this asset strip assembly, ranging between 8 and 64. - For the current generation of asset strips, which show the suffix "G3" on its hardware label, the BCM2 automatically detects the number of its tag ports (rack units), and you *cannot* change this value. - For old "non-G3" asset strips, there is no automatic detection for them so you must manually adjust this value.
Numbering Mode	The rack unit numbering method in a rack/cabinet. *Top-Down*: The numbering starts from the highest rack unit of a rack/cabinet. *Bottom-Up*: The numbering starts from the lowest rack unit of a rack/cabinet.
Numbering Offset	The start number in the rack unit numbering. For example, if this value is set to 3, then the first number is 3, the second number is 4, and so on.
Orientation	The asset strip's orientation by indicating the location of its RJ-45 connector. *Top Connector*: The RJ-45 connector is located on the top. *Bottom Connector*: The RJ-45 connector is located on the bottom. Asset strips can detect their strip orientation and show it in this field. You need to adjust this value only when your asset strips are the oldest ones without tilt sensors implemented.
Color with connected tag	Click this field to determine the LED color denoting the presence of an asset tag. Default is green.
Color without connected tag	Click this field to determine the LED color denoting the absence of an asset tag. Default is red.

For color settings, there are two ways to set the color.

- Click a color in the color palette.
- Type the hexadecimal RGB value of the color, such as #00FF00.
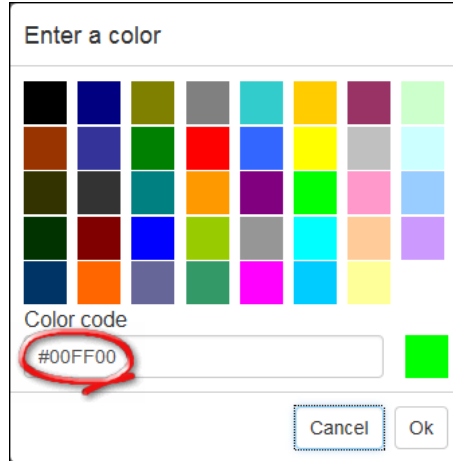
3. Click Ok. The rack unit numbering and LED color settings are immediately updated on the Rack Units list illustrated below.

- The 'Index' number is the physical tag port number printed on the asset strip, which is not configurable. However, its order will change to reflect the latest rack unit numbering.

- A blade extension strip and a *programmable* tag are marked with the word 'programmable' in the Asset/ID column. You can customize their Asset IDs. For instructions, refer to this section's last procedure below.
- If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

▶ **To customize a single rack unit's settings:**

You can make a specific rack unit's LED behave differently from the others on the asset strip, including the LED light and color.

1. Click the desired rack unit on the Rack Units list. The setup dialog for the selected one appears.

Setup of Rack Unit 3

Name

Operation Mode

Auto (based on Tag)

LED Mode

On

LED Color

Cancel   Save

2. Make changes to the information by typing a new value or clicking that field to select a different option.

Field	Description
Name	Name for this rack unit.
	For example, you can name it based on the associated IT device.
Operation Mode	Determine whether this rack unit's LED behavior automatically changes according to the presence and absence of the asset tag.
	▪ *Auto*: The LED behavior varies, based on the asset tag's presence.
	▪ *Manual Override*: This option differentiates this rack unit's LED behavior.

Field	Description
LED Mode	This field is configurable only after the Operation Mode is set to Manual Override. Determine how the LED light behaves for this particular rack unit. ▪ *On*: The LED stays lit. ▪ *Off*: The LED stays off. ▪ *Slow blinking*: The LED blinks slowly. ▪ *Fast blinking*: The LED blinks quickly.
LED Color	This field is configurable only after the Operation Mode is set to Manual Override. Determine what LED color is shown for this rack unit if the LED is lit.

▶ **To expand a blade extension strip:**

A blade extension strip, like an asset strip, has multiple tag ports. An extension strip is marked with a grayer color on the Asset Strip page, and its tag ports list is collapsed by default.
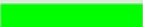
Note: If you need to temporarily disconnect the blade extension strip from the asset strip, wait at least 1 second before re-connecting it back, or the BCM2 device may not detect it.

1. Locate the rack unit (tag port) where the blade extension strip is connected. Click its slot number, whose format is similar to **1-N** ∧, where N is the total number of its tag ports.

2. All tag ports of the blade extension strip are listed below it. Their port numbers are displayed in the Slot column.

Rack Units							
							Program Asset IDs
Rack unit ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	1			000015B914BB	Auto	On	
2	2	1-16 ⌄		0000ABC12345 (programmable)	Auto	On	
	Extension	1		000015B9160A			
	Extension	2		000015B91610			
	Extension	3		000015B91622			
	Extension	4		000015B9158C			
	Extension	5		000015B91600			
	Extension	6		000015B91546			
	Extension	7					
	Extension	8					
	Extension	9					
	Extension	10					
	Extension	11					
	Extension	12					
	Extension	13					
	Extension	14					
	Extension	15					
	Extension	16					
3	3			000015B9152E	Auto	On	
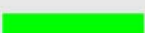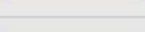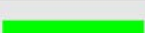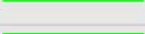
- To hide the blade extension slots list, click **1-N ⌄** .

▶ **To customize asset IDs on programmable asset tags:**

You can customize asset IDs only when the asset tags are "programmable" ones. Non-programmable tags do not support this feature. In addition, you can also customize the ID of a blade extension strip.

If a barcode reader is intended, connect it to the computer you use to access the BCM2.

1. Click Program Asset IDs.

Rack Units							
							Program Asset IDs
Rack unit ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	16				Auto	On	
2	15				Auto	On	
3	14				Auto	On	
4	13				Auto	On	
5	12				Auto	On	
6	11				Auto	On	
7	10			(programmable)	Auto	On	
8	9			(programmable)	Auto	On	
9	8			(programmable)	Auto	On	
10	7			00001492BD47	Auto	On	
11	6			00001492CB50	Auto	On	

2. In the Asset/ID column, enter the customized asset IDs by typing values or scanning the barcode.
   - When using a barcode reader, first click the desired rack unit, and then scan the asset tag. Repeat this step for all desired rack units.

- An asset ID contains up to 12 characters that comprise only numbers and/or UPPER CASE alphabets. Lower case alphabets are NOT accepted.

Rack Units				
				Rack Units
Rack unit ▲	Index	Slot	Name	Asset / ID
1	16			Tag ID
2	15			Tag ID
3	14			Tag ID
4	13			Tag ID
5	12			Tag ID
6	11			Tag ID
7	10			WINDOWS
8	9			LINUX
9	8			ROUTER ✕
10	7			00001492BD47

3. Verify the correctness of customized asset IDs and modify as needed.

4. Click Apply at the bottom of the page or Rack Units (see below) to save changes.

Rack Units				
				Rack Units
Rack unit ▲	Index	Slot	Name	Asset / ID
1	16			Tag ID
2	15			Tag ID

Asset Strip Automatic Firmware Upgrade

After connecting the asset strip to the BCM2, it automatically checks its own firmware version against the version of the asset strip firmware stored in the BCM2 firmware. If two versions are different, the asset strip automatically starts downloading the new firmware from the BCM2 to upgrade its own firmware.

During the firmware upgrade, the following events take place:

- The asset strip is completely lit up, with the blinking LEDs cycling through diverse colors.
- A firmware upgrade process is indicated in the BCM2 web interface.
- An SNMP trap is sent to indicate the firmware upgrade event.

External Beeper

After connecting and detecting a supported external beeper, the BCM2 shows 'External Beeper' in place of 'Feature Port' in the menu.

Note: For connection instructions, see **Connecting an External Beeper** *(on page 55).*

To open the External Beeper page, click it in the Menu. This page shows an external beeper's status, including:

- Number of the FEATURE port where this external beeper is connected
- Its device type
- Its connection status
- The beeper's state - off or active

For the functionality of this icon ⚙ on the top-right corner, see *Feature Port* (on page 108).

Schroff LHX/SHX

You must enable the LHX/SHX support for the BCM2 to detect the presence of a supported Schroff® LHX/SHX heat exchanger. See *Miscellaneous* (on page 250).

After enabling the LHX/SHX support and connecting a supported Schroff® LHX/SHX heat exchanger to the BCM2, the BCM2 shows the connected device type in place of 'Feature Port' in the menu -- LHX 20, LHX 40 or SHX 30.

Note: For connection instructions, see Connecting a Schroff LHX/SHX Heat Exchanger.

To open the LHX/SHX page, click 'LHX 20', 'LHX 40' or 'SHX 30' in the Menu. Then you can monitor and administer the connected LHX/SHX device with the following.

- Name the heat exchanger
- Monitor LHX/SHX built-in sensors and device states
- Configure the air outlet temperature setpoint
- Configure the default fan speed
- Configure the air temperature/fan speed thresholds (for alert generation)
- Request maximum cooling using the fan speed and opening the cold water valve
- Acknowledge alerts or errors remotely, such as failed LHX/SHX sensors or emergency cooling activation
- Accumulative operating hours
- Indicate the number of power supplies present and whether a condenser pump is present

Available information/operation is model dependent. For example, only LHX devices can show sensor alerts. See your LHX/SHX user documentation for details.

Important: The LHX/SHX settings are stored on the port where the LHX/SHX device is connected, and are lost if that device is re-connected to a different BCM2 port.

For the functionality of this icon on the top-right corner, see *Feature Port* (on page 108).

▶ **To view the LHX/SHX device state:**

The Operation State field indicates whether the device is operating fine, and the Switch State field indicates its power status.

If the device does not operate properly, such as some sensor failure, it shows "critical" and the symbol .

▶ **To turn on or off the LHX/SHX device:**

1. Click the desired power-control button on the top-right corner.

    : Power ON.

    : Power OFF.

2. Confirm the operation on the confirmation message.

▶ **To configure LHX/SHX settings:**

1. Click Edit Settings.
2. Configure the settings as needed.
    -   Provide a customized name.
    -   Specify the desired air outlet setpoint temperature.
    -   Specify the default fan speed.
3. Click Save.

▶ **To view all sensor data and configure thresholds:**

1. Locate the Sensors section, which lists all air outlet/inlet temperatures and fan speeds, and indicates the door closed/open status of the LHX/SHX device.
2. To set the thresholds for any temperature or fan speed sensor implemented on the LHX/SHX device:
    a. Click the desired sensor.
    b. Click Edit Thresholds.
    c. Enable and set the desired thresholds and deassertion hysteresis.

        Note that assertion timeout is NOT available on LHX/SHX.
    d. Click Save.

3. After thresholds are enabled, sensors may be highlighted in yellow or red if they enter the warning or critical range. See *Yellow- or Red-Highlighted Sensors* (see "*The Yellow- or Red-Highlighted Sensors*" on page 66, on page 95).

Tip: You can also create event rules to notify you of the warning or critical levels. See **Event Rules and Actions** *(on page 190).*

▶ **To view sensor alerts and LHX event log:**

Remote alert acknowledgment is supported by the LHX-20 and LHX-40. The SHX-30 does not support this feature.

1. Locate the Alert States section.

2. If any LHX sensors fail, they are indicated. Click Acknowledge to acknowledge the sensor failure.

3. To view the history of LHX events, click Show Event Log to go to the Event Log page.

▶ **Operation time statistics:**

This section indicates the accumulative operation hours of the LHX/SHX device and its fans since the device is connected to the BCM2 and turned on.

Available time units in the statistics --

- h: hour(s)
- d: day(s)

▶ **Request maximum cooling:**

Only SHX 30 supports this feature. See *SHX Request Maximum Cooling* (on page 121).

SHX Request Maximum Cooling

The BCM2 allows you to remotely activate the Schroff SHX 30's maximum cooling feature. Both LHX 20 and LHX 40 do not support remote activation of maximum cooling.

The Request Maximum Cooling feature is available only after the BCM2 detects SHX 30. For additional information on the SHX 30 maximum cooling feature, see the SHX 30 documentation.

▶ **To perform maximum cooling:**

- Go to the SHX page, and click Request Maximum Cooling.

  Then the SHX 30 enters into emergency cooling mode and runs at its maximum cooling level of 100% in order to cool the device.

When maximum cooling is requested for an SHX 30, the message "Maximum cooling requested" is displayed.

▶ **To stop maximum cooling:**
- Click Cancel Maximum Cooling.

Power CIM

After connecting and detecting a Raritan power CIM, the BCM2 shows 'Power CIM' in place of 'Feature Port' in the menu. See Dominion KX II / III Configuration or Dominion KSX II, SX or SX II Configuration.

Open the Power CIM page by clicking it in the Menu. This page shows the CIM's status, including:

- Number of the FEATURE port where this CIM is connected
- Its device type
- Its connection status

For the functionality of this icon ⚙ on the top-right corner, see *Feature Port* (on page 108).

User Management

User Management menu deals with user accounts, permissions, and preferred measurement units on a per-user basis.

The BCM2 is shipped with one built-in administrator account: **admin**, which is ideal for initial login and system administrator. You can neither delete 'admin' nor change its permissions.

A "role" determines the tasks/actions a user is permitted to perform on the BCM2 so you must assign one or multiple roles to each user.

Click 'User Management' in the Menu, and the following submenu displays.

Submenu command	Refer to...
Users	*Creating Users* (on page 123)
Roles	*Creating Roles* (see "*Creating a Role*" on page 132, on page 128)
Change Password	*Changing Your Password* (on page 61)
Preferences	*Setting Your Preferred Measurement Units* (on page 130)
Default Preferences	*Setting Default Measurement Units* (on page 131)

Creating Users

All users must have a user account, containing the login name and password. Multiple users can log in simultaneously using the same login name.

To add users, choose User Management > Users >

Note that you must enter information in the fields showing the message 'required.'

▶ **User information:**

Field/setting	Description
User Name	The name the user enters to log in to the BCM2. ▪ 4 to 32 characters ▪ Case sensitive ▪ Spaces are NOT permitted.
Full Name	The user's first and last names.
Password, Confirm Password	▪ 4 to 64 characters ▪ Case sensitive ▪ Spaces are permitted.
Telephone Number	The user's telephone number
eMail Address	The user's email address ▪ Up to 64 characters ▪ Case sensitive
Enable	When selected, the user can log in to the BCM2.

Field/setting	Description
Force password change on next login	When selected, a password change request automatically appears when next time the user logs in. For details, see *Changing Your Password* (on page 61).

▶ **SSH:**

You need to enter the SSH public key only if the public key authentication for SSH is enabled. See *Changing SSH Settings* (on page 162).

1. Open the SSH public key with a text editor.
2. Copy and paste all content in the text editor into the SSH Public Key field.

▶ **SNMPv3:**

The SNMPv3 access permission is disabled by default.

Field/setting	Description
Enable SNMPv3	Select this checkbox when intending to permit the SNMPv3 access by this user. *Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See* **Configuring SNMP Settings** *(on page 159).*
Security Level	Click the field to select a preferred security level from the list: ▪ None: No authentication and no privacy. This is the default. ▪ Authentication: Authentication and no privacy. ▪ Authentication & Privacy: Authentication and privacy.

- **Authentication Password**: This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Same as User Password	Select this checkbox if the authentication password is identical to the user's password. To specify a different authentication password, disable the checkbox.

Field/setting	Description
Password, Confirm Password	Type the authentication password if the 'Same as User Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

- **Privacy Password**: This section is configurable only when 'Authentication & Privacy' is selected.

Field/setting	Description
Same as Authentication Password	Select this checkbox if the privacy password is identical to the authentication password. To specify a different privacy password, disable the checkbox.
Password, Confirm Password	Type the privacy password if the 'Same as Authentication Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

- **Protocol**: This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Authentication	Click this field to select the desired authentication protocol. Two protocols are available: ▪ MD5 ▪ SHA-1 (default)
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: ▪ DES (default) ▪ AES-128

▶ **Preferences:**

This section determines the measurement units displayed in the web interface and command line interface for this user.

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).

Field	Description
Length Unit	Preferred units for length or height -- Meter or Feet.
Pressure Unit	Preferred units for pressure -- Pascal or Psi. ■ Pascal = one newton per square meter ■ Psi = pounds per square inch

Note: Users can change the measurement units at any time by setting their own preferences. See **Setting Your Preferred Measurement Units** *(on page 130).*

▶ **Roles:**

Select one or multiple roles to determine the user's permissions. To select all roles, select the top-most checkbox in the header row.

If the built-in roles do not satisfy your needs, add new roles by clicking
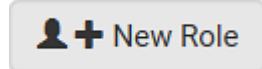
👤➕ New Role. See *Creating Roles* (see "*Creating a Role*" on page 132, on page 128).

The Operator role is assigned to a newly-created user account by default.

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration • Switch Outlet (if your BCM2 is outlet-switching capable) • View Event Settings • View Local Event Log

Note: With multiple roles selected, a user has the union of all roles' permissions.

Editing or Deleting Users

To edit or delete users, choose User Management > Users to open the Users page, which lists all users.

In the Enabled column:

- ✔ : The user is enabled.
- ✖ : The user is disabled.

If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

▶ **To edit or delete a user account:**

1. On the Users page, click the desired user. The Edit User page for that user opens.
2. Make changes as needed.
    - For information on each field, see *Creating Users* (on page 123).
    - To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password remains unchanged.
    - To delete this user, click 🗑, and confirm the operation.
3. Click Save.

▶ **To delete multiple user accounts:**

1. On the Users page, click 🗹 to make checkboxes appear in front of user names.

    Tip: To delete only one user, you can simply click that user without making the checkboxes appear. See the above procedure.

2. Select one or multiple users.
    - To select all roles, except for the admin role, select the top-most checkbox in the header row.
3. Click 🗑.
4. Click Delete on the confirmation message.

Creating Roles

A role is a combination of permissions. Each user must have at least one role.

The BCM2 provides two built-in roles. The Operator role is assigned to a newly-created user account per default. See *Creating Users* (on page 123).

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration • Switch Outlet (if your BCM2 is outlet-switching capable) • View Event Settings • View Local Event Log

If the two do not satisfy your needs, add new roles.

▶ **To create a role:**

1. Choose User Management > Roles > .

2. Assign a role name.
   - 1 to 32 characters long
   - Case sensitive
   - Spaces are permitted as of release 3.3.0
3. Type a description for the role in the Description field.
4. Select the desired privilege(s).
   - The 'Administrator Privileges' includes all privileges.
   - The 'Unrestricted View Privileges' includes all 'View' privileges.

5. To select any privilege requiring the argument setting, click ➕ to select the desired arguments.

   - For example, on an outlet-switching capable model, you can specify the outlets that are allowed to be switched on/off for the 'Switch Outlet' privilege as shown below.
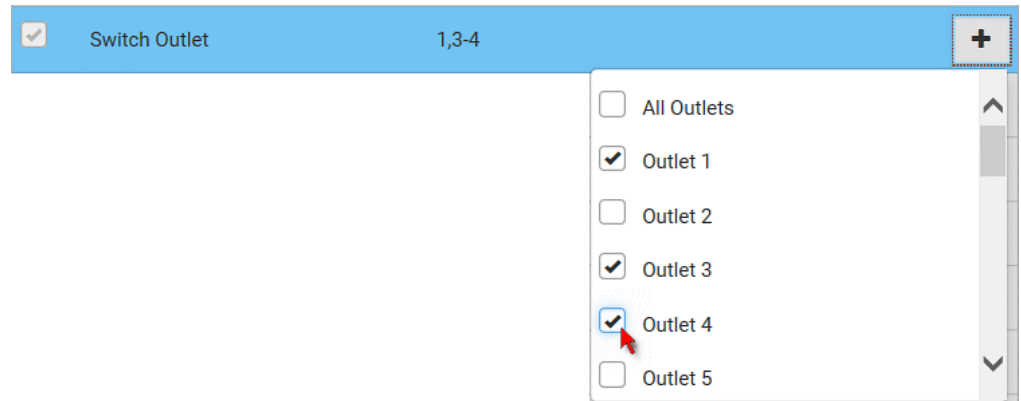
6. Click Save.

Now you can assign the role to any user. See *Creating Users* (on page 123) or *Editing or Deleting Users* (on page 127).

Editing or Deleting Roles

Choose User Management > Roles to open the Roles page, which lists all roles.

If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

The Admin role is not user-configurable so the lock icon 🔒 displays, indicating that you are not allowed to configure it.

▶ **To edit a role:**

1. On the Roles page, click the desired role. The Edit Role page opens.
2. Make changes as needed.
   - The role name cannot be changed.
   - To delete this role, click 🗑, and confirm the operation.
3. Click Save.

▶ **To delete any roles:**

1. On the Roles page, click 🗹 to make checkboxes appear in front of roles.

129

Tip: To delete only one role, you can simply click that user without making the checkboxes appear. See the above procedure.

2. Select one or multiple roles.
   - To select all roles, except for the Admin role, select the top-most checkbox in the header row.
3. Click ![trash icon] on the top-right corner.
4. Click Delete on the confirmation message.

Setting Your Preferred Measurement Units

You can change the measurement units shown in the BCM2 user interface according to your own preferences regardless of the permissions you have.

Tip: Preferences can also be changed by administrators for specific users on the Edit User page. See **Editing or Deleting Users** *(on page 127).*

Measurement unit changes only apply to the web interface and command line interface.

Setting your own preferences does not change the default measurement units. See *Setting Default Measurement Units* (on page 131).

▶ **To select the measurement units you prefer:**

1. Choose User Management > Preferences.
2. Make changes as needed.

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length Unit	Preferred units for length or height -- Meter or Feet.
Pressure Unit	Preferred units for pressure -- Pascal or Psi. ▪ Pascal = one newton per square meter ▪ Psi = pounds per square inch

3. Click Save.

Setting Default Measurement Units

Default measurement units are applied to all BCM2 user interfaces across all users, including users accessing the BCM2 via external authentication servers. For a list of affected user interfaces, see *User Interfaces Showing Default Units* (on page 131). The front panel display also shows the default measurement units.

Note: The preferred measurement units set by any individual user or by the administrator on a per-user basis will override the default units in the web interface and command line interface. See **Setting Your Preferred Measurement Units** *(on page 130) or* **Creating Users** *(on page 123).*

▶ **To set up default user preferences:**

1. Click User Management > Default Preferences.
2. Make changes as needed.

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length Unit	Preferred units for length or height -- Meter or Feet.
Pressure Unit	Preferred units for pressure -- Pascal or Psi. ▪ Pascal = one newton per square meter ▪ Psi = pounds per square inch

3. Click Save.

User Interfaces Showing Default Units

Default measurement units will apply to the following user interfaces or information:

- Web interface for "newly-created" local users when they have not configured their own preferred measurement units. See *Creating Users* (on page 123).
- Web interface for users who are authenticated via LDAP/Radius servers.
- The sensor report sent because of the "Send Sensor Report" action. See *Send Sensor Report* (on page 215).
- Front panel LCD display.

Setting Up Roles

A role defines the operations and functions a user is permitted to perform or access. Every user must be assigned at least a role.

The BCM2 is shipped with two built-in roles: **Admin** and **Operator**.

- The Admin role provides full permissions. You can neither modify nor delete this role.
- The Operator role provides limited permissions for frequently-used functions. You can modify or delete this role. By default, the Operator role contains these permissions:
  - Change PMC, PMB, & PMM Configuration
  - Acknowledge Alarms
  - View Event Settings
  - View Local Event Log
  - Change Own Password

  The Operator role is assigned to a newly created user profile by default. See *Creating a User Profile* (see "*Creating Users*" on page 123).

Permissions

- Change PMC, PMB, & PMM Configuration
  - Configuring, editing, and deleting a power meter
  - Configuring, editing, and deleting a panel (BCM)
  - Creating, editing and deleting a circuit
  - Reset active energy counters
- Acknowledge Alarms
- View Event Settings
- View Local Event Log
- Change Own Password

Creating a Role

Create a new role when you need a new combination of permissions.

▶ **To create a role:**

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.

3. Type the role's name in the Role Name field.

4. Type a description for the role in the Description field.

5. Click the Privileges tab to assign one or multiple permissions.

    a. Click Add. The "Add Privileges to new Role" dialog appears.

    b. Select the permission you want from the Privileges list.

    c. If the permission you selected contains any argument setting, the Arguments list is shown to the right, such as the Switch Actuator permission. Then select one or multiple arguments.

    d. Click Add to add the selected permission (and arguments if any).

    e. Repeat Steps *a* to *d* until you add all necessary permissions.

6. Click OK.

Now you can assign the new role to any users. See *Creating a User Profile* (see "*Creating Users*" on page 123) or *Modifying a User Profile* (see "*Editing or Deleting Users*" on page 127).

Modifying a Role

You can change an existing role's settings except for the name.

▶ **To modify a role:**

1. Choose User Management > Roles. The Manage Roles dialog appears.

    Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to modify by clicking it.

3. Click Edit or double-click the role. The Edit Role 'XXX' dialog appears, where XXX is the role name.

    Tip: You can also access the Edit Role 'XXX' dialog by clicking the Edit Role button in the Edit User 'XXX' dialog.

4. Modify the text shown in the Description field if necessary.

5. To change the permissions, click the Privileges tab.

    Note: You cannot change the Admin role's permissions.

6. To delete any permissions, do this:

    a. Select the permission you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

    b. Click Delete.

7. To add any permissions, do this:

a. Click Add. The "Add Privileges to Role XXX" dialog appears, where XXX is the role name.

b. Select the permission you want from the Privileges list.

c. If the permission you selected contains any argument setting, the Arguments list is shown to the right, such as the Switch Actuator permission. Then select one or multiple arguments.

d. Click Add to add the selected permission (and arguments if any).

e. Repeat Steps *a* to *d* until you add all necessary permissions.

8. To change a specific permission's arguments, do this:

a. Select the permission by clicking it.

b. Click Edit. The "Edit arguments of privilege XXX" dialog appears, where XXX is the privilege name.

Note: If the permission you selected does not contain any arguments, the Edit button is disabled.

c. Select the argument you want. You can make multiple selections.

d. Click OK.

9. Click OK.

Device Settings

Click 'Device Settings' in the Menu, and the following submenu displays.

Menu command	Submenu command	Refer to...
Network		*Configuring Network Settings* (on page 135)
Network Services	HTTP	*Changing HTTP(S) Settings* (on page 158)
	SNMP	*Configuring SNMP Settings* (on page 159)
	SMTP Server	*Configuring SMTP Settings* (on page 160)
	SSH	*Changing SSH Settings* (on page 162)
	Telnet	*Changing Telnet Settings* (on page 162)
	Modbus	*Changing Modbus Settings* (on page 163)
	Server Advertising	*Enabling Service Advertising* (on page 164)
Security	IP Access Control	*Creating IP Access Control Rules* (on page 165)
	Role Access Control	*Creating Role Access Control Rules* (on page 168)
	SSL Certificate	*Setting Up an SSL/TLS Certificate* (on page 170)
	Authentication	*Setting Up External Authentication* (on page 175)

Menu command	Submenu command	Refer to...
	Login Settings	*Configuring Login Settings* (on page 184)
	Password Policy	*Configuring Password Policy* (on page 185)
	Service Agreement	*Enabling the Restricted Service Agreement* (on page 186)
Date/Time		*Setting the Date and Time* (on page 187)
Event Rules		*Event Rules and Actions* (on page 190)
Data Logging		*Setting Data Logging* (on page 235)
Data Push		*Configuring Data Push Settings* (on page 236)
Server Reachability		*Monitoring Server Accessibility* (on page 238)
Front Panel*		*Front Panel Settings* (on page 242)
Serial Port		*Configuring the Serial Port* (on page 243)
Lua Scripts		*Lua Scripts* (on page 245)
Miscellaneous		*Miscellaneous* (on page 250)

* The availability of "Front Panel" depends on the model.

Configuring Network Settings

Configure wired, wireless, and Internet protocol-related settings on the Network page after connecting the BCM2 to your network.

You can enable both the wired and wireless networking on the BCM2 so that it has multiple IP addresses -- wired and wireless IP. For example, you can obtain one IPv4 and/or IPv6 address by enabling one Ethernet interface, and obtain one more IPv4 and/or IPv6 address by enabling/configuring the wireless interface. This also applies when the BCM2 enters the port forwarding mode so that the BCM2 has more than one IPv4 or IPv6 address in the port forwarding mode.

However, the BCM2 in the BRIDGING mode obtains "only one" IP address for wired networking. Wireless networking is NOT supported in this mode.

Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

▶ **To set up the network settings:**
1. Choose Device Settings > Network.

2. To use DHCP-assigned DNS servers and gateway instead of static ones, go to step 3. To manually specify DNS servers and default gateway, configure the Common Network Settings section. See *Common Network Settings* (on page 138).

   ▪ Static routes and cascading mode are in this section. You need to configure them only when there are such local requirements. See *Setting the Cascading Mode* (on page 149) and *Static Route Examples* (on page 145).

3. To configure IPv4/IPv6 settings for a *wired* network, click the ETHERNET or BRIDGE section. See *Wired Network Settings* (on page 137).

   ▪ If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings.

4. To configure IPv4/IPv6 settings for a *wireless* network, click the WIRELESS section. See *Wireless Network Settings* (on page 140).

   ▪ You must connect a USB wireless LAN adapter to the BCM2 for wireless networking.

   Note: If the device's cascading mode is set to 'Bridging' or its role is set to 'Slave' in the port forwarding mode, the wireless settings will be disabled.

5. To configure the ETHERNET interface settings, see *Ethernet Interface Settings* (on page 139).

6. Click Save.

▶ **After enabling either or both Internet protocols:**

After enabling IPv4 and/or IPv6, all but not limited to the following protocols will be compliant with the selected Internet protocol(s):

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL/TLS
- SNMP
- SysLog

Note: The BCM2 supports TLS 1.0, 1.1 and 1.2.

Wired Network Settings

On the Network page, click the ETHERNET section to configure IPv4/IPv6 settings.

If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings. See *Setting the Cascading Mode* (on page 149).

▶ **Enable Interface:**

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETHERNET section, but not available in the BRIDGE section.

Enable Interface	✔

▶ **IPv4 settings:**

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP Auto Configuration	Select the method to configure IPv4 settings. ▪ DHCP: Auto-configure IPv4 settings via DHCP servers. ▪ Static: Manually configure the IPv4 settings.

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
  - ▪ Consists of alphanumeric characters and/or hyphens
  - ▪ Cannot begin or end with a hyphen
  - ▪ Cannot contain more than 63 characters
  - ▪ Cannot contain punctuation marks, spaces, and other symbols
- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".
  - Example: *192.168.84.99/24*

▶ **IPv6 settings:**

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP Auto Configuration	Select the method to configure IPv6 settings. ▪ Automatic: Auto-configure IPv6 settings via DHCPv6.

Field/setting	Description
	▪ Static: Manually configure the IPv6 settings.

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

    Example: *fd07:2fa:6cff:1111::0/128*

Common Network Settings

Common Network Settings are OPTIONAL, not required. Therefore, leave them unchanged if there are no specific local networking requirements.

Field	Description
Cascading Mode	Leave it to the default "None" unless you are establishing a cascading chain. For more information, refer to: ▪ Cascading Multiple BCM2 Devices for Sharing Ethernet Connectivity ▪ *Setting the Cascading Mode* (on page 149)
DNS Resolver Reference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. ▪ IPv4 Address: Use the IPv4 addresses. ▪ IPv6 Address: Use the IPv6 addresses.
DNS Suffixes (optional)	Specify a DNS suffix name if needed.
First/Second/Third DNS Server	Manually specify static DNS server(s). ▪ If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. ▪ If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the BCM2 will use DHCP-assigned DNS servers.

Field	Description
IPv4/IPv6 Routes	You need to configure these settings only when your local network contains two subnets, and you want BCM2 to communicate with the other subnet.
	If so, make sure IP forwarding has been enabled in your network, and then you can click 'Add Route' to add static routes.
	See *Static Route Examples* (on page 145).

Ethernet Interface Settings

By default the Ethernet interface is enabled.

▶ **Enable Interface:**

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETHERNET section, but not available in the BRIDGE section.

Enable Interface	☑

▶ **Other Ethernet settings:**

Field	Description
Speed	Select a LAN speed.
	• Auto: System determines the optimum LAN speed through auto-negotiation.
	• 10 MBit/s: Speed is always 10 Mbps.
	• 100 MBit/s: Speed is always 100 Mbps.
Duplex	Select a duplex mode.
	• Auto: The BCM2 selects the optimum transmission mode through auto-negotiation.
	• Full: Data is transmitted in both directions simultaneously.
	• Half: Data is transmitted in one direction (to or from the BCM2 device) at a time.

Field	Description
Current State	Show the LAN's current status, including the current speed and duplex mode.

Note: Auto-negotiation is disabled after setting both the speed and duplex settings of the BCM2 to NON-Auto values, which may result in a duplex mismatch.

Wireless Network Settings

If the device's cascading mode is set to 'Bridging' or its role is set to 'Slave' in the port forwarding mode, the wireless settings will be disabled. See *Setting the Cascading Mode* (on page 149).

By default the wireless interface is disabled. You should enable it if wireless networking is wanted.

▶ **Interface Settings:**

Field/setting	Description
Enable Interface	Enable or disable the wireless interface. When disabled, the wireless networking fails.
Hardware State	Check this field to ensure that the BCM2 device has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported.
SSID	Type the name of the wireless access point (AP)
Force AP BSSID	If the BSSID is available, select this checkbox
BSSID	Type the MAC address of an access point
Enable High Throughput (802.11n)	Enable or disable 802.11n protocol.

Raritan.
A brand of ❑legrand

Field/setting	Description
Authentication	Select an authentication method. ▪ No Authentication: No authentication data is required. ▪ PSK: A Pre-Shared Key is required. ▪ EAP - PEAP: Use Protected Extensible Authentication Protocol. Only MSCHAPv2 is supported. Enter required authentication data in the fields that appear.
Pre-Shared Key	This field appears only when PSK is selected. Type the PSK string
Identity	This field appears only when 'EAP - PEAP' is selected. Type your user name.
Password	This field appears only when 'EAP - PEAP' is selected. Type your password.
CA Certificate	This field appears only when 'EAP - PEAP' is selected. A third-party CA certificate may or may not be needed. If needed, follow the steps below.

- **Available settings for the CA Certificate:**

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the BCM2 to verify the validity of the TLS certificate that will be installed. ▪ For example, the BCM2 will check the certificate's validity period against the system time.
Browse...	Click this button to install a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.

Field/setting	Description
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow wireless connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the BCM2 system time is earlier than the firmware build before synchronizing with any NTP server. • The incorrect system time issue may occur when the BCM2 has once been powered off for a long time.

▶ **IPv4 settings:**

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP Auto Configuration	Select the method to configure IPv4 settings. • DHCP: Auto-configure IPv4 settings via DHCP servers. • Static: Manually configure the IPv4 settings.

• **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
  ▪ Consists of alphanumeric characters and/or hyphens
  ▪ Cannot begin or end with a hyphen
  ▪ Cannot contain more than 63 characters
  ▪ Cannot contain punctuation marks, spaces, and other symbols
• **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".
  Example: *192.168.84.99/24*

▶ **IPv6 settings:**

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP Auto Configuration	Select the method to configure IPv6 settings. ▪ Automatic: Auto-configure IPv6 settings via DHCPv6. ▪ Static: Manually configure the IPv6 settings.

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

    Example: *fd07:2fa:6cff:1111::0/128*

▶ **(Optional) To view the wireless LAN diagnostic log:**

- Click Show WLAN Diagnostic Log. See *Wireless LAN Diagnostic Log* (on page 143).

Wireless LAN Diagnostic Log

The BCM2 provides a diagnostic log for inspecting connection errors that occurred over the wireless network interface. The information is useful for technical support.

Note that the WLAN Diagnostic Log shows data only after the Network Interface is set to Wireless.

Each entry in the log consists of:

- ID number
- Date and time
- Description

▶ **To view the log:**

1. Choose Device Settings > Network > WIRELESS > Show WLAN Diagnostic Log. See *Configuring Network Settings* (on page 135).
2. To go to other pages of the log, click the pagination bar at the bottom of the page.

- If there are more than 5 pages and the page numbers displayed

  in the bar does not show the desired one, click [...] to have it show the next or previous five page numbers, if available.

| First | Previous | 1 | 2 | 3 | 4 | 5 | ... | Next | Last |

3. To refresh the diagnostic, click ⟳ **Refresh** on the top-right corner.
4. If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

▶ **To clear the diagnostic log:**

1. On the top-right corner of the log, click ⋮ > 🗑 Clear Log.
2. Click Clear Log on the confirmation message.

Raritan.
A brand of legrand

Static Route Examples

This section describes two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and BCM2 devices in the examples use static IP addresses.

Most of local multiple networks are not directly reachable and require the use of a gateway. Therefore, we will select Gateway in the following examples. If your local multiple networks are directly reachable, you should select Interface rather than Gateway.

Note: If Interface is selected, you should select an interface name instead of entering an IP address. See **Interface Names** *(on page 148).*

▶ **IPv4 example:**
- Your BCM2: *192.168.100.64*
- Two NICs: *192.168.200.75* and *192.168.100.88*
- Two networks: *192.168.200.0* and *192.168.100.0*
- Subnet mask: *24*
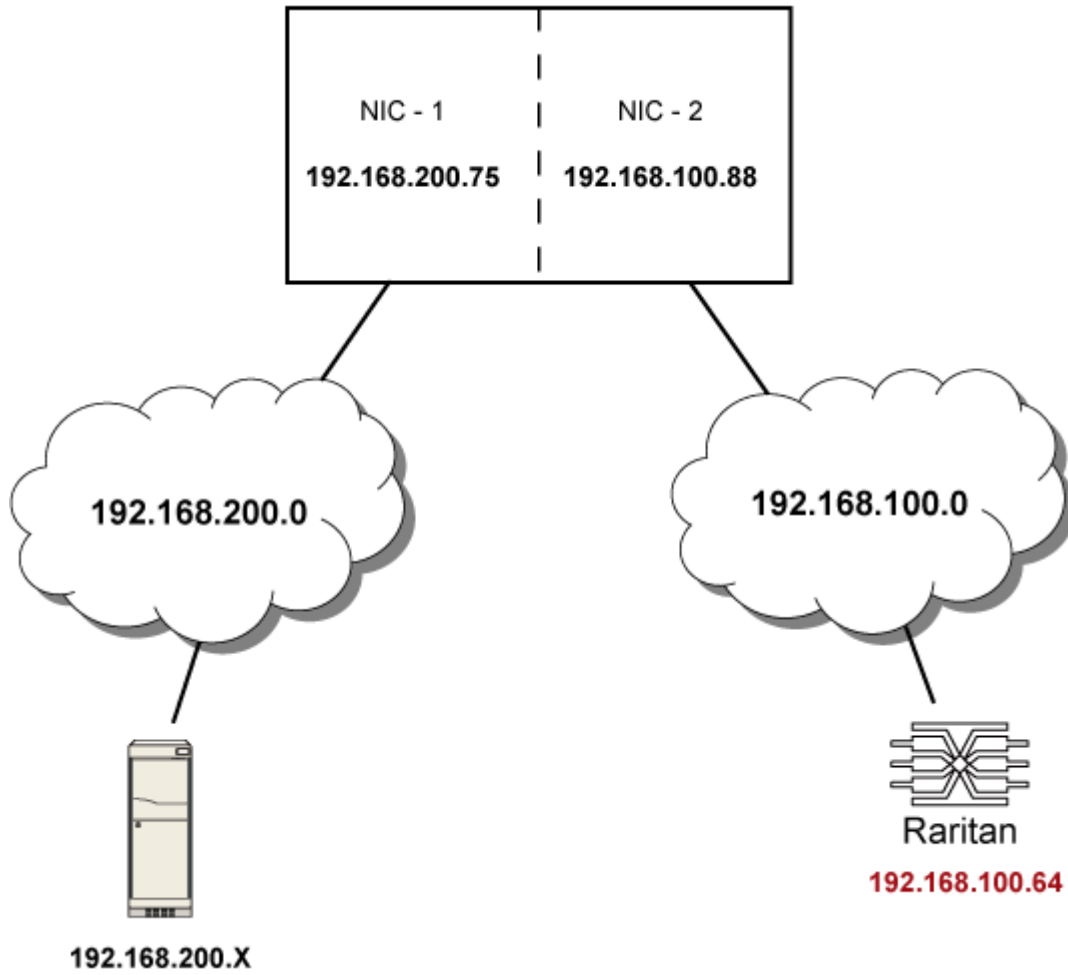
In this example, NIC-2 (192.168.100.88) is the next hop router for your
BCM2 to communicate with any device in the other subnet 192.168.200.0.
In the IPv4 "Static Routes" section, you should specify:

1	192.168.200.0/24	Gateway	192.168.100.88	↑ ↓ 🗑

Raritan.
A brand of legrand

Tip: If you have configured multiple static routes, you can click on any route and then make changes, use ⬆ *or* ⬇ *to re-sort the priority, or click* 🗑 *to delete it.*

▶ **IPv6 example:**

- Your BCM2: *fd07:2fa:6cff:2405::30*
- Two NICs: *fd07:2fa:6cff:1111::50* and *fd07:2fa:6cff:2405::80*
- Two networks: *fd07:2fa:6cff:1111::0* and *fd07:2fa:6cff:2405::0*
- Prefix length: *64*
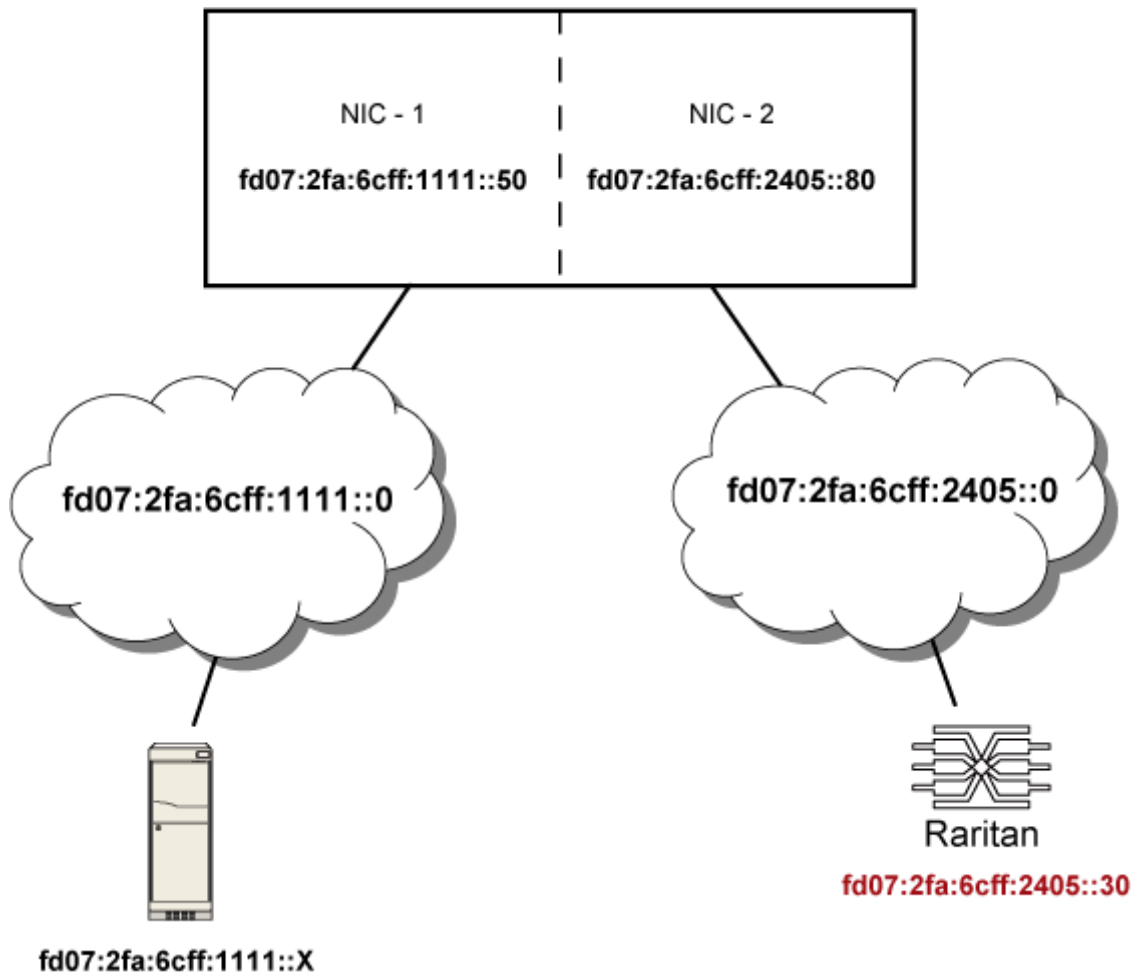
In this example, NIC-2 (fd07:2fa:6cff:2405::80) is the next hop router for your BCM2 to communicate with any device in the other subnet fd07:2fa:6cff:1111::0. In the IPv6 "Static Routes" section, you should specify:

| 1 | fd07:2fa:6cff:2405::0/64 | Gateway | fd07:2fa:6cff:2405::80 ✕ |

Tip: If you have configured multiple static routes, you can click on any route and then make changes, use ⬆ or ⬇ to re-sort the priority, or click 🗑 to delete it.

Interface Names

When your local multiple networks are "directly reachable", you should select Interface for static routes. Then choose the interface where another network is connected.

| 192.168.200.0/24 | Interface | BRIDGE
ETHERNET
WIRELESS |

▶ **Interface list for BCM2:**

Interface name	Description
BRIDGE	When another wired network is connected to the Ethernet port of your BCM2, and your BCM2 has been set to the bridging mode, select this interface name instead of the Ethernet interface.
ETHERNET	When another wired network is connected to the Ethernet port of your BCM2, select this interface name.
WIRELESS	When another wireless network is connected to your BCM2, select this interface name.

▶ **Interface list for BCM2-iX7:**

Interface name	Description
BRIDGE	When another wired network is connected to the Ethernet port of your BCM2, and your BCM2 has

Raritan.
A brand of ◻legrand®

Interface name	Description
	been set to the bridging mode, select this interface name instead of the Ethernet interface.
ETH1	When another wired network is connected to the ETH1 port of your BCM2, select this interface name.
ETH2	When another wired network is connected to the ETH2 port of your BCM2, select this interface name.
WIRELESS	When another wireless network is connected to your BCM2, select this interface name.

Setting the Cascading Mode

A maximum of 16 BCM2 devices can be cascaded to share one Ethernet connection. See Cascading Multiple BCM2 Devices for Sharing Ethernet Connectivity.

The cascading mode configured on the master device determines the Ethernet sharing method, which is either network bridging or port forwarding. See *Overview of the Cascading Modes* (on page 151).

Only a user with the Change Network Settings can configure the cascading mode.

Note: The BCM2 in the Port Forwarding mode does not support APIPA. See APIPA and Link-Local Addressing.

▶ **To configure the cascading mode:**

1. Connect the device that you will cascade to the LAN and find its IP address, or connect it to a computer.
   - For the computer connection instructions, see Connecting the BCM2 to a Computer.
   - To find the IP address, see Device Info.
2. Log in to its web interface.
3. Choose Device Settings > Network.
4. Select the preferred mode in the Cascading Mode field.
   - None: No cascading mode is enabled. This is the default.
   - Bridging: Each device in the cascading chain is accessed with a different IP address.

- Port Forwarding: Each device in the cascading chain is accessed with the same IP address but with a different port number assigned. For details on port numbers, see *Port Number Syntax* (on page 152).

Tip: If selecting Port Forwarding, the Device Information page will show a list of port numbers for all cascaded devices.

5. For the port forwarding mode, one to two more fields have to be configured. Note that if either setting is incorrectly configured, a networking issue occurs.
   - Role: Master or Slave. This is to determine which device is the master and which ones are slave devices.
   - Downstream interface: USB or Ethernet. This is to determine which port of the master device is connected to Slave 1.

6. Now you can configure the network settings.
   - Bridging mode: Click the BRIDGE section on the same page.
   - Port forwarding mode: Click the ETHERNET or WIRELESS section on the same page, depending on the networking method you prefer.

7. Click Save.

For information on accessing each cascaded device in the Port Forwarding mode, see *Port Forwarding Examples* (on page 154).

For information on wired or wireless network settings, see *Wired Network Settings* (on page 137) or *Wireless Network Settings* (on page 140).

Special application: You can "loop" a cascading chain to create network communication redundancy (bridging mode only), but only when your network supports R/STP protocol. Make sure that your network has R/STP enabled if using a cascade loop (bridging mode) or else network loops may occur.

▶ **Online USB-cascading information:**

For more information on the USB-cascading configuration, see the *Cascading Guide*, which is available from Raritan website's *Support page* (*http://www.raritan.com/support/*).

Overview of the Cascading Modes

You must apply a cascading mode to the cascading configuration. See *Setting the Cascading Mode* (on page 149).

▶ **Overview:**

- The Bridging mode supports the wired network only, while the Port Forwarding mode supports both wired and wireless networks.
- All cascading modes support a maximum of 16 devices in a chain.
- All cascading modes support both DHCP and static IP addressing.
- In the Bridging mode, each cascaded device has a unique IP address. In the Port Forwarding mode, all cascaded devices share the same IP address.
- Each cascaded device can be remotely accessed through the network regardless of the cascading mode.

▶ **Illustration:**

In the following diagrams, it is assumed that users enable the DHCP networking in the cascading configuration comprising four devices. "M" is the master device and "S" is the slave device.

- **"Bridging" mode:**

In this mode, the DHCP server communicates with every cascaded device respectively and assigns four *different* IP addresses. Each device has its own IP address. The way to remotely access each cascaded device is completely the same as accessing a standalone device in the network.
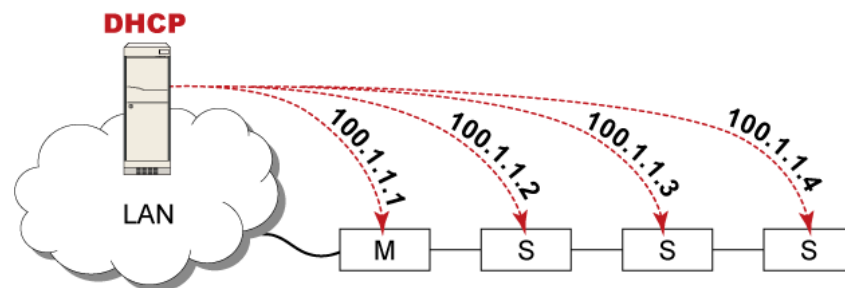
- **"Port Forwarding" mode:**

  In this mode, the DHCP server communicates with the master device alone and assigns only one IP address. All slave devices share the same IP address as the master device. You must specify a 5XXXX port number (where X is a number) when remotely accessing any slave device via the shared IP address. See *Port Number Syntax* (on page 152).
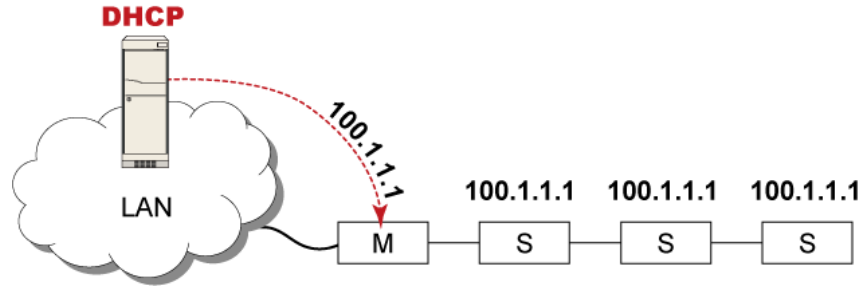
Port Number Syntax

In the Port Forwarding mode, all devices in the USB-cascading configuration share the same IP address. To access any cascaded device, you must assign an appropriate port number to it.

- Master device: The port number is either *5NNXX* or the standard TCP/UDP port.

- Slave device: The port number is *5NNXX*.

▶ **5NNXX port number syntax:**

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

Protocols	NN
HTTPS	00
HTTP	01
SSH	02
TELNET	03
SNMP	05
MODBUS	06

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

  The following table only lists 7 slave devices, but the port forwarding supports up to 15 slave devices.

Position	XX
Master device	00
Slave 1	01
Slave 2	02
Slave 3	03
Slave 4	04
Slave 5	05
Slave 6	06
Slave 7	07

For example, to access the Slave 4 device via Modbus/TCP, the port number is 50604. See *Port Forwarding Examples* (on page 154) for further illustrations.

Tip: The full list of each cascaded device's port numbers can be retrieved from the web interface. Choose Maintenance > Device Information > Port Forwarding.

▶ **Standard TCP/UDP ports:**

The master device can be also accessed through standard TCP/UDP ports as listed in the following table.

Protocols	Port Numbers
HTTPS	443
HTTP	80
SSH	22
TELNET	23
SNMP	161
MODBUS	502

In the Port Forwarding mode, the BCM2 does NOT allow you to modify the standard TCP/UDP port configuration, including HTTP, HTTPS, SSH, Telnet and Modbus/TCP.

Port Forwarding Examples

To access a cascaded device in the Port Forwarding mode, assign a port number to the IP address.

- Master device: Assign proper 5NNXX port numbers or standard TCP/UDP ports. See *Port Number Syntax* (on page 152) for details.
- Slave device: Assign proper 5NNXX port numbers.

Assumption: *The Port Forwarding mode is applied to a USB-cascading configuration comprising three Raritan devices. The IP address is 192.168.84.77.*

▶ **Master device:**

Position code for the master device is '00' so each port number is 5NN00 as listed below.

Protocols	Port numbers
HTTPS	50000
HTTP	50100
SSH	50200
TELNET	50300
SNMP	50500
MODBUS	50600

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

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

▶ **Slave 1 device:**

Position code for Slave 1 is '01' so each port number is 5NN01 as shown below.

Protocols	Port numbers
HTTPS	50001
HTTP	50101
SSH	50201
TELNET	50301
SNMP	50501
MODBUS	50601

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 Slave 2 is '02' so each port number is 5NN02 as shown below.

Protocols	Port numbers
HTTPS	50002
HTTP	50102
SSH	50202
TELNET	50302
SNMP	50502
MODBUS	50602

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:

  http://192.168.84.77:50102/

- To access Slave 2 via SSH, the command is:

  ssh -p 50202 192.168.84.77

Adding, Removing or Swapping Cascaded Devices

Change the cascading mode first before adding any device to a cascading chain, or before disconnecting a cascaded device from the chain.

If you only want to change the cascading mode of an existing chain, or swap the master and slave device, always start from the slave device.

Note: If the following procedures are not followed, a networking issue occurs. When a networking issue occurs, check the cascading connection and/or software settings of all devices in the chain. See **Cascading Troubleshooting** *(on page 483).*

▶ **To add a device to an existing chain:**

1. Connect the device that you will cascade to the LAN and find its IP address, or connect it to a computer.

2. Log in to this device and set its cascading mode to be the same as the existing chain's cascading mode. See *Setting the Cascading Mode* (on page 149).

3. Connect it to the chain, using either USB or Ethernet cable.

▶ **To remove a device from the chain:**

1. Log in to the desired cascaded device, and change its cascading mode to None.

   Exception: If you are going to connect the removed device to another cascading chain, set its cascading mode to be the same as the cascading mode of another chain.

2. Now disconnect it from the cascading chain.

▶ **To swap the master and slave device:**

- In the bridging mode, you can swap the master and slave devices by simply disconnecting ALL cascading cables from them, and then reconnecting cascading cables. No changes to software settings are required.

- In the port forwarding mode, you must follow the procedure below:

  a. Access the slave device that will replace the master device, and set its role to 'Master', and correctly set the downstream interface.

  b. Access the master device, set its role to 'Slave'.

    c. Swap the master and slave device now. You must disconnect ALL cascading cables connected to the two devices first before swapping them and reconnecting cascading cables.

▶ **To change the cascading mode applied to a chain:**

1. Access the last slave device, and change its cascading mode.

   ▪ If the new cascading mode is 'Port Forwarding', you must also set its role to 'Slave'.

2. Access the second to last, third to last and so on until the first slave device to change their cascading modes one by one.

3. Access the master device, and change its cascading mode.

   ▪ If the new cascading mode is 'Port Forwarding', you must also set its role to 'Master', and correctly select the downstream interface.

Configuring Network Services

The BCM2 supports the following network communication services.

HTTPS and HTTP enable the access to the web interface. Telnet and SSH enable the access to the command line interface. See *Using the Command Line Interface* (on page 279).

By default, SSH is enabled, Telnet is disabled, and all TCP ports for supported services are set to standard ports. You can change default settings if necessary.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure.

Submenu command	Refer to
HTTP	*Changing HTTP(S) Settings* (on page 158)
SNMP	*Configuring SNMP Settings* (on page 159)
SMTP Server	*Configuring SMTP Settings* (on page 160)
SSH	*Changing SSH Settings* (on page 162)
Telnet	*Changing Telnet Settings* (on page 162)
Modbus	*Changing Modbus Settings* (on page 163)
Service Advertising	*Enabling Service Advertising* (on page 164)

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

Changing HTTP(S) Settings

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the BCM2 so it is a more secure protocol than HTTP. The BCM2 supports TLS *1.0*, *1.1* and *1.2*.

By default, any access to the BCM2 via HTTP is automatically redirected to HTTPS. You can disable this redirection if needed.

▶ **To change HTTP or HTTPS port settings:**

1. Choose Device Settings > Network Services > HTTP.
2. Enable either or both protocols by selecting the corresponding 'Enable' checkbox.
3. To use a different port for HTTP or HTTPS, type a new port number.

   Warning: Different network services cannot share the same TCP port.

4. To redirect the HTTP access to the BCM2 to HTTPS, select the "Redirect HTTP connections to HTTPS."

   ▪ The redirection checkbox is configurable only when both HTTP and HTTPS have been enabled.

Special note for AES ciphers:

The BCM2 device's SSL/TLS-based protocols, including HTTPS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between the BCM2 and the client (such as a web browser), which is impacted by the cipher priority of the BCM2 and the client's cipher availability/settings.

Tip: If intending to force the BCM2 to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings. For example, you can enable a cipher and disable the other in the Firefox via the "about:config" command.

Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the BCM2 device. Enabling SNMP communication allows the manager to retrieve and even control the power status of each outlet.

Besides, you may need to configure the SNMP destination(s) if the built-in "System SNMP Notification Rule" is enabled and the SNMP destination has not been set yet. See *Event Rules and Actions* (on page 190).

▶ **To configure SNMP communication:**

1. Choose Device Settings > Network Services > SNMP.

2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding checkbox.

   ▪ The SNMP v1/v2c read-only access is enabled by default. The default Read Community String is 'public.'

   ▪ To enable read-write access, type the Write Community String. Usually the string is 'private.'

3. Enter the MIB-II system group information, if applicable.

   ▪ sysContact - the contact person in charge of the system

   ▪ sysName - the name assigned to the system

   ▪ sysLocation - the location of the system

4. To configure SNMP notifications:

   a. Select the Enable SNMP Notifications checkbox.

   b. Select a notification type -- SNMPv2c Trap, SNMPv2c Inform, SNMPv3 Trap, and SNMPv3 Inform.

   c. Specify the SNMP notification destinations and enter necessary information. For details, refer to:

      ▪ *SNMPv2c Notifications* (on page 272)

      ▪ *SNMPv3 Notifications* (on page 273)

   Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See **Available Actions** *(on page 207). To add more than three SNMP destinations, you can create new SNMP notification actions. See* **Send an SNMP Notification** *(on page 218).*

5. You must download the SNMP MIB for your BCM2 to use with your SNMP manager.

a. Click the Download MIBs title bar to show the download links.

> **Download MIBs** ⌄

b. Click the -MIB download link. See *Downloading SNMP MIB* (on page 274).

6. Click Save.

Configuring SMTP Settings

The BCM2 can be configured to send alerts or event messages to a specific administrator by email. See *Event Rules and Actions* (on page 190).

To send emails, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See *Viewing or Clearing the Local Event Log* (on page 253).

▶ **To set SMTP server settings:**

1. Choose Device Settings > Network Services > SMTP Server.
2. Enter the information needed.

Field	Description
Server Name	Type the name or IP address of the mail server.
Port	Type the port number. ▪ Default is 25
Sender Email Address	Type an email address for the sender.
Number of Sending Retries	Type the number of email retries. ▪ Default is 2 retries
Time Between Sending Retries	Type the interval between email retries in minutes. ▪ Default is 2 minutes.
Server Requires Authentication	Select this checkbox if your SMTP server requires password authentication.

Raritan.
A brand of ☐legrand

Field	Description
User Name, Password	Type a user name and password for authentication after selecting the above checkbox. ▪ The length of user name and password ranges between 4 and 64. Case sensitive. ▪ Spaces are not allowed for the user name, but allowed for the password.
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this checkbox.

▪ **Settings for the CA Certificate:**

Field/setting	Description
Browse…	Click this button to install a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.

3. Now that you have set the SMTP settings, you can test it to ensure it works properly.

   a. Type the recipient's email address in the Recipient Email Addresses field. Use a comma to separate multiple email addresses.

   b. Click Send Test Email.

   c. Check if the recipient(s) receives the email successfully.

4. Click Save.

▶ **Special note for AES ciphers:**

The BCM2 device's SSL/TLS-based protocols, including SMTP over StartTLS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between the BCM2 and the client (such as a web browser), which is impacted by the cipher priority of the BCM2 and the client's cipher availability/settings.

Tip: If intending to force the BCM2 to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Changing SSH Settings

You can enable or disable the SSH access to the command line interface, change the TCP port, or set a password or public key for login over the SSH connection.

▶ **To change SSH settings:**

1. Choose Device Settings > Network Services > SSH.
2. To enable or disable the SSH access, select or deselect the checkbox.
3. To use a different port, type a port number.
4. Select one of the authentication methods.
    - Password authentication only: Enables the password-based login only.
    - Public key authentication only: Enables the public key-based login only.
    - Password and public key authentication: Enables both the password- and public key-based login. This is the default.
5. Click Save.

If the public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connection. See *Creating Users* (on page 123).

Changing Telnet Settings

You can enable or disable the Telnet access to the command line interface, or change the TCP port.

▶ **To change Telnet settings:**

1. Choose Device Settings > Network Services > Telnet.
2. To enable the Telnet access, select the checkbox.

3. To use a different port, type a new port number.

4. Click Save.

Changing Modbus Settings

You can enable or disable the Modbus/TCP access to the BCM2, set it to the read-only mode, or change the TCP port.

▶ **To change the Modbus/TCP settings:**

1. Choose Device Settings > Network Services > Modbus.

2. To enable the Modbus/TCP access, select the "Modbus/TCP Access" checkbox.

3. To use a different port, type a new port number.

4. To enable the Modbus read-only mode, select the checkbox of the "Read-only mode" field. To enable the read-write mode, deselect it.

Enabling Service Advertising

The BCM2 advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and MDNS (Multicast DNS). The advertised services are discovered by clients that have implemented DNS-SD and MDNS.

The advertised services include the following:

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

By default, this feature is enabled.

Enabling this feature also enables Link-Local Multicast Name Resolution (LLMNR) and/or MDNS, which are required for resolving APIPA host names. See APIPA and Link-Local Addressing.

The service advertisement feature supports both IPv4 and IPv6 protocols.

If you have set a preferred host name for IPv4 and/or IPv6, that host name can be used as the zero configuration .local host name, that is, *<preferred_host_name>.local*, where <preferred_host_name> is the preferred host name you have specified for BCM2. The IPv4 host name is the first priority. If an IPv4 host name is not available, then use the IPv6 host name.

Note: For information on configuring IPv4 and/or IPv6 network settings, see **Wired Network Settings** *(on page 137).*

▶ **To enable or disable service advertising:**

1. Choose Device Settings > Network Services > Service Advertising.
2. To enable the service advertising, select either or both checkboxes.
   - To advertise via MDNS, select the Multicast DNS checkbox.
   - To advertise via LLMNR, select the Link-Local Multicast Name Resolution checkbox.
3. Click Save.

Configuring Security Settings

The BCM2 provides tools to control access. You can enable the internal firewall, create firewall rules, and set login limitations. In addition, you can create and install the certificate or set up external authentication servers for access control. This product supports the SHA-2 certificate.

Tip: To force all HTTP accesses to the BCM2 to be redirected to HTTPS, see **Changing HTTP(S) Settings** *(on page 158).*

Submenu command	Refer to
IP Access Control	*Creating IP Access Control Rules* (on page 165)
Role Access Control	*Creating Role Access Control Rules* (on page 168)
SSL Certificate	*Setting Up an SSL/TLS Certificate* (on page 170)
Authentication	*Setting Up External Authentication* (on page 175)
Login Settings	*Configuring Login Settings* (on page 184)
Password Policy	*Configuring Password Policy* (on page 185)
Service Agreement	*Enabling the Restricted Service Agreement* (on page 186)

Creating IP Access Control Rules

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the BCM2, based on the IP address of the host sending or receiving the traffic. When creating rules, keep these principles in mind:

- **Rule order is important.**

  When traffic reaches or is sent from the BCM2 device, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored.

- **Subnet mask is required.**

  When typing the IP address, you must specify BOTH the address and a subnet mask. For example, to specify a single address in a Class C network, use this format:

  x.x.x.x/24

  where */24* = a subnet mask of 255.255.255.0.

  To specify an entire subnet or range of addresses, change the subnet mask accordingly.

Note: Valid IPv4 addresses range from 0.0.0.0 through 255.255.255.255.

▶ **To configure IPv4 access control rules:**

1. Choose Device Settings > Security > IP Access Control.

2. Select the Enable IPv4 Access Control checkbox to enable IPv4 access control rules.

3. Determine the IPv4 default policy.

   ▪ Accept: Accepts traffic from all IPv4 addresses.

   ▪ Drop: Discards traffic from all IPv4 addresses, without sending any failure notification to the source host.

   ▪ Reject: Discards traffic from all IPv4 addresses, and an ICMP message is sent to the source host for failure notification.

4. Go to the Inbound Rules section or the Outbound Rules section according to your needs.

   ▪ Inbound rules control the data sent to the BCM2.

   ▪ Outbound rules control the data sent from the BCM2.

5. Create rules. See the tables for different operations.

ADD a rule to the end of the list

▪ Click Append.
▪ Type an IP address and subnet mask in the IP/Mask field.
▪ Select an option in the Policy field.
  ▪ Accept: Accepts traffic from/to the specified IP address(es).
  ▪ Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
  ▪ Reject: Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

INSERT a rule between two rules
▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert Above. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select Accept, Drop or Reject in the Policy field. See the above for their descriptions.

The system automatically numbers the rule.

6. When finished, the rules are listed.

- You can select any existing rule and then click ![up arrow button] or ![down arrow button] to change its priority.

7. Click Save. The rules are applied.

▶ **To configure IPv6 access control rules:**

1. On the same page, select the Enable IPv6 Access Control checkbox to enable IPv6 access control rules.

2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.

3. **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Editing or Deleting IP Access Control Rules

When an existing IP access control rule requires updates of IP address range and/or policy, modify them accordingly. Or you can delete any unnecessary rules.

▶ **To modify or delete a rule:**

1. Choose Device Settings > Security > IP Access Control.

2. Go to the IPv4 or IPv6 section.

3. Select the desired rule in the list.

   - Ensure the IPv4 or IPv6 checkbox has been selected, or you cannot edit or delete any rule.

4. Perform the desired action.

   - Make changes to the selected rule, and then click Save. For information on each field, see *Creating IP Access Control Rules* (on page 165).

   - Click ![trash icon] to remove it.

   - To resort its order, click ![up arrow button] or ![down arrow button].

5. Click Save.

   - IPv4 rules: **Make sure you click the Save button in the IPv4 section**, or the changes made to IPv4 rules are not saved.

   - IPv6 rules: **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Creating Role Access Control Rules

Role-based access control rules are similar to IP access control rules, except they are applied to members of a specific role. This enables you to grant system permissions to a specific role, based on their IP addresses.

Same as IP access control rules, the order of role-based access control rules is important, since the rules are executed in numerical order.

▶ **To create IPv4 role-based access control rules:**

1. Choose Device Settings > Security > Role Access Control.

2. Select the "Enable Role Based Access Control for IPv4" checkbox to enable IPv4 access control rules.

3. Determine the IPv4 default policy.

    ▪ Allow: Accepts traffic from all IPv4 addresses regardless of the user's role.

    ▪ Deny: Drops traffic from all IPv4 addresses regardless of the user's role.

4. Create rules. See the tables for different operations.

ADD a rule to the end of the list

▪ Click Append.
 ▪ Type a starting IP address in the Start IP field.
 ▪ Type an ending IP address in the End IP field.
 ▪ Select a role in the Role field. This rule applies to members of this role only.
 ▪ Select an option in the Policy field.
     ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role
     ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role

Raritan.
A brand of ◻legrand

INSERT a rule between two rules
▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert Above. ▪ Type a starting IP address in the Start IP field. ▪ Type an ending IP address in the End IP field. ▪ Select a role in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny in the Policy field. See the above for their descriptions.

The system automatically numbers the rule.

5. When finished, the rules are listed on this page.

   ▪ You can select any existing rule and then click [↑] or [↓] to change its priority.

6. Click Save. The rules are applied.

▶ **To configure IPv6 access control rules:**

1. On the same page, select the "Enable Role Based Access Control for IPv6" checkbox to enable IPv6 access control rules.

2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.

3. **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Editing or Deleting Role Access Control Rules

You can modify existing rules to update their roles/IP addresses, or or delete them when they are no longer needed.

▶ **To modify a role-based access control rule:**

1. Choose Device Settings > Security > Role Access Control.

2. Go to the IPv4 or IPv6 section.

3. Select the desired rule in the list.
   ▪ Ensure the IPv4 or IPv6 checkbox has been selected, or you cannot select any rule.

4. Perform the desired action.
   ▪ Make changes to the selected rule, and then click Save. For information on each field, see *Creating Role Access Control Rules* (on page 168).

- Click [image: trash icon] to remove it.

- To resort its order, click [image: up arrow] or [image: down arrow].

5. Click Save.

- IPv4 rules: **Make sure you click the Save button in the IPv4 section**, or the changes made to IPv4 rules are not saved.

- IPv6 rules: **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Setting Up an SSL/TLS Certificate

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

Having an X.509 digital certificate ensures that both parties in an SSL/TLS connection are who they say they are.

▶ **To obtain a CA-signed certificate:**

1. Create a Certificate Signing Request (CSR) on the BCM2. See *Creating a CSR* (on page 171).

2. Submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate.

3. Install the CA-signed certificate onto the BCM2. See *Installing a CA-Signed Certificate* (on page 172).

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

▶ **A CSR is not required in either scenario below:**

- Make the BCM2 create a *self-signed* certificate. See *Creating a Self-Signed Certificate* (on page 173).

- Appropriate, valid certificate and key files are already available, and you just need to install them. See *Installing or Downloading Existing Certificate and Key* (on page 174).

[Raritan logo]
A brand of [legrand logo]

Creating a CSR

Follow this procedure to create the CSR for your BCM2 device.

Note that you must enter information in the fields showing the message 'required.'

required

▶ **To create a CSR:**

1. Choose Device Settings > Security > SSL Certificate.
2. Provide the information requested.
    - **Subject:**

Field	Description
Country	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the *ISO website* (*http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm*).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your BCM2 device.
Email Address	An email address where you or another administrative user can be reached.

Warning: If you generate a CSR without values entered in the required fields, you cannot obtain third-party certificates.

- **Key Creation Parameters:**

Field	Do this
Key Length	Select an available key length (bits). A larger key length enhances the security, but slows down the BCM2 device's response. - Only 2048 is available now.
Self Sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**

Field	Do this
Challenge, Confirm Challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional. The value should be 4 to 64 characters long. Case sensitive.

3. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.

4. Click Download Certificate Signing Request to download the CSR to your computer.

    a. You are prompted to open or save the file. Click Save to save it onto your computer.

    b. Submit it to a CA to obtain the digital certificate.

    c. If the CSR contains incorrect data, click Delete Certificate Signing Request to remove it, and then repeat the above steps to re-create it.

5. To store the newly-created private key on your computer, click Download Key in the **New SSL Certificate** section.

    Note: The Download Key button in the Active SSL Certificate section is for downloading the private key of the currently-installed certificate rather than the newly-created one.
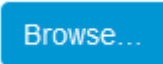
    ▪ You are prompted to open or save the file. Click Save to save it onto your computer.

6. After getting the CA-signed certificate, install it. See *Installing a CA-Signed Certificate* (on page 172).

Installing a CA-Signed Certificate

To get a certificate from a certificate authority (CA), first create a CSR and send it to the CA. See *Creating a CSR* (on page 171).

After receiving the CA-signed certificate, install it onto the BCM2.

▶ **To install the CA-signed certificate:**

1. Choose Device Settings > Security > SSL Certificate.

2. Click [Browse...] to navigate to the CA-signed certificate file.

3. Click Upload to install it.

4. To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

Creating a Self-Signed Certificate

When appropriate certificate and key files for the BCM2 device are unavailable, the alternative, other than submitting a CSR to the CA, is to generate a self-signed certificate.

Note that you must enter information in the fields showing the message 'required.'

required

▶ **To create and install a self-signed certificate:**

1. Choose Device Settings > Security > SSL Certificate.
2. Enter information.

Field	Description
Country	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the *ISO website* (*http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm*).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your BCM2 device.
Email Address	An email address where you or another administrative user can be reached.
Key Length	Select an available key length (bits). A larger key length enhances the security, but slows down the BCM2 device's response. ▪ Only 2048 is available now.
Self Sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self Sign checkbox is selected. Type the number of days for which the self-signed certificate will be valid.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear.

3. Click Create New SSL Key to create both the self-signed certificate and private key. This may take several minutes to complete.

4. Once complete, do the following:

   a. Double check the data shown in the New SSL Certificate section.

   b. If correct, click "Install Key and Certificate" to install the self-signed certificate and private key.

   Tip: To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

   If incorrect, click "Delete Key and Certificate" to remove the self-signed certificate and private key, and then repeat the above steps to re-create them.

5. (Optional) To download the self-signed certificate and/or private key, click Download Certificate or Download Key in the New SSL Certificate section.

   ▪ You are prompted to open or save the file. Click Save to save it onto your computer.

   Note: The Download Key button in the Active SSL Certificate section is for downloading the private key of the currently-installed certificate rather than the newly-created one.

Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any BCM2 for backup or file transfer. For example, you can install the files onto a replacement BCM2 device, add the certificate to your browser and so on.

If valid certificate and private key files are already available, you can install them on the BCM2 without going through the process of creating a CSR or a self-signed certificate.

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

▶ **To download active key and certificate files from the BCM2:**

1. Choose Device Settings > Security > SSL Certificate.

2. In the *Active SSL Certificate* section, click Download Key and Download Certificate respectively.

   Note: The Download Key button in the New SSL Certificate section, if present, is for downloading the newly-created private key rather than the one of the currently-installed certificate.

3. You are prompted to open or save the file. Click Save to save it onto your computer.

▶ **To install available key and certificate files onto the BCM2:**

1. Choose Device Settings > Security > SSL Certificate.

2. Select the "Upload Key and Certificate" checkbox at the bottom of the page.

3. The Key File and Certificate File fields appear. Click **Browse...** to select the key and/or certificate file.

4. Click Upload. The selected files are installed.

5. To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

Setting Up External Authentication

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

For security purposes, users attempting to log in to the BCM2 must be authenticated. The BCM2 supports the following authentication mechanisms:

- Local user database on the BCM2
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (Radius) protocol

By default, the BCM2 is configured for local authentication. If you stay with this method, you only need to create user accounts. See *Creating Users* (on page 123).

If you prefer external authentication, you must provide the BCM2 with information about the external Authentication and Authorization (AA) server.

If both local and external authentication is needed, create user accounts on the BCM2 in addition to providing the external AA server data.

When configured for external authentication, all BCM2 users must have an account on the external AA server. Local-authentication-only users will have no access to the BCM2 except for the admin, who always can access the BCM2.

If the external authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log. See *Viewing or Clearing the Local Event Log* (on page 253).

Note that only users who have both the "Change Authentication Settings" and "Change Security Settings" permissions can configure or modify the authentication settings.

▶ **To enable external authentication:**

1. Collect external AA server information. See *Gathering LDAP/Radius Information* (on page 177).

2. Enter required data for external AA server(s) on the BCM2. See *Adding LDAP/LDAPS Servers* (on page 178) or *Adding Radius Servers* (on page 181).

   - For illustrations, see *LDAP Configuration Illustration* (on page 451) or *Radius Configuration Illustration* (on page 456).

3. If both the external and local authentication is needed, or you have to return to the local authentication only, see *Managing External Authentication Settings* (on page 183).

▶ **Special note about the AES cipher:**

The BCM2 device's SSL/TLS-based protocols, including LDAPS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between the BCM2 and the client (such as a web browser), which is impacted by the cipher priority of the BCM2 and the client's cipher availability/settings.

Tip: If intending to force the BCM2 to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Gathering LDAP/Radius Information

It requires knowledge of your AA server settings to configure the BCM2 for external authentication. If you are not familiar with these settings, consult your AA server administrator for help.

▶ **Information needed for LDAP authentication:**
- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over TLS) is being used
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*
    - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*

> - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.

- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

▶ **Information needed for Radius authentication:**

- The IP address or host name of the Radius server
- Authentication protocol used by the Radius server
- Shared secret for a secure communication
- UDP authentication port and accounting port used by the Radius server

Adding LDAP/LDAPS Servers

To use LDAP authentication, enable it and enter the information you have gathered.
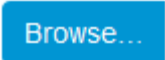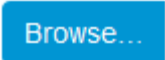
Note that you must enter information in the fields showing the message 'required.'

```
required
```

▶ **To add LDAP/LDAPS servers:**

1. Choose Device Settings > Security > Authentication.
2. Click New in the LDAP Servers section.
3. Enter information.

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your LDAP/LDAPS server. ▪ Important: Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	This checkbox appears only when there are existing AA server settings on the BCM2. To duplicate any existing AA server's settings, refer to the duplicating procedure below.

Field/setting	Description
Type of LDAP Server	Choose one of the following options: ▪ OpenLDAP ▪ Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
Security	Determine whether you would like to use Transport Layer Security (TLS) encryption, which allows the BCM2 to communicate securely with the LDAPS server. Three options are available: ▪ StartTLS ▪ TLS ▪ None
Port (None/StartTLS)	The default Port is 389. Either use the standard LDAP TCP port or specify another port.
Port (TLS)	**Configurable only when "TLS" is selected in the Security field.** The default is 636. Either use the default port or specify another one.
Enable verification of LDAP Server Certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the BCM2 prior to the connection. If the certificate validation fails, the connection is refused.
CA Certificate	Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click **Browse...** to select and install the certificate file. ▪ Click Show to view the installed certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Anonymous Bind	Use this checkbox to enable or disable anonymous bind. ▪ To use anonymous bind, select this checkbox. ▪ When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.

Field/setting	Description
Bind DN	**Required after deselecting the Anonymous Bind checkbox.** Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind Password, Confirm Bind Password	**Required after deselecting the Anonymous Bind checkbox.** Enter the Bind password.
Base DN for Search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. ▪ Example: `ou=dev,dc=example,dc=com`
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. ▪ Usually it is the `uid`.
User Entry Object Class	The object class for user entries. ▪ Usually it is `inetOrgPerson`.
User Search Subfilter	Search criteria for finding LDAP user objects within the directory tree.
Active Directory Domain	The name of the Active Directory Domain. ▪ Example: `testradius.com`

4. To verify if the authentication configuration is set correctly, click Test Connection to check whether the BCM2 can connect to the new server successfully.

   Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** *(on page 183).*

5. Click Add Server. The new LDAP server is listed on the Authentication page.

6. To add more servers, repeat the same steps.

7. **In the Authentication Type field, select LDAP.** Otherwise, the LDAP authentication does not work.

8. Click Save. The LDAP authentication is now in place.

► **To duplicate LDAP/LDAPS server settings:**

If you have added any LDAP/LDAPS server to the BCM2, and the server you will add shares identical settings with an existing one, the most convenient way is to duplicate that LDAP/LDAPS server's data and then revise the IP address/host name.

1. Repeat Steps 1 to 2 in the above procedure.
2. Select the "Copy settings from existing LDAP server" checkbox.
3. Click the "Select LDAP Server" field to select the LDAP/LDAPS server whose settings you want to copy.
4. Modify the IP Address/Hostname field.
5. Click Add Server.

Note: If the BCM2 clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the BCM2 and the LDAP server to use the same NTP server(s).

Adding Radius Servers

To use Radius authentication, enable it and enter the information you have gathered.

Note that you must enter information in the fields showing the message 'required.'

required

► **To add Radius servers:**

1. Choose Device Settings > Security > Authentication.
2. Click New in the Radius section.
3. Enter information.

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your Radius server.
Type of RADIUS Authentication	Select an authentication protocol. ▪ PAP (Password Authentication Protocol) ▪ CHAP (Challenge Handshake Authentication Protocol) CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.

Field/setting	Description
Authentication Port, Accounting Port	The default are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Timeout	This sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared Secret, Confirm Shared Secret	The shared secret is necessary to protect communication with the Radius server.

4. To verify if the authentication configuration is set correctly, click Test Connection to check whether the BCM2 can connect to the new server successfully.

   Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** *(on page 183).*

5. Click Add Server. The new Radius server is listed on the Authentication page.

6. To add more servers, repeat the same steps.

7. **In the Authentication Type field, select Radius.** Otherwise, the Radius authentication does not work.

8. Click Save. Radius authentication is now in place.

Managing External Authentication Settings

Choose Device Settings > Security > Authentication to open the Authentication page, where you can:

- Enable both the external and local authentication
- Edit or delete a server
- Resort the access order of servers
- Test the connection to a server
- Disable external authentication without removing servers

▶ **To test, edit or delete a server, or resort the server list:**

1. Select a server in the list.

Access Order	IP Address / Hostname	Security	Port	LDAP Server Type
1	192.168.91.100	None	389	OpenLDAP
2	192.168.1.33	StartTLS	389	OpenLDAP
3	192.168.8.95	None	389	Microsoft Active Directory

2. Perform the desired action.
   - Click Edit to edit its settings, and click Modify Server to save changes. For information on each field, see *Adding LDAP/LDAPS Servers* (on page 178) or *Adding Radius Servers* (on page 181).
   - Click Delete to delete the server, and then confirm the operation.
   - Click Test Connection to test the connection to the selected server. User credentials may be required.
   - Click ⌃ or ⌄ to change the server order, which determines the access priority, and click Save Order to save the new sequence.

   Note: Whenever the BCM2 is successfully connected to one external authentication server, it STOPS trying to access the remaining servers in the authentication list regardless of the user authentication result.

▶ **To enable both the external and local authentication:**

1. In the Authentication Type field, select the external authentication you want -- LDAP or Radius.

2. Select the following checkbox. Then the BCM2 always tries external authentication first. Whenever the external authentication fails, the BCM2 switches to local authentication.

✔ Use Local Authentication if Remote Authentication is not available

3. Click Save.

▶ **To disable external authentication:**

1. In the Authentication Type, select Local.

2. Click Save.

Configuring Login Settings

Choose Device Settings > Security > Login Settings to open the Login Settings page, where you can:

- Configure the user blocking feature.

  Note: The user blocking function applies only to local authentication instead of external authentication through AA servers.

- Determine the timeout period for any inactive user.

- Prevent simultaneous logins using the same login name.

▶ **To configure user blocking:**

1. To enable the user blocking feature, select the "Block user on login failure" checkbox.

2. In the "Maximum number of failed logins" field, type a number. This is the maximum number of login failure the user is permitted before the user is blocked from accessing the BCM2.

3. In the "Block timeout" field, type a value or click ⬍ to select a time option. This setting determines how long the user is blocked.

   - If you type a value, the value must be followed by a time unit, such as '4 min.' See Time Units.

4. Click Save.

Tip: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command over a local connection. See **Unblocking a User** *(on page 437).*

▶ **To set limitations for login timeout and use of identical login names:**

1. In the "Idle timeout period" field, type a value or click ⬓ to select a time option. This setting determines how long users are permitted to stay idle before being forced to log out.

    ▪ If you type a value, the value must be followed by a time unit, such as '4 min.' See Time Units.

    ▪ Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the BCM2.

2. Select the "Prevent concurrent login with same username" checkbox if intending to prevent multiple persons from using the same login name simultaneously.

3. Click Save.

Configuring Password Policy

Choose Device Settings > Security > Password Policy to open the Password Policy page, where you can:

- Force users to use strong passwords.
- Force users to change passwords at a regular interval -- that is, password aging.

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the BCM2 device.

▶ **To configure password aging:**

1. Select the 'Enabled' checkbox of Password Aging.

2. In the Password Aging Interval field, type a value or click ⬓ to select a time option. This setting determines how often users are requested to change their passwords.

    ▪ If you type a value, the value must be followed by a time unit, such as '10 d.' See Time Units.

3. Click Save.

▶ **To force users to create strong passwords:**

1. Select the 'Enabled' checkbox of Strong Passwords to activate the strong password feature. The following are the default settings:

Minimum length	= 8 characters
Maximum length	= 32 characters
At least one lowercase character	= Required
At least one uppercase character	= Required
At least one numeric character	= Required
At least one special character	= Required
Number of forbidden previous passwords	= 5

Note: The maximum password length accepted by the BCM2 is 64 characters.

2. Make changes to the default settings as needed.
3. Click Save.

Enabling the Restricted Service Agreement

The restricted service agreement feature, if enabled, forces users to read a security agreement when they log in to the BCM2.

Users must accept the agreement, or they cannot log in.

An event notifying you if a user has accepted or declined the agreement can be generated. See *Default Log Messages* (on page 196)

▶ **To enable the service agreement:**

1. Click Device Settings > Security > Service Agreement.
2. Select the Enforce Restricted Service Agreement checkbox.
3. Edit or paste the content as needed.
    ▪ A maximum of 10,000 characters can be entered.
4. Click Save.

▶ **Login manner after enabling the service agreement:**

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed in the login screen.

Do either of the following, or the login fails:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

  Tip: To select the agreement checkbox using the keyboard, first press Tab to go to the checkbox and then Enter.

- In the CLI, type y when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Setting the Date and Time

Set the internal clock on the BCM2 device manually, or link to a Network Time Protocol (NTP) server.

Note: If you are using Sunbird's Power IQ to manage the BCM2, you must configure Power IQ and the BCM2 to have the same date/time or NTP settings.

▶ **To set the date and time:**

1. Choose Device Settings > Date/Time.

2. Click the Time Zone field to select your time zone from the list.

3. If the daylight saving time applies to your time zone, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.

   - If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.

4. Select the method for setting the date and time.

Customize the date and time

▪ Select User Specified Time.

▪ Type values in the Date field using the yyyy-mm-dd format, or click [icon] to select a date. For details, see *Calendar* (on page 188).

▪ Type values in the Time field using the hh:mm:ss format, or click ⌃ ⌄ to adjust values.

    ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM or PM button.

| 12 | : | 00 | : | 00 | AM |

Use the NTP server

▪ Select "Synchronize with NTP Server."

▪ There are two ways to assign the NTP servers:

    ▪ To use the DHCP-assigned NTP servers, DO NOT enter any NTP servers for the First and Second NTP Server.

      DHCP-assigned NTP servers are available only when either IPv4 or IPv6 DHCP is enabled.

    ▪ To use the manually-specified NTP servers, specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.

      Click Check NTP Servers to verify the validity and accessibility of the manually-specified NTP servers.

5.   Click Save.

The BCM2 follows the NTP server sanity check per the IETF RFC. If your BCM2 has problems synchronizing with a Windows NTP server, see *Windows NTP Server Synchronization Solution* (on page 189).

Calendar

The calendar icon [icon] in the Date field is a convenient tool to select a custom date. Click it and a calendar appears.

Button	Function
arrows	Switch between months.

Button	Function
dates (01-31)	Click a date.
Today	Select today.
Clear	Clear the entry, if any, in the Date field.
Close	Close the calendar.

Windows NTP Server Synchronization Solution

The NTP client on the BCM2 follows the NTP RFC so the BCM2 rejects any NTP servers whose root dispersion is more than one second. An NTP server with a dispersion of more than one second is considered an inaccurate NTP server by the BCM2.

Note: For information on NTP RFC, visit
http://tools.ietf.org/html/rfc4330 http://tools.ietf.org/html/rfc4330 *to refer to section 5.*

Windows NTP servers may have a root dispersion of more than one second, and therefore cannot synchronize with the BCM2. When the NTP synchronization issue occurs, change the dispersion settings to resolve it.

▶ **To change the Windows NTP's root dispersion settings:**

1. Access the registry settings associated with the root dispersion on the Windows NTP server.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

2. *AnnounceFlags* must be set to 0x05 or 0x06.
   - 0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)
   - 0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

   Note: Do NOT use 0x08 (Automatic reliable time server) because its dispersion starts at a high value and then gradually decreases to one second or lower.

3. *LocalClockDispersion* must be set to 0.

Event Rules and Actions

A benefit of the product's intelligence is its ability to notify you of or react to a change in conditions. This event notification or reaction is an "event rule."

An event rule consists of two parts:

- Event: This is the situation where the BCM2 or a device connected to it meets a certain condition. For example, the inlet's voltage reaches the warning level.
- Action: This is the response to the event. For example, the BCM2 notifies the system administrator of the event via email.

If you want the BCM2 to perform one action at a regular interval instead of waiting until an event occurs, you can schedule that action. For example, you can make the BCM2 email the temperature report every hour.

Note that you need the Administrator Privileges to configure event rules.

▶ **To create an event rule:**

1. Choose Device Settings > Event Rules.
2. If the needed action is not available yet, create it by clicking New Action.

    a. Assign a name to this action.

    b. Select the desired action and configure it as needed.

    c. Click Create.

    For details, see *Available Actions* (on page 207).

3. Click New Rule to create a new rule.

    a. Assign a name to this rule.

    b. Make sure the Enabled checkbox is selected, or the new event rule does not work.

    c. In the Event field, select the event to which you want the BCM2 to react.

    d. In the Available Actions field, select the desired action(s) to respond to the selected event.

    e. Click Create.

    For details, see *Built-in Rules and Rule Configuration* (on page 191).

▶ **To create a scheduled action:**

1. If the needed action is not available yet, create it by clicking New Action. See above.

Note: When creating scheduled actions, available actions are less than usual because it is meaningless to schedule certain actions like "Alarm," "Log event message," "Send email," "Syslog message" and the like.

2. Click ![New Scheduled Action] to schedule the desired action.

    a. Assign a name to this scheduled action.

    b. Make sure the Enabled checkbox is selected, or the BCM2 does not perform this scheduled action.

    c. Set the interval time, which ranges from every minute to yearly.

    d. In the Available Actions field, select the desired action(s).

    e. Click Create.

    For details, see *Scheduling an Action* (on page 224).

Built-in Rules and Rule Configuration

The BCM2 is shipped with four built-in event rules, which cannot be deleted. If the built-in event rules do not satisfy your needs, create new rules.

▶ **Built-in rules:**

*   *System Event Log Rule:*

    This causes ANY event occurred to the BCM2 to be recorded in the internal log. It is enabled by default.

    Note: For the default log messages generated for each event, see **Default Log Messages** *(on page 196).*

*   *System SNMP Notification Rule:*

    This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the BCM2. It is disabled by default.

*   *System Tamper Detection Alarmed:*

    This causes the BCM2 to send alarm notifications if a DX tamper sensor has been connected and the BCM2 detects that the tamper sensor enters the alarmed state. It is enabled by default.

*   *System Tamper Detection Unavailable:*

    This causes the BCM2 to send alarm notifications if a DX tamper sensor was once connected or remains connected but then the BCM2 does not detect the presence of the tamper sensor. It is enabled by default.

▶ **Event rule configuration illustration:**

1. Choose Device Settings > Event Rules > ➕ New Rule.

2. Click the Event field to select an event type.

   ▪ <Any sub-event> means all events shown on the list.

   ▪ <Any Numeric Sensor> means all numeric sensors of the BCM2, including internal and environmental sensors. <Any Numeric Sensor> is especially useful if you want to receive the notifications when any numeric sensor's readings pass through a specific threshold.

3. In this example, the Peripheral Device Slot is selected, which is related to the environmental sensor packages. Then a sensor ID field for this event type appears. Click this additional field to specify which sensor should be the subject of this event.

4. In this example, sensor ID 2 (Slot 2) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.

5. In this example, Numeric Sensor is selected because we want to select numeric-sensor-related event(s). Then a field for numeric-sensor-related events appears. Click this field to select one of the numeric-sensor-related events from the list.

6. In this example, 'Above upper critical threshold' is selected because we want the BCM2 to react only when the selected temperature sensor's reading enters the upper critical range. A "Trigger condition" field appears, requiring you to define the "exact" condition related to the "upper critical" event.

Event	Peripheral Device Slot
	Slot 2 (Temperature 2)
	Numeric Sensor
	Above upper critical threshold
Trigger condition	○ Asserted
	○ Deasserted
	● Both

7. Select the desired radio button to finish the event configuration. Refer to the following table for different types of radio buttons.

   ▪ If needed, you may refer to event rule examples in the section titled *Sample Event Rules* (on page 231).

8. To select any action(s), select them one by one from the Available Actions list.

   ▪ To select all available actions, click Select All.

9. To remove any action(s) from the Selected Actions field, click that action's ✖.

   ▪ To remove all actions, click Deselect All.

▶ **Radio buttons for different events:**

According to the event you select, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: The BCM2 takes the action only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. ▪ Deasserted: The BCM2 takes the action only when the selected event disappears or stops. That is, the status of the selected event transits from TRUE to FALSE. ▪ Both: The BCM2 takes the action both when the event occurs (asserts) and when the event stops/disappears (deasserts).
State sensor state change	Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both." ▪ Alarmed/Open/On: The BCM2 takes the action only when the chosen sensor enters the alarmed, open or on state. ▪ No longer alarmed/Closed/Off: The BCM2 takes the action only when the chosen sensor returns to the normal, closed, or off state. ▪ Both: The BCM2 takes the action whenever the chosen sensor switches its state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: The BCM2 takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: The BCM2 takes the action only when the chosen sensor is detected and becomes available. ▪ Both: The BCM2 takes the action both when the chosen sensor becomes unavailable or available.

Event types	Radio buttons
Network interface link state	▪ Link state is up: The BCM2 takes the action only when the network link state changes from down to up. ▪ Link state is down: The BCM2 takes the action only when the network link state changes from up to down. ▪ Both: The BCM2 takes the action whenever the network link state changes.
Function enabled or disabled	▪ Enabled: The BCM2 takes the action only when the chosen function is enabled. ▪ Disabled: The BCM2 takes the action only when the chosen function is disabled. ▪ Both: The BCM2 takes the action when the chosen function is either enabled or disabled.
Restricted service agreement	▪ Accepted: The BCM2 takes the action only when the specified user accepts the restricted service agreement. ▪ Declined: The BCM2 takes the action only when the specified user rejects the restricted service agreement. ▪ Both: The BCM2 takes the action both when the specified user accepts or rejects the restricted service agreement.
Server monitoring event	▪ Monitoring started: The BCM2 takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: The BCM2 takes the action only when the monitoring of any specified server stops. ▪ Both: The BCM2 takes the action when the monitoring of any specified server starts or stops.

Event types	Radio buttons
Server reachability	▪ Unreachable: The BCM2 takes the action only when any specified server becomes inaccessible. ▪ Reachable: The BCM2 takes the action only when any specified server becomes accessible. ▪ Both: The BCM2 takes the action when any specified server becomes either inaccessible or accessible.
Device connection or disconnection, such as a USB-cascaded slave device	▪ Connected: The BCM2 takes the action only when the selected device is physically connected to it. ▪ Disconnected: The BCM2 takes the action only when the selected device is physically disconnected from it. ▪ Both: The BCM2 takes the action both when the selected device is physically connected to it and when it is disconnected.
+12V Supply Status	Available radio buttons include "Fault," "Ok" and "Both." ▪ Fault: The BCM2 takes the action only when the selected 12V power supply to the controller enters the fault state. ▪ Ok: The BCM2 takes the action only when when the selected 12V power supply to the controller enters the OK state. ▪ Both: The BCM2 takes the action whenever the selected 12 power supply's status changes.

Default Log Messages

Following are default log messages recorded internally and emailed to specified recipients when BCM2 events occur (are TRUE) or, in some cases, stop or become unavailable (are FALSE). See *Send Email* (on page 214) for information configuring email messages to be sent when specified events occur.

Raritan.
A brand of ❑legrand

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Asset Management > State	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'.	
Asset Management > Rack Unit > * > Tag Connected	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Rack Unit > * > Blade Extension Connected	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Firmware Update	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'): status changed to '[STATE]'.	
Asset Management > Device Config Changed	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'.	
Asset Management > Rack Unit Config Changed	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to: LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]'	
Asset Management > Blade Extension Overflow	Blade extension overflow occurred on strip [STRIPID] ('[STRIPNAME]').	Blade extension overflow cleared for strip [STRIPID] ('[STRIPNAME]').
Asset Management > Composite Asset Strip Composition Changed	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]').	
Card Reader Management > Card inserted	Card Reader with id '[CARDREADERID]' connected.	
Card Reader Management > Card Reader attached	Card Reader with id '[CARDREADERID]' disconnected.	
Card Reader Management > Card Reader detached	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' inserted.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Card Reader Management > Card removed	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' removed.	
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware validation failed	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update started	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update completed	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update failed	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device identification changed	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device settings saved	Device settings saved from host '[USERIP]'	
Device > Device settings restored	Device settings restored from host '[USERIP]'.	
Device > Data push failed	Data push to URL [DATAPUSH_URL] failed. [ERRORDESC].	
Device > Event log cleared	Event log cleared by user '[USERNAME]' from host '[USERIP]'.	
Device > Bulk configuration saved	Bulk configuration saved from host '[USERIP]'.	
Device > Bulk configuration copied	Bulk configuration copied from host '[USERIP]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Device > Network interface link state is up	The [IFNAME] network interface link is now up.	The [IFNAME] network interface link is now down.
Device > Peripheral Device Firmware Update	Firmware update for peripheral device [EXTSENSORSERIAL] from [OLDVERSION] to [VERSION] [SENSORSTATENAME].	
Device > Sending SMTP message failed	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed.	
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGERPORT] failed or no response. [ERRORDESC].	
Device > Sending Syslog message failed	Sending Syslog message to server [SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO]) failed. [ERRORDESC].	
Device > Sending SMS message failed	Sending SMS message to '[PHONENUMBER]' failed.	
Device > An LDAP error occurred	An LDAP error occurred: [LDAPERRORDESC].	
Device > An Radius error occurred	An Radius error occurred: [RADIUSERRORDESC].	
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.	
Device > USB slave connected	USB slave connected.	USB slave disconnected.
Device > WLAN authentication over TLS with incorrect system clock	Established connection to wireless network '[SSID]' via Access Point with BSSID '[BSSID]' using '[AUTHPROTO]' authentication with incorrrect system clock.	
Energywise > Enabled	User '[USERNAME]' from host '[USERIP]' enabled EnergyWise.	User '[USERNAME]' from host '[USERIP]' disabled EnergyWise.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Peripheral Device Slot > * > Numeric Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > Numeric Sensor > Above upper critical threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Above upper warning threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Below lower warning threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Below lower critical threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical' at [READING].
Peripheral Device Slot > * > State Sensor/Actuator > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > State Sensor/Actuator > Alarmed/Open/On	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].
Inlet > * > Enabled	Inlet '[INLET]' has been enabled by user '[USERNAME]' from host '[USERIP]'.	Inlet '[INLET]' has been disabled by user '[USERNAME]' from host '[USERIP]'.
Inlet > * > Sensor > * > Unavailable	Sensor '[INLETSENSOR]' on inlet '[INLET]' unavailable.	Sensor '[INLETSENSOR]' on inlet '[INLET]' available.
Inlet > * > Sensor > * > Above upper critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper critical'.
Inlet > * > Sensor > * > Above	Sensor '[INLETSENSOR]' on inlet	Sensor '[INLETSENSOR]' on inlet

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
upper warning threshold	'[INLET]' asserted 'above upper warning'.	'[INLET]' deasserted 'above upper warning'.
Inlet > * > Sensor > * > Below lower warning threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower warning'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower warning'.
Inlet > * > Sensor > * > Below lower critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower critical'.
Inlet > * > Sensor > Active Energy > Reset	Sensor '[INLETSENSOR]' on inlet '[INLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.	
Modem > Dial-in link established	An incoming call from caller '[CALLERID]' was received.	The incoming call from caller '[CALLERID]' was disconnected: [CALLENDREASON].
Modem > Modem attached	A [MODEMTYPE] modem was attached.	
Modem > Modem detached	A [MODEMTYPE] modem was removed.	
Outlet > * > Power control > Powered on	Outlet '[OUTLET]' has been powered on by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Power control > Powered off	Outlet '[OUTLET]' has been powered off by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Power control > Power cycled	Outlet '[OUTLET]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Sensor > * > Unavailable	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' unavailable.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' available.
Outlet > * > Sensor > * > Above upper critical threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper critical'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper critical'.
Outlet > * > Sensor > * > Above upper warning threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper warning'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper warning'.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Outlet > * > Sensor > * > Below lower warning threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower warning'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower warning'.
Outlet > * > Sensor > * > Below lower critical threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower critical'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower critical'.
Outlet > * > Sensor > Active Energy > Reset	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Sensor > Outlet State > On	Outlet '[OUTLET]' state changed to on.	Outlet '[OUTLET]' state changed to off.
Outlet > * > Pole > * > Sensor > Unavailable	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' unavailable.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' available.
Outlet > * > Pole > * > Sensor > Above upper critical threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper critical'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper critical'.
Outlet > * > Pole > * > Sensor > Above upper warning threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper warning'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper warning'.
Outlet > * > Pole > * > Sensor > Below lower warning threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower warning'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower warning'.
Outlet > * > Pole > * > Sensor > Below lower critical threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower critical'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower critical'.
Overcurrent Protector > * > Sensor > * > Unavailable	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available.
Overcurrent Protector > * > Sensor > * > Above upper critical threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper critical'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper critical'.

Raritan.
A brand of ⬜legrand

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Overcurrent Protector > * > Sensor > * > Above upper warning threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper warning'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper warning'.
Overcurrent Protector > * > Sensor > * > Below lower warning threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower warning'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower warning'.
Overcurrent Protector > * > Sensor > * > Below lower critical threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower critical'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower critical'.
Overcurrent Protector > * > Sensor > Trip > Open	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is open.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is closed.
PDU > Load Shedding > Started	PX placed in Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.	PX removed from Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.
PDU > Sensor > +12V Supply Status > fault	Global sensor 'powerSupplyStatus' entered fault state.	PDU > Sensor > +12V Supply Status > fault
PDU > Sensor > +12V Supply Status > Unavailable	Global sensor 'powerSupplyStatus' unavailable.	Global sensor 'powerSupplyStatus' available.
Server Monitoring > * > Error	Error monitoring server '[MONITOREDHOST]': [ERRORDESC]	
Server Monitoring > * > Monitored	Server '[SERVER]' is now being monitored.	Server '[SERVER]' is no longer being monitored.
Server Monitoring > * > Unreachable	Server '[SERVER]' is unreachable.	Server '[SERVER]' is reachable.
Server Monitoring > * > Unrecoverable	Connection to server '[MONITOREDHOST]' could not be restored.	
User Activity > * > User logon state	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.
User Activity > * > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User accepted the Restricted Service Agreement	User '[USERNAME]' from host '[USERIP]" accepted the Restricted Service Agreement.	User '[USERNAME]' from host '[USERIP]" declined the Restricted Service Agreement.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
User Activity > * > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.	
User Activity > * > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.	
User Administration > User added	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User modified	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User deleted	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password changed	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password settings changed	Password settings changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role added	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role modified	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role deleted	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
Webcam Management > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') added to port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam detached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') removed from port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam settings changed	Webcam '[WEBCAMNAME]' settings changed by user '[USERNAME]'.	
LHX/SHX > Connected	LHX has been connected to [PORTTYPE] port [PORTID].	LHX has been disconnected from [PORTTYPE] port [PORTID].
LHX/SHX > Operational State	LHX connected to [PORTTYPE] port [PORTID] has been switched on.	LHX connected to [PORTTYPE] port [PORTID] has been switched off.

Raritan.
A brand of legrand

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
LHX/SHX > Sensor > Unavailable	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available.
LHX/SHX > Sensor > Above upper critical threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper critical'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical'.
LHX/SHX > Sensor > Above upper warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning'.
LHX/SHX > Sensor > Below lower warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower warning'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning'.
LHX/SHX > Sensor > Below lower critical threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower critical'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical'.
LHX/SHX > Base Electronics Failure	The base electronics on LHX at [PORTTYPE] port '[PORTID]' failed.	
LHX/SHX > Condenser Pump Failure	The condenser pump on LHX at [PORTTYPE] port '[PORTID]' failed.	The condenser pump on LHX at [PORTTYPE] port '[PORTID]' is back to normal.
LHX/SHX > Emergency Cooling	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated.	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated.
LHX/SHX > Maximum cooling request	Maximum cooling was requested for LHX at [PORTTYPE] port '[PORTID]'.	Maximum cooling is not any more requested for LHX at [PORTTYPE] port '[PORTID]'.
LHX/SHX > Parameter Data Loss	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'.	
LHX/SHX > ST-Bus Communication Error	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'.	
LHX/SHX > Collective fault	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'.	
LHX/SHX > Door Contact	The door of LHX at [PORTTYPE] port '[PORTID]' was opened.	The door of LHX at [PORTTYPE] port '[PORTID]' was closed.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
LHX/SHX > Sensor Failure	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port '[PORTID]' at sensor '[LHXSENSORID]'.	
LHX/SHX > Fan Failure	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'.	
LHX/SHX > Power Supply Failure	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'.	
LHX/SHX > Threshold Air Inlet	The air inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The air inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > Threshold Air Outlet	The air outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The air outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > Threshold Water Inlet	The water inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The water inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > Threshold Water Outlet	The water outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The water outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > Voltage Low	The supply voltage on LHX at [PORTTYPE] port '[PORTID]' is low.	The supply voltage on LHX at [PORTTYPE] port '[PORTID]' is back to normal.
LHX/SHX > Threshold Humidity	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > External Water Cooling Failure	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'.	
LHX/SHX > Water Leak	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'.	

The asterisk symbol (*) represents anything you select for the 'trigger' events.

Raritan.
A brand of legrand

Available Actions

The BCM2 comes with three built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

▶ **Built-in actions:**

- *System Event Log Action:*

  This action records the selected event in the internal log when the event occurs.

- *System SNMP Notification Action:*

  This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

  Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. See **Editing or Deleting a Rule/Action** *(on page 230). Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See* **Configuring SNMP Settings** *(on page 159).*

- *System Tamper Alarm:*

  This action causes the BCM2 to show the alarm for the DX tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules. For information on acknowledging an alarm, see *Dashboard - Alarms* (on page 70).

▶ **Actions you can create:**

1. Choose Device Settings > Event Rules > ➕ New Action.
2. Click the Action field to select an action type from the list.
3. Below is the list of available actions.

   Note: The "Change load shedding state" and "Switch outlets" options are only available for outlet-switching capable models.

Action	Function
Alarm	Requires the user to acknowledge the alert after it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action. See *Alarm* (on page 209).
Change load shedding state	Enters or quits the load shedding mode. See *Change Load Shedding State* (on page 211).

Action	Function
Execute an action group	Creates a group of actions comprising existing actions. See *Action Group* (on page 210).
External beeper	Enables or disables the connected external beeper, or causes it to enter an alarm cycle. See *External Beeper* (on page 211).
Internal beeper	Turns on or off the internal beeper. See *Internal Beeper* (on page 212).
Log event message	Records the selected events in the internal log. See *Log an Event Message* (on page 212).
Push out sensor readings	Sends internal sensor log, environmental sensor log or asset management strip data to a remote server using HTTP POST requests. See *Push Out Sensor Readings* (on page 212).
Record snapshots to webcam storage	Makes a connected webcam start or stop taking snapshots. See *Record Snapshots to Webcam Storage* (on page 213).
Request LHX/SHX maximum cooling	Applies the maximum cooling to the LHX/SHX device. See *Request LHX/SHX Maximum Cooling* (on page 214). This option is available only when the Schroff LHX/SHX support has been enabled.
Send email	Emails a textual message. See *Send Email* (on page 214).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See *Send Sensor Report* (on page 215).
Send SMS message	Sends a message to a mobile phone. See *Send SMS Message* (on page 217).
Send snapshots via email	Emails the snapshots captured by a connected Logitech® webcam (if available). See *Send Snapshots via Email* (on page 218).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See *Send an SNMP Notification* (on page 218).

Action	Function
Start/stop Lua script	If you are a developer who can create a Lua script, you can upload it to the BCM2, and have the BCM2 automatically perform or stop the script in response to an event. See *Start or Stop a Lua Script* (on page 220).
Switch LHX/SHX	Switches on or off the LHX/SHX device. See *Switch LHX/SHX* (on page 221). This option is available only when the Schroff LHX/SHX support has been enabled.
Switch outlets	Switches on, off or cycles the power to the specified outlet(s). See *Switch Outlets* (on page 221).
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See *Switch Peripheral Actuator* (on page 222).
Syslog message	Makes the BCM2 automatically forward event messages to the specified syslog server. See *Syslog Message* (on page 223).

4. Enter the information as needed and click Create.

5. Then you can assign the newly-created action to an event rule or schedule it. See *Event Rules and Actions* (on page 190).

Alarm

The Alarm is an action that requires users to acknowledge an alert. This helps ensure that the user is aware of the alert.

If the Alarm action has been included in a specific event rule and no one acknowledges that alert after it occurs, the BCM2 resends or regenerates an alert notification regularly until the alert is acknowledged or the maximum number of alert notifications is sent.

For information on acknowledging an alert, see Dashboard.

▶ **Operation:**

1. Choose Device Settings > Event Rules > .

2. Select Alarm from the Action list.

3. In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications. Available methods vary, depending on how many notification-based actions have been created. Notification-based action types include:

- External beeper
- Syslog message
- Send email
- Send SMS message
- Internal beeper

If no appropriate actions are available, create them first.

a. To select any methods, select them one by one in the Available field.

   To add all available methods, simply click Select All.

b. To delete any methods, click a method's ✖ in the Selected field.

   To remove all methods, simply click Deselect All.

4. To enable the notification-resending feature, select the "Enable Re-scheduling of Alarm Notifications" checkbox.

5. In the "Re-scheduling Period" field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly.

6. In the "Re-scheduling Limit" field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.

7. **(Optional)** You can instruct the BCM2 to send the acknowledgment notification after the alarm is acknowledged in the Acknowledgment Notifications field. Available methods are identical to those for generating alarm notifications.

a. In the Available field, select desired methods one by one, or click Select All. See step 3 for details.

b. In the Selected field, click any method's ✖ to remove unnecessary ones, or click Deselect All.

Action Group

You can create an action group that performs up to 32 actions. After creating such an action group, you can easily assign this set of actions to any event rule rather than selecting all needed actions one by one per rule.

If the needed action is not available yet, create it first. See *Available Actions* (on page 207).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select "Execute an action group" from the Action list.

3. To select any action(s), select them one by one from the Available Actions list.

   ▪ To select all available actions, click Select All.

4. To remove any action(s) from the Selected Actions field, click that action's ✖.

   ▪ To remove all actions, click Deselect All.

Change Load Shedding State

The "Change load shedding state" action is available only when your BCM2 is able to control outlet power. Use this action to activate or deactivate the load shedding mode for responding to a specific event. For additional informtion, see Load Shedding Mode.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select "Change load shedding state" from the Action list.

3. In the Operation field, select either one below:

   ▪ Start Load Shedding: Enters the load shedding mode when the specified event occurs.

   ▪ Stop Load Shedding: Quits the load shedding mode when the specified event occurs.

External Beeper

If an external beeper is connected to the BCM2, the BCM2 can change the beeper's behavior or status to respond to a certain event.

▶ **To control the connected external beeper:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select "External beeper" from the Action list.

3. In the Beeper Port field, select the port where the external beeper is connected. This port is the FEATURE port.

4. In the Beeper Action field, select an action for the external beeper to carry out.

   ▪ Alarm: Causes the external beeper to sound an alarm cycle every 20 seconds - stays on for 0.7 seconds and then off for 19.3 seconds.

   ▪ On: Turns on the external beeper so that it buzzes continuously.

   ▪ Off: Turns off the external beeper so that it stops buzzing.

Warning: If you create an event rule for the external beeper but disconnect it when an event causes it to beep, the beeper no longer beeps after it is re-connected even though the event triggering the beeping action remains asserted.

Internal Beeper

You can have the built-in beeper of the BCM2 turned on or off when a certain event occurs.

▶ **Operation:**

1. Choose Device Settings > Event Rules > **✚ New Action** .
2. Select "Internal beeper" from the Action list.
3. Select an option from the Operation field.
   - Turn Beeper On: Turns on the internal beeper to make it buzz.
   - Turn Beeper Off: Turns off the internal beeper to make it stop buzzing.

Log an Event Message

The option "Log event message" records the selected events in the internal log.

The default log message generated for each type of event is available in the section titled *Default Log Messages* (on page 196).

Push Out Sensor Readings

You can configure the BCM2 to push sensor log to a remote server after a certain event occurs, including logs of internal sensors, environmental sensors and actuators.

If you have connected Raritan's asset strips to the BCM2, you can also configure the BCM2 to push the data to a server.

Before creating this action, make sure that you have properly defined the destination servers and the data to be sent on the Data Push page. See *Configuring Data Push Settings* (on page 236).

Tip: To send the data at a regular interval, schedule this action. See **Scheduling an Action** *(on page 224). Note that the "Asset management log" is generated only when there are changes made to any asset strips or asset tags, such as connection or disconnection events.*

▶ **Operation:**

1. Choose Device Settings > Event Rules > **✚ New Action** .

Raritan.
A brand of ☐legrand

2. Select "Push out sensor readings" from the Action list.

3. Select a server or host which receives the asset strip data or sensor log in the Destination field.

   - If the desired destination is not available yet, go to the Data Push page to specify it.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

Per default the snapshots are stored on the BCM2. You can specify a remote server to store snapshots. See *Viewing Saved Snapshots and Managing Storage* (on page 269).

▶ **Operation:**

1. Choose Device Settings > Event Rules > **+ New Action**.

2. Select "Record snapshots to webcam storage" from the Action list.

3. Select a webcam in the Webcam field.

4. Select the action to perform - "Start recording" or "Stop recording."

   If "Start recording" is selected, adjust the values of the following:

   - Number of Snapshots - the number of snapshots to be taken when the event occurs.

     The maximum amount of snapshots that can be stored on the BCM2 is 10. If you set it for a number greater than 10 and the storage location is on the BCM2, after the 10th snapshot is taken and stored, the oldest snapshots are overwritten. Storing snapshots on a remote server does not have such a limitation.

   - Time Before First Snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.

   - Time Between Snapshots - the amount of time in seconds between when each snapshot is taken.

Request LHX/SHX Maximum Cooling

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See *Miscellaneous* (on page 250).

The "Request LHX/SHX Maximum Cooling" action applies the maximum cooling to the SHX-30 device only. The LHX-20 and LHX-40 devices do not support this feature.

In the maximum cooling mode, an SHX-30 device runs at 100% fan speed and the cold water valve is open 100%.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action .
2. Select "Request LHX/SHX Maximum Cooling" from the Action list.
3. In the Available LHX/SHX field, select the desired SHX-30 device one by one, or click Select All.
4. To remove any SHX-30 device from the Selected LHX/SHX field, click that device's ✖ or click Deselect All.

Send Email

You can configure emails to be sent when an event occurs and can customize the message.

Messages consist of a combination of free text and BCM2 placeholders. The placeholders represent information is pulled from the BCM2 and inserted into the message.

For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
```

translates to

```
JQPublic logged into the device on 2012-January-30 21:00
```

For a list and definition of available variables, see *Email and SMS Message Placeholders* (on page 227).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action .
2. Select "Send email" from the Action list.
3. In the "Recipient Email Addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
4. To use the SMTP server specified on the SMTP Server page, make sure the "Use custom SMTP Server" checkbox is NOT selected.

To use a different SMTP server, select this checkbox. The fields for customized SMTP settings appear. For information on each field, see *Configuring SMTP Settings* (on page 160).

Default messages are sent based on the event. For a list of default log messages and events that trigger them, see *Default Log Messages* (on page 196).

5. If needed, select the Use Custom Log Message checkbox, and then create a custom message up to 1024 characters in the provided field.

    ▪ When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just click the desired placeholder. For details, see *Email and SMS Message Placeholders* (on page 227).

    ▪ To start a new line in the text box, press Enter.

    ▪ If needed, you can resize the text box by dragging the bottom-right corner.

Send Sensor Report

You may set the BCM2 so that it automatically reports the latest readings or states of one or multiple sensors by sending a message or email or simply recording the report in a log. These sensors can be either internal or environmental sensors as listed below.

•   Inlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor and active energy.

•   Outlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor, active energy and outlet state (for outlet-switching capable PDUs only).

•   Overcurrent protector sensors, including RMS current and tripping state.

•   Peripheral device sensors, which can be any Raritan environmental sensor packages connected to the BCM2, such as temperature or humidity sensors.

An example of this action is available in the section titled *Send Sensor Report Example* (on page 226).

▶   **Operation:**

1. Choose Device Settings > Event Rules > .

2. Select "Send sensor report" from the Action list.

3. In the Destination Actions section, select the method(s) to report sensor readings or states. The number of available methods varies, depending on how many messaging actions have been created.

    The messaging action types include:

    ▪ Log event message

- Syslog message
- Send email
- Send SMS message

a. If no messaging actions are available, create them now. See *Available Actions* (on page 207).

b. To select any methods, select them one by one in the Available field.

To add all available methods, simply click Select All.

c. To delete any methods, click a method's ✖ in the Selected field.

To remove all methods, simply click Deselect All.

4. In the Available Sensors field, select the desired target's sensor.

a. Click the first ⬍ to select a target component from the list.
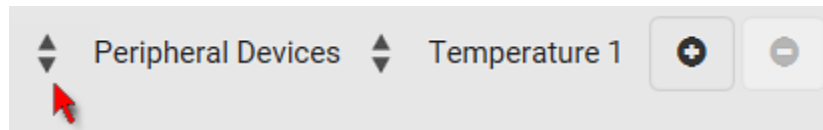
b. Click the second ⬍ to select the specific sensor for the target from the list.
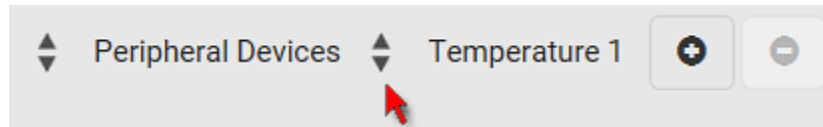
c. Click ⊕ to add the selected sensor to the Report Sensors list box.

For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.

5. To report additional sensors simultaneously, repeat the above step to add more sensors.

- To remove any sensor from the Report Sensors list box, select it and click ⊖ . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

6. To immediately send out the sensor report, click Send Report Now.

Tip: When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings. See **Email and SMS Message Placeholders** *(on page 227).*

Send SMS Message

You can configure SMS messages to be sent when an event occurs and can customize the message.

Messages consist of a combination of free text and BCM2 placeholders. The placeholders represent information which is pulled from the BCM2 and inserted into the message.

A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged into the BCM2 in order to send SMS messages. See *Connecting a GSM Modem* (on page 54).

Note: The BCM2 cannot receive SMS messages.

For example:

`[USERNAME] logged into the device on [TIMESTAMP]`

translates to

`JQPublic logged into the device on 2012-January-30 21:00`

For a list and definition of available variables, see *Email and SMS Message Placeholders* (on page 227).

▶ **Operation:**

1. Choose Device Settings > Event Rules > .
2. Select "Send SMS message" from the Action list.
3. In the Recipient Phone Number field, specify the phone number of the recipient.
4. Select the Use Custom Log Message checkbox, and then create a custom message in the provided text box.
   - When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just click the desired placeholder. For details, see *Email and SMS Message Placeholders* (on page 227).
   - To start a new line in the text box, press Enter.
   - If needed, you can resize the text box by dragging the bottom-right corner.

Note: Only the 7-bit ASCII charset is supported for SMS messages.

Send Snapshots via Email

This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ![New Action].

2. Select "Send snapshots via email" from the Action list.

3. In the "Recipient Email Addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.

4. To use the SMTP server specified on the SMTP Server page, make sure the "Use custom SMTP Server" checkbox is NOT selected.

   To use a different SMTP server, select this checkbox. The fields for customized SMTP settings appear. For information on each field, see *Configuring SMTP Settings* (on page 160).

5. Select the webcam that is capturing the images you want sent in the email.

6. Adjust the values of the following:

   ▪ Number of Snapshots - the number of snapshots to be taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.

   ▪ Snapshots per Mail - the number of snapshots to be sent at one time in the email.

   ▪ Time Before First Snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.

   ▪ Time Between Snapshots - the amount of time in seconds between when each snapshot is taken.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ![New Action].

2. Select "Send SNMP notification" from the Action list.

3. Select the type of SNMP notification. See either procedure below according to your selection.

▶ **To send SNMP v2c notifications:**

1. In the Notification Type field, select SNMPv2c Trap or SNMPv2c Inform.

2. For SNMP INFORM communications, leave the resend settings at their default or do the following:

   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.

4. In the Port fields, enter the port number used to access the device(s).

5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the BCM2 and all SNMP management stations.

Tip: An SNMP v2c notification action permits only a maximum of three SNMP destinations. To assign more than three SNMP destinations to a specific rule, first create several SNMP v2c notification actions, each of which contains completely different SNMP destinations, and then add all of these SNMP v2c notification actions to the same rule.

▶ **To send SNMP v3 notifications:**

1. In the Notification Type field, select SNMPv3 Trap or SNMPv3 Inform.

2. For SNMP TRAPs, the engine ID is prepopulated.

3. For SNMP INFORM communications, leave the resend settings at their default or do the following:

   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:

a. Host name

b. Port number

c. User ID for accessing the host -- make sure the User ID has the SNMPv3 permission.

d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

Start or Stop a Lua Script
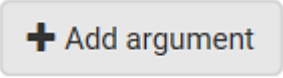
If you have created or loaded a Lua script file into the BCM2, you can have that script automatically run or stop in response to a specific event.

For instructions on creating or loading a Lua script into this product, see *Lua Scripts* (on page 245).

▶ **To automatically start or stop a Lua script:**

1. Choose Device Settings > Event Rules > New Action.

2. Select "Start/stop Lua script" from the Action list.

3. In the Operation field, select Start Script or Stop Script.

4. In the Script field, select the script that you want it to be started or stopped when an event occurs.

- No script is available if you have not created or loaded it into the BCM2.

5. To apply different arguments than the default, do the following. Note that the newly-added arguments will override this script's default arguments.

   a. Click **+ Add argument** .

   b. Type the key and value.

   c. Repeat the same steps to enter more arguments as needed.

      - To remove any existing argument, click **–** adjacent to it.

Switch LHX/SHX

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See *Miscellaneous* (on page 250).

Use this action to switch the LHX/SHX on or off when, for example, temperature thresholds are reached.

▶ **Operation:**

1. Choose Device Settings > Event Rules > **+ New Action** .
2. Select "Switch LHX/SHX" from the Action list.
3. In the Operation field, select Turn LHX/SHX On or Turn LHX/SHX Off.
4. In the Available LHX/SHX field, select the LHX/SHX device to be turned on or off. To select all available LHX/SHX devices, click Select All.

   To remove any LHX/SHX device from the Selected LHX/SHX field, click that device's ✖. To remove all devices, click Deselect All.

Switch Outlets

The "Switch outlets" action is available only when your BCM2 is outlet-switching capable. This action turns on, off or power cycles a specific outlet.

▶ **Operation:**

1. Choose Device Settings > Event Rules > **+ New Action** .
2. Select "Switch outlets" from the Action list.
3. In the Operation field, select an operation for the selected outlet(s).
   - Turn Outlet On: Turns on the selected outlet(s).
   - Turn Outlet Off: Turns off the selected outlet(s).

- Cycle Outlet: Cycles power to the selected outlet(s).

4. To specify the outlet(s) where this action will be applied, select them one by one from the Available Outlets list.

   - To add all outlets, click Select All.

5. To remove any outlets from the Selected Outlets field, click that outlet's ✖.

   - To remove all outlets, click Deselect All.

6. If "Turn Outlet On" or "Cycle Outlet" is selected in step 3, you can choose to select the "Use sequence order and delays" checkbox so that all selected outlets will follow the power-on sequence defined on the page of Outlets.

Switch Peripheral Actuator

If you have any actuator connected to the BCM2, you can set up the BCM2 so it automatically turns on or off the system controlled by the actuator when a specific event occurs.

Note: For information on connecting actuators, see **DX Sensor Packages** (on page 37).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select "Switch peripheral actuator" from the Action list.

3. In the Operation field, select an operation for the selected actuator(s).

   - Turn On: Turns on the selected actuator(s).

   - Turn Off: Turns off the selected actuator(s).

4. To select the actuator(s) where this action will be applied, select them one by one from the Available Actuators list.

   - To add all actuators, click Select All.

5. To remove any selected actuator from the Selected Actuators field, click that actuator's ✖.

   - To remove all actuators, click Deselect All.

Syslog Message

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up - UDP, TCP or TLS over TCP.

The BCM2 may or may not detect the syslog message transmission failure. If yes, it will log this syslog failure as well as the failure reason in the event log. See *Viewing or Clearing the Local Event Log* (on page 253).

▶ **Operation:**

1. Choose Device Settings > Event Rules > .
2. Select "Syslog message" from the Action list.
3. In the Syslog Server field, specify the IP address to which the syslog is forwarded.
4. In the Transport Protocol field, select one of the syslog protocols: TCP, UDP or TCP+TLS. The default is UDP.

Transport protocols	Next steps
UDP	▪ In the UDP Port field, type an appropriate port number. Default is 514. ▪ Select the "Legacy BSD Syslog Protocol" checkbox if applicable.
TCP	NO TLS certificate is required. Type an appropriate port number in the TCP Port field.

TCP+TLS	A TLS certificate is required. Do the following:
	a. Type an appropriate port number in the "TCP Port" field. Default is 6514.
	
	b. In the CA Certificate field, click to select a TLS certificate. After installing the certificate, you may:
	  ▪ Click Show to view its contents.
	  ▪ Click Remove to delete it if it is inappropriate.
	c. Determine whether to select the "Allow expired and not yet valid certificates" checkbox.
	  ▪ To always send the event message to the specified syslog server as long as a TLS certificate is available, select this checkbox.
	  ▪ To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

Scheduling an Action

An action can be regularly performed at a preset time interval instead of being triggered by a specific event. For example, you can make the BCM2 report the reading or state of a specific sensor regularly by scheduling the "Send Sensor Report" action.

When scheduling an action, make sure you have a minimum of 1-minute buffer between this action's creation and first execution time. Otherwise, the scheduled action will NOT be performed at the specified time when the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling it at 10:59 am or earlier.

If the needed action is not available yet, create it first. See *Available Actions* (on page 207).

▶ **Operation:**

1. Choose Device Settings > Event Rules >
   ✚ New Scheduled Action.

2. To select any action(s), select them one by one from the Available Actions list.

   ▪ To select all available actions, click Select All.

3. To remove any action(s) from the Selected Actions field, click that action's ✖.

   ▪ To remove all actions, click Deselect All.

4. Select the desired frequency in the Execution Time field, and then specify the time interval or a specific date and time in the field(s) that appear.

Execution time	Frequency settings
Minutes	Click the Frequency field to select an option. The frequency ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	Type a value in the Minute field, which is set to either of the following: ▪ The Minute field is set to 0 (zero). Then the action is performed at 1:00 am, 2:00 am, 3:00 am and so on. ▪ The Minute field is set to a non-zero value. For example, if it is set to 30, then the action is performed at 1:30 am, 2:30 am, 3:30 am and so on.
Daily	Type values or click ∧ ∨. The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. | 12	:	00	AM | For example, if you specify 01:30PM, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. ▪ Days range from Sunday to Saturday. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.
Monthly	Both the date and time must be specified for the monthly option. ▪ The dates range from 1 to 31. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. Note that NOT every month has the date 31, and February in particular does not have the date 30 and probably even 29. Check the calendar when selecting 29, 30 or 31.

Execution time	Frequency settings
Yearly	This option requires three settings: ▪ Month - January through December. ▪ Day of month - 1 to 31. ▪ Time - the value is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.

An example of the scheduled action is available in the section titled *Send Sensor Report Example* (on page 226).

Send Sensor Report Example

To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

▶ **Steps:**

1. Click ![New Action] to create a 'Send email' action that sends an email to the desired recipient(s). For details, see *Send Email* (on page 214).
   - In this example, this action is named *Email a Sensor Report*.
   - If intended, you can customize the email messages in this action.

2. Click ![New Action] to create a 'Send sensor report' action that includes the 'Email a Sensor Report' action as its destination action. For details, see *Send Sensor Report* (on page 215).
   - In this example, this action is named *Send Temperature Sensor Readings*.
   - You can specify more than one temperature sensor as needed in this action.

3. Click ![New Scheduled Action] to create a timer for performing the 'Send Temperature Sensor Readings' action hourly. For details, see *Scheduling an Action* (on page 224).
   - In this example, the timer is named *Hourly Temperature Sensor Reports*.
   - To perform the specified action at 12:30 pm, 01:30 pm, 02:30 pm, and so on, select Hourly, and set the Minute to 30.

Then the BCM2 will send out an email containing the specified temperature sensor readings hourly every day.

Whenever you want the BCM2 to stop sending the temperature report, simply deselect the Enabled checkbox in the timer.

Email and SMS Message Placeholders

Actions of "Send email" and "Send SMS message" allow you to customize event messages. See *Send Email* (on page 214) or *Send SMS Message* (on page 217).

When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Simply drag the scroll bar and then click the desired placeholder to insert it into the custom message. Or you can type a keyword in the "search" box to quickly find the desired placeholder.

If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

To make the Event Context Information disappear, click anywhere outside its window.

Following are placeholders that can be used in custom messages.

Placeholder	Definition
[ACTIVEINLET]	The label of the newly activated inlet
[AMSBLADESLOTPOSITION]	The (horizontal) slot position, an action applies to
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDOPMODE]	The LED operating mode
[AMSNAME]	The name of an asset strip
[AMSNUMBER]	The numeric ID of an asset strip
[AMSRACKUNITPOSITION]	The (vertical) rack unit position, an action applies to
[AMSSTATE]	The human readable state of an asset strip
[AMSTAGID]	The asset tag ID
[CIRCUITCTRATING]	The circuit CT rating
[CIRCUITCURRENTRATING]	The circuit current rating
[CIRCUITNAME]	The circuit name
[CIRCUITPOLE]	The circuit power line identifier

Placeholder	Definition
[CIRCUITSENSOR]	The circuit sensor name
[CIRCUIT]	The circuit identifier
[CONFIGPARAM]	The name of a configuration parameter
[CONFIGVALUE]	The new value of a parameter
[DATETIME]	The human readable timestamp of the event occurrence
[DEVICEIP]	The IP address of the device, the event occurred on
[DEVICENAME]	The name of the device, the event occurred on
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot
[EXTSENSOR]	The peripheral device identifier
[IFNAME]	The human readable name of a network interface
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[INLET]	The power inlet label
[ISASSERTED]	Boolean flag whether an event condition was entered (1) or left (0)
[LDAPERRORDESC]	An LDAP error occurred
[LHXFANID]	The ID of a fan connected to an LHX/SHX
[LHXPOWERSUPPLYID]	The ID of an LHX/SHX power supply
[LHXSENSORID]	The ID of an LHX/SHX sensor probe
[MONITOREDHOST]	The name or IP address of a monitored host
[OCPSENSOR]	The overcurrent protector sensor name
[OCP]	The overcurrent protector label
[OLDVERSION]	The firmware version the device is being upgraded from

Placeholder	Definition
[OUTLETNAME]	The outlet name
	Note: If any outlet does not have a name, neither an outlet name nor an outlet number will be shown in the custom message for it. Therefore, it is recommended to check the availability of all outlet names if intending to use this placeholder.
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[OUTLET]	The outlet label
[PDUPOLESENSOR]	The sensor name for a certain power line
[PDUSENSOR]	The PDU sensor name
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The phone number an SMS was sent to
[PORTID]	The label of the external port, the event triggering device is connected to
[PORTTYPE]	The type of the external port (for example, 'feature' or 'auxiliary'), the event triggering device is connected to
[POWERMETERPOLE]	The PMC power meter line identifier
[POWERMETERSENSOR]	The PMC power meter sensor name
[POWERMETER]	The PMC power meter ID
[RADIUSERRORDESC]	A Radius error occurred
[ROMCODE]	The rom code of an attached peripheral device
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREADING]	The value of a sensor reading
[SENSORREPORT]	The formatted sensor report contents
[SENSORSTATENAME]	The human readable state of a sensor
[SMTPRECIPIENTS]	The list of recipients, an SMTP message was sent to
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SysContact as configured for SNMP
[SYSLOCATION]	SysLocation as configured for SNMP

Placeholder	Definition
[SYSNAME]	SysName as configured for SNMP
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[TRANSFERSWITCHREASON]	The transfer reason
[TRANSFERSWITCHSENSOR]	The transfer switch sensor name
[TRANSFERSWITCH]	The transfer switch label
[UMTARGETROLE]	The name of a user management role, an action was applied on
[UMTARGETUSER]	The user, an action was triggered for
[USERIP]	The IP address, a user connected from
[USERNAME]	The user who triggered an action
[VERSION]	The firmware version the device is upgrading to

Editing or Deleting a Rule/Action

You can change the settings of an event rule, action or scheduled action, or delete them.

Exception: Some settings of the built-in event rules or actions are not user-configurable. Besides, you cannot delete built-in rules and actions. See **Built-in Rules and Rule Configuration** *(on page 191) or* **Available Actions** *(on page 207).*

▶ **To edit or delete an event rule, action or scheduled action:**

1. Choose Device Settings > Event Rules.
2. Click the desired one in the list of rules, actions or scheduled actions. Its setup page opens.
3. Perform the desired action.
   ▪ To modify settings, make necessary changes and then click Save.
   ▪ To delete it, click 🗑 Delete on the top-right corner. Then click Delete on the confirmation message.

Sample Event Rules

Sample PDU-Level Event Rule

In this example, we want the BCM2 to record the firmware upgrade failure in the internal log when it happens.

The event rule involves:

- Event: Device > Firmware update failed
- Action: System Event Log Action

▶ **To create this PDU-level event rule:**

1. For an event at the PDU level, select "Device" in the Event field.

2. Select "Firmware update failed" so that the BCM2 responds to the event related to firmware upgrade failure.

3. To make the BCM2 record the firmware update failure event in the internal log, select "System Event Log Action" in the Available Actions field.

Sample Outlet-Level Event Rule

In this example, we want the BCM2 to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

The event rule involves:

- Event: Outlet > Outlet 3 > Sensor > Any sub-event
- Action: System SNMP Notification Action

▶ **To create this outlet-level event rule:**

1. For an event at the outlet level, select "Outlet" in the Event field.

2. Select "Outlet 3" because that is the desired outlet.

3. Select "Sensor" to refer to sensor-related events.

4. Select "Any sub-event" to include all events related to all sensors of this outlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.

5. To make the BCM2 send SNMP notifications, select "System SNMP Notification Action" in the Available Actions field.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See **Enabling and Configuring SNMP** *(on page 271).*

Then the SNMP notifications are sent when:

- Any numeric sensor's reading enters the warning or critical range.

- Any sensor reading or state returns to normal.
- Any sensor becomes unavailable.
- The active energy sensor is reset.
- Any state sensor changes its state.

For example, when the outlet 3's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Inlet-Level Event Rule

In this example, we want the BCM2 to send SNMP notifications to the SNMP manager for any sensor change event of the Inlet I1.

The event rule involves:

- Event: Inlet > Sensor > Any sub-event
- Action: System SNMP Notification Action

▶ **To create the above event rule:**

1. For an event at the inlet level, select "Inlet" in the Event field.
2. Select "Sensor" to refer to sensor-related events.
3. Select "Any sub-event" to include all events related to all sensors of this inlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
4. To make the BCM2 send SNMP notifications, select "System SNMP Notification Action" in the Available Actions box.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See **Enabling and Configuring SNMP** *(on page 271).*

Then the SNMP notifications are sent when:

- Any numeric sensor's reading enters the warning or critical range.
- Any sensor reading or state returns to normal.
- Any sensor becomes unavailable.
- The active energy sensor is reset.

For example, when the Inlet I1's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Environmental-Sensor-Level Event Rule

This section applies to outlet-switching capable models only.

In this example, we want BCM2 to activate the load shedding function when a contact closure sensor enters the alarmed state. This event rule requires creating a new action before creating the rule.

▶ **Step 1: create a new action for activating the load shedding**

1. Choose Device Settings > Event Rules > ➕ **New Action**.
2. In this illustration, assign the name "Activate Load Shedding" to the new action.
3. In the Action field, select "Change load shedding state."
4. In the Operation field, select Start Load Shedding.
5. Click Create to finish the creation.

After the new action is created, follow the procedure below to create an event rule that triggers the load shedding mode when the contact closure sensor enters the alarmed state. This event rule involves the following:

*   Event: Peripheral Device Slot > Slot 1 > State Sensor/Actuator > Alarmed/Open/On
*   Trigger condition: Alarmed
*   Action: Activate Load Shedding

▶ **Step 2: create the contact closure-triggered load shedding event rule**

1. Click ➕ **New Rule** on the Event Rules page.
2. In this illustration, assign the name "Contact Closure Triggered Load Shedding" to the new rule.
3. In the Event field, select "Peripheral Device Slot" to indicate we are specifying an event related to the environmental sensor package.
4. Select the ID number of the desired contact closure sensor. In this illustration, the ID number of the desired contact closure sensor is 1, so select Slot 1.

    Note: ID numbers of all sensors/actuators are available on the Peripherals page. See **Peripherals** *(on page 90).*

5. Select "State Sensor/Actuator" because the contact closure sensor is a state sensor.

6. Select "Alarmed" since we want the BCM2 to respond when the selected contact closure sensor changes its state related to the "alarmed" state.

7. In the "Trigger condition" field, select the Alarmed/Open/On radio button so that the action is taken only when the contact closure sensor enters the alarmed state.

8. Select "Activate Load Shedding" from the Available Actions list.

A Note about Infinite Loop

You should avoid building an infinite loop when creating event rules.

The infinite loop refers to a condition where the BCM2 keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one more event.

Example 1

This example illustrates an event rule which continuously causes the BCM2 to send out email messages.

Event selected	Action included
Device > Sending SMTP message failed	Send email

Example 2

This example illustrates an event rule which continuously causes the BCM2 to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send email

Example 3

This example illustrates a situation where two event rules combined regarding the outlet state changes causes the BCM2 to continuously power cycle outlets 1 and 2 in turn.

Event selected	Action included
Outlet > Outlet 1 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 2 (Switch outlets --> Cycle Outlet --> Outlet 2)

Event selected	Action included
Outlet > Outlet 2 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 1 (Switch outlets --> Cycle Outlet --> Outlet 1)

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the BCM2 to generate an alert. The measurement then returns to a value within the threshold, but the BCM2 does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the BCM2 uses. See *"To De-assert" and Deassertion Hysteresis* (on page 86).

Setting Data Logging

The BCM2 can store 120 measurements for each sensor in a memory buffer. This memory buffer is known as the data log. Sensor readings in the data log can be retrieved using SNMP.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since the BCM2 internal sensors are measured every second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in the log gets overwritten.

Whenever measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

Note: The BCM2 device's SNMP agent must be enabled for this feature to work. See **Enabling and Configuring SNMP** *(on page 271). In addition, using an NTP time server ensures accurately time-stamped measurements.*

By default, data logging is enabled. You must have the "Administrator Privileges" or "Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration" permissions to change the setting.

▶ **To configure the data logging feature:**

1. Choose Device Settings > Data Logging.

2. To enable the data logging feature, select the "Enable" checkbox in the General Settings section.

3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.

4. Verify that all sensor logging is enabled. If not, click Enable All at the bottom of the page to have all sensors selected.

   ▪ You can also click the topmost checkbox labeled "Logging Enabled" in the header row of each section to select all sensors of the same type.

   ▪ If any section's number of sensors exceeds 35, the remaining sensors are listed on next page(s). If so, a pagination bar similar to the following diagram displays in this section, which you can click any button to switch between pages.

5. Click Save. This button is located at the bottom of the page.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the BCM2, it is NOT recommended to do so.

Configuring Data Push Settings

You can push the sensor or asset strip data to a remote server for data synchronization. The data will be sent in JSON format using HTTP POST requests. You need to set up the destination and authentication for data push on the BCM2.

For instructions on connecting asset strips, see *Connecting Asset Management Strips* (see "*Connecting Asset Management Sensors*" on page 46).

After configuring the destination and authentication settings, do either or both of the following:

• To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule.

• To push the data at a regular interval, schedule the data push action. See *Event Rules and Actions* (on page 190).

▶ **To configure data push settings:**

1. Choose Device Settings > Data Push.

2. To specify a destination, click .

3. Do the following to set up the URL field.

a. Click ⬍ to select *http* or *https*.

b. Type the URL or host name in the accompanying text box.

4. If selecting https, a CA certificate is required for making the connection. Click **Browse...** to install it. Then you can:

- Click Show to view the certificate's content.
- Click Remove to delete the installed certificate if it is inappropriate.

5. If the destination server requires authentication, select the Use Authentication checkbox, and enter the following data.

- User name
- Password

6. In the Entry Type field, determine the data that will be transmitted.

- Asset management tag list: Transmit the information of the specified asset strip(s), including the general status of the specified strip(s) and a list of asset tags. The asset tags list also includes those on blade extension strips, if any.

- Asset management log: Transmit the log of all asset strips, which is generated when there are changes made to asset tags and asset strips, including asset tag connection or disconnection events.

- Sensor log: Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/actuators that you have selected on the Data Logging page. See *Setting Data Logging* (on page 235).

7. If "Asset management tag list" is selected in the above step, specify the asset strip(s) whose information to send. For BCM2 with only one FEATURE port, only one asset strip is available.

- To specify the asset strip(s), select them one by one from the Available AMS Ports list. Or click Select All to add all.

- To remove the asset strip(s), click that asset strip's ✖ in the Selected AMS Ports field. Or click Deselect All to remove all.

8. Click Create.

9. Repeat the same steps for additional destinations.

▶ **To modify or delete data push settings:**

1. On the Data Push page, click the one you want in the list.

2. Perform either action below.

- To modify settings, make necessary changes and then click Save.

- To delete it, click , and then confirm it on the confirmation message.

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the BCM2 device continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed.

This function is especially useful when you are not located in an area with Internet connectivity.

BCM2 can monitor the accessibility of any IT device, such as database servers, remote authentication servers, power distribution units (PDUs), and so on. It supports monitoring a maximum of 8 devices.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings for optimal results.

Tip: To make the BCM2 automatically log, send notifications or perform other actions for any server monitoring events, you can create event rules. See **Event Rules and Actions** *(on page 190). An example is available in* **Example: Ping Monitoring and SNMP Notifications** *(on page 240).*

▶ **To add IT equipment for ping monitoring:**

1. Choose Device Settings > Server Reachability.
2. Click .
3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.
4. Configure the following.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.
Number of successful pings to enable feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait time after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).

Field	Description
Wait time after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time before resuming pinging after failure	The wait time before the BCM2 resumes pinging after the monitored equipment is declared "Unreachable." Valid range is 1 to 1200 (seconds).
Number of consecutive failures before disabling feature (0 = unlimited)	The number of times the monitored equipment is declared "Unreachable" consecutively before the BCM2 disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. Click Create.

6. To add more IT devices, repeat the same steps.

In the beginning, the status of the added IT equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before the BCM2 can declare that the monitored device is reachable or unreachable.

▶ **To check the server monitoring states and results:**

1. After adding IT equipment for monitoring, all IT devices are listed on the Server Reachability page.

2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.

3. The column labeled "Status" indicates the accessibility of each monitored equipment.

Status	Description
Reachable	The monitored equipment is accessible.
Unreachable	The monitored equipment is inaccessible.
Waiting for reliable connection	The connection between the BCM2 device and the monitored equipment is not reliably established yet.

Editing or Deleting Ping Monitoring Settings

You can edit the ping monitoring settings of any IT device or simply delete it if no longer needed.

▶ **To modify or delete any monitored IT device:**

1. Choose Device Settings > Server Reachability.

2. Click the desired one in the list.

3. Perform the desired action.

   ▪ To modify settings, make necessary changes and then click Save. For information on each field, see *Monitoring Server Accessibility* (on page 238).

   ▪ To delete it, click 🗑 on the top-right corner.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your BCM2 to make sure that PDU is properly operating all the time, and the BCM2 must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power sources are different between your BCM2 and the monitored PDU.

This requires the following two steps.

▶ **Step 1: Set up the ping monitoring for the target PDU**

1. Choose Device Settings > Server Reachability.

2. Click ➕ **Monitor New Server**.

3. Ensure the "Enable ping monitoring for this server" checkbox is selected.

4. Enter the data shown below.

   ▪ Enter the server's data.

Field	Data entered
IP address/hostname	192.168.84.95

   ▪ To make the BCM2 declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3
Wait time after successful ping	5

- To make the BCM2 declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 seconds * 3 pings), enter the following data.

Field	Data entered
Wait time after unsuccessful ping	4
Number of consecutive unsuccessful pings for failure	3

- To make the BCM2 stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared. After 60 seconds, the BCM2 will re-ping the target PDU, enter the following data.

Field	Data entered
Wait time before resuming pinging after failure	60

- The "Number of consecutive failures before disabling feature (0 = unlimited)" can be set to any value you want.

5. Click Create.

▶ **Step 2: Create an event rule to send SNMP notifications for the target PDU**

1. Choose Device Settings > Event Rules.
2. Click ➕ New Rule.
3. Select the Enabled checkbox to enable this new rule.
4. Configure the following.

Field/setting	Data specified
Rule name	Send SNMP notifications for PDU (192.168.84.95) inaccessibility
Event	Choose Server Monitoring > 192.168.84.95 > Unreachable
Trigger condition	Select the Unreachable radio button

This will make the BCM2 react only when the target PDU becomes inaccessible.

5. Select the System SNMP Notification Action.

Note: If you have not configured the System SNMP Notification Action to specify the SNMP destination(s), see **Editing or Deleting a Rule/Action** *(on page 230).*

Front Panel Settings

You can set up the default mode of the front panel display, and front panel functions for outlet switching, actuator control, or RCM self-test.

Note that available front panel settings are model dependent.

- Outlet switching -- available on outlet-switching capable models only.
- Actuator control -- available on all models.
- Default front panel mode setup -- available on all models, except for the PX3-3000 series, which does NOT provide inlet sensor information.
- RCM self-test -- available on those models which support residual current monitoring. See BCM2 Models with Residual Current Monitoring.

▶ **To configure the front panel settings:**

1. Choose Device Settings > Front Panel.
2. Configure the following:
   - To configure the default view of the LCD display, select one mode below.

Note: The default view is shown in the automatic mode. See Automatic and Manual Modes.

Mode	Data entered
Automatic mode	The LCD display cycles through both the inlet and overcurrent protector information. This is the default. Overcurrent protector information is available only when you BCM2 has overcurrent protectors.
Inlet overview	The LCD display cycles through the inlet information only.

- To enable the front panel outlet-switching function, select the "Outlet switching" checkbox.
- To enable the front panel actuator-control function, select the "Peripheral actuator control" checkbox.
- By default the front panel RCM self-test function, if available, is enabled. See Disabling or Enabling Front Panel RCM Self-Test.

3. Now you can turn on or off outlets/actuators by operating the front panel. See Power Control and *Peripherals* (on page 21).

Configuring the Serial Port

You can change the bit rate of the serial port labeled CONSOLE / MODEM on the BCM2. The default bit rate for both console and modem operation is 115200 bps.

The BCM2 supports using the following devices via the serial interface:

- A computer or Raritan KVM product for console management.
- An analog modem for remote dial-in and access to the CLI.
- A GSM modem for sending out SMS messages to a cellular phone.

Bit-rate adjustment may be necessary. Change the bit rate before connecting the supported device to the BCM2 through the serial port, or there are communication problems.

Note: The serial port bit-rate change is required when the BCM2 works in conjunction with Raritan's Dominion LX KVM switch. Dominion LX only supports 19200 bps for communications over the serial interface.

You can set diverse bit-rate settings for console and modem operations. Usually the BCM2 can detect the device type, and automatically apply the preset bit rate.

The BCM2 will indicate the detected device in the Port State section of the Serial Port page. For example, if an analog modem is detected, the Port State section looks similar to the following.

To configure serial port or modem settings, choose Device Settings > Serial Port.

▶ **To change the serial port baud rate settings:**

1. Click the "Connected device" field to make the serial port enter an appropriate state.

Options	Description
Automatic detection	The BCM2 automatically detects the type of the device connected to the serial port. Select this option unless your BCM2 cannot correctly detect the device type.
Force console	The BCM2 attempts to recognize that the connected device is set for the console mode.
Force analog modem	The BCM2 attempts to recognize that the connected device is an analog modem.
Force GSM modem	The BCM2 attempts to recognize that the connected device is a GSM modem.

2. Click the Console Baud Rate field to select the baud rate intended for console management.

    Note: For a serial RS-232 or USB connection between a computer and the BCM2, leave it at the default (115200 bps).

3. Click the Modem Baud Rate field to select the baud rate for the modem connected to the BCM2.

The following modem settings/fields appear in the web interface after the BCM2 detects the connection of an analog or GSM modem.

▶ **To configure the analog modem:**

1. Select the "Answer incoming calls" checkbox to enable the remote access via a modem. Otherwise, deselect it.

2. Type a value in the "Number of rings before answering" field to determine the number of rings the BCM2 must wait before answering the call.

▶ **To configure the GSM modem:**

1. Enter the SIM PIN code.

2. Select the "Use custom SMS center number" checkbox if a custom SMS center will be used.

    ▪ Enter the SMS center number in the "SMS center" field.

3. If needed, click Advanced Information to view detailed information about the modem, SIM and mobile network.

4. To test whether the BCM2 can successfully send out SMS messages with the modem settings:

    a. Enter the number of the recipient's phone in the Recipient Phone field.

    b. Click Send SMS Test to send a test SMS message.

Raritan.
A brand of ⬛legrand

Lua Scripts

If you can write or obtain any Lua scripts, you can create or load them into the BCM2 to control its behaviors.

Raritan also provides some Lua scripts examples, which you can load as needed.

Note: Not all Raritan Lua script examples can apply to your BCM2 model. You should read each example's introduction before applying them.
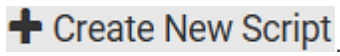
You must have the Administrator Privileges to manage Lua scripts.

Writing or Loading a Lua Script

You can enter or load up to 4 scripts to the BCM2.

*Tip: If you can no longer enter or load a new script after reaching the upper limit, you can either delete any existing script or simply modify/replace an existing script's codes. See **Modifying or Deleting a Script** (on page 249).*

▶ **To write or load a Lua script:**

1. Choose Device Settings > Lua Scripts > .
2. Type a name for this script. Its length ranges between 1 to 63 characters.

    The name must contain the following characters only.
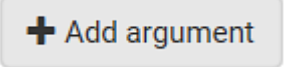
    ▪ Alphanumeric characters

    ▪ Underscore (_)

    ▪ Minus (-)

    Note: Spaces are NOT permitted.

3. Determine whether and when to automatically execute the loaded script.

Checkbox	Behavior when selected
Start automatically at system boot	Whenever the BCM2 reboots, the script is automatically executed.
Restart after termination	The script is automatically executed each time after 10 seconds since the script execution finishes.

4. (Optional) Determine the arguments that will be executed by default.

    a. Click .

245

b.   Type the key and value.

c.   Repeat the same steps to enter more arguments as needed.

- To remove any existing argument, click [**—**] adjacent to it.

Note: Default arguments are overridden by the new arguments specified with the "Start with Arguments" command or with any Lua-script-related event rule. See **Manually Starting or Stopping a Script** *(on page 247) or* **Start or Stop a Lua Script** *(on page 220).*

5.   In the Source Code section, do one of the following. It is recommended to leave the Enable Syntax Highlighting checkbox selected unless you do not need different text colors to identify diverse code syntaxes.

- To write a Lua script, type the codes in the Source Code section.

Source Code

[Load Local File]   [Load Example]

☑ Enable Syntax Highlighting

```
-- Type your codes here.
```
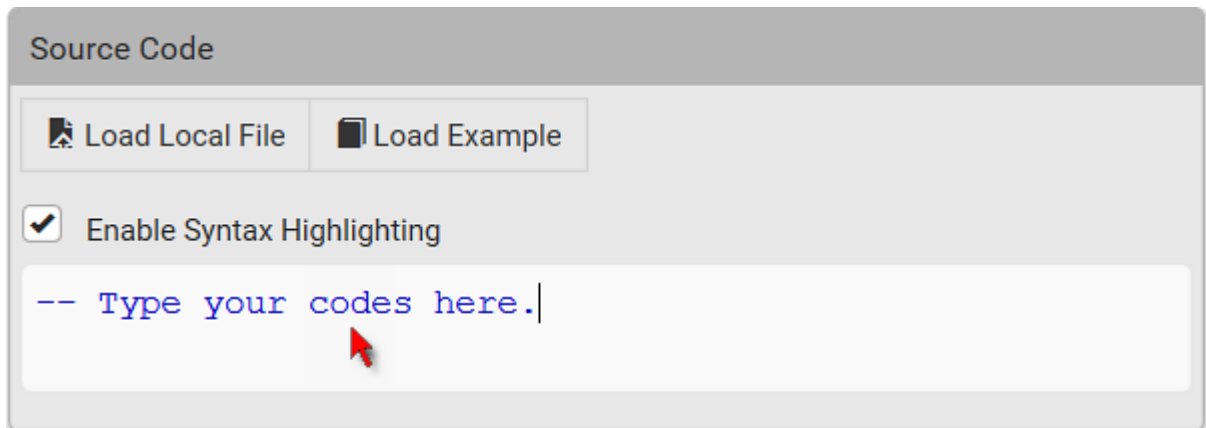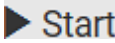
- To load an existing Lua script file, click Load Local File.
- To use one of Raritan's Lua script examples, click Load Example.

Warning: The newly-loaded script will overwrite all existing codes in the Source Code section. Therefore, do not load a new script if the current script meets your needs.

6.   If you chose to load a script or Raritan's example in the previous step, its codes are then displayed in the Source Code section. Double check the codes. If needed, modify the codes to meet your needs.

7.   Click Create.

▶ **Next steps:**

* To execute the newly-added script now, click ![Start], or click ⋮ >
  Start with Arguments. See *Manually Starting or Stopping a Script*
  (on page 247).
* To add more scripts, return to the scripts list by clicking "Lua
  Scripts" again in the Menu, and then repeat the above steps.

Manually Starting or Stopping a Script

You can manually start or stop an existing Lua script at any time.

When starting a script, you can choose to start it either with its default
arguments or with new arguments.

*Tip: To have the BCM2 automatically start or stop a script in response to
an event, create an event rule. See* **Event Rules and Actions** *(on page
190) and* **Start or Stop a Lua Script** *(on page 220).*
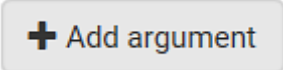
▶ **To manually start a script:**
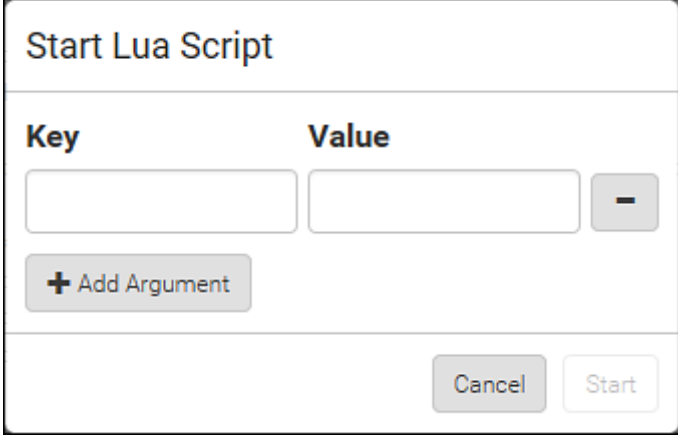
1. Choose Device Settings > Lua Scripts. The Lua scripts list displays.

Lua Scripts			+ Create New Script
Name	**State**	**Autostart**	**Restart**
script-1	Terminated	yes	no
script-2	New	no	yes
script-3	Running	no	no

2. Click the desired script whose state is either 'Terminated' or 'New.'
   For details, see *Checking Lua Scripts States* (on page 249).

3. To start with default arguments, click ![Start].

   To start with new arguments, click ⋮ > Start with Arguments.
   Newly-assigned arguments will override default ones.

4. If you chose "Start with Arguments" in the above step, enter the key
   and value in the Start Lua Script dialog.
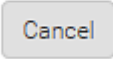
- Click if needing additional arguments.
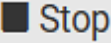
5. Click Start.

6. The script output will be shown in the Script Output section.

    - If needed, click to delete the existing output data.

▶ **To manually stop a script:**

1. Choose Device Settings > Lua Scripts.

2. Click the desired script whose state is either 'Running' or 'Restarting.' For details, see *Checking Lua Scripts States* (on page 249).

3. Click on the top-right corner.

4. Click Stop on the confirmation message.

Checking Lua Scripts States

Choose Device Settings > Lua Scripts to show the scripts list, which indicates the current state and settings of each script.

Lua Scripts			➕ Create New Script
Name	**State**	**Autostart**	**Restart**
script-1	Terminated	yes	no
script-2	New	no	yes
script-3	Running	no	no

▶ **State:**

Four script states are available.

- *New*: The script is never executed since the device boot.
- *Running*: The script is currently being executed.
- *Terminated*: The script was once executed, but stops now.
- *Restarting*: The script will be executed. Only the scripts with the "Restart" column set to "yes" will show this state.

▶ **Autostart:**

This column indicates whether the checkbox labeled "Start automatically at system boot" is enabled. See *Writing or Loading a Lua Script* (on page 245).

▶ **Restart:**

This column indicates whether the checkbox labeled "Restart after termination" is enabled. See *Writing or Loading a Lua Script* (on page 245).

Modifying or Deleting a Script

You can edit an existing script's codes or even replace it with a new script. Or you can simply remove a unnecessary script from the BCM2.

▶ **To modify or replace a script:**

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.

3. Click ⋮ > Edit Script.

4. Make changes to the information shown, except for the script's name, which cannot be revised.

   - To replace the current script, click Load Local File or Load Example to select a new script.

▶ **To delete a script:**

1. Choose Device Settings > Lua Scripts.

2. Click the desired one in the scripts list.

3. Click ⋮ > Delete.

4. Click Delete on the confirmation message.

Miscellaneous

By default, the Schroff LHX/SHX heat exchanger support and Cisco EnergyWise feature implemented on the BCM2 are disabled.

Support needs to be enabled for the LHX/SHX information to appear in the BCM2 web interface. Besides, Schroff LHX/SHX support must be enabled in order for the LHX-MIB to be accessible through SNMP.

If a Cisco® EnergyWise energy management architecture is implemented in your place, you can enable the Cisco EnergyWise endpoint implemented on the BCM2 so that this BCM2 becomes part of the Cisco EnergyWise domain.

To enable either feature, choose Device Settings > Miscellaneous.

▶ **To enable the support for Schroff LHX/SHX:**

1. Select the Schroff LHX/SHX Support checkbox.

2. Click Save in the *Features* section.

3. Click Apply on the confirmation message.

4. The BCM2 reboots.

▶ **To set the Cisco EnergyWise configuration:**

1. Select the Enable EnergyWise checkbox.

2. Configure the following:

Field	Description
Domain name	Type the name of a Cisco EnergyWise domain where the BCM2 belongs - Up to 127 printable ASCII characters are permitted. - Spaces and asterisks are NOT acceptable.

Field	Description
Domain password	Type the authentication password (secret) for entering the Cisco EnergyWise domain ▪ Up to 127 printable ASCII characters are permitted. ▪ Spaces and asterisks are NOT acceptable.
Port	Type a User Datagram Protocol (UDP) port number for communications in the Cisco EnergyWise domain. ▪ Range from 1 to 65535. ▪ Default is 43440.
Polling interval	Type a polling interval to determine how often the BCM2 is queried in the Cisco EnergyWise domain. ▪ Range from 30 to 600 ms. ▪ Default is 180 ms.

3. Click Save in the *EnergyWise* section.

Maintenance

Click 'Maintenance' in the Menu, and the following submenu displays.

Submenu command	Refer to...
Device Information	Device Information
Connected Users	*Viewing Connected Users* (on page 252)
Event Log	*Viewing or Clearing the Local Event Log* (on page 253)
Update Firmware	*Updating the BCM2 Firmware* (on page 254)
Firmware History	*Viewing Firmware Update History* (on page 257)
Bulk Configuration	*Bulk Configuration* (on page 257)
Backup/Restore	*Backup and Restore of Device Settings* (on page 260)
Network Diagnostic	*Network Diagnostics* (on page 262)
Download Diagnostic	*Downloading Diagnostic Information* (on page 263)
Unit Reset	▪ *Rebooting the BCM2 Device* (on page 263) ▪ *Resetting All Settings to Factory Defaults* (on page 264)
About iPDU	*Retrieving Software Packages Information* (on page 265)

Viewing Connected Users

You can check which users have logged in to the BCM2 device and their status. If you have administrator privileges, you can terminate any user's connection to the BCM2.

▶ **To view and manage connected users:**

1. Choose Maintenance > Connected Users. A list of logged-in users displays.

   If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

Column	Description
User name	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.

Client Type	The interface through which the user is being connected to the BCM2.
	▪ Web GUI: Refers to the web interface.
	▪ CLI: Refers to the command line interface (CLI).
	  The information in parentheses following "CLI" indicates how this user is connected to the CLI.
	  - Serial: The local connection, such as the serial RS-232 or USB connection.
	  - SSH: The SSH connection.
	  - Telnet: The Telnet connection.
	▪ Webcam Live Preview: Refers to the live webcame image sessions. See below.

Idle Time	The length of time for which a user remains idle.
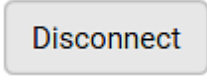
2. To disconnect any user, click the corresponding **Disconnect** .
   a. Click Disconnect on the confirmation message.
   b. The disconnected user is forced to log out.

▶ **If there are live webcam sessions:**

All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window of the sender and two sessions of the remote recipients, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all of the three sessions of a specific URL.

The IP address refers to the IP address of the host where the Primary Standalone Live Preview window exists, NOT the IP address of the other two associated sessions.

For more webcam information, see *Webcam Management* (on page 265).

Viewing or Clearing the Local Event Log

By default, the BCM2 captures certain system events and saves them in a local (internal) event log.

You can view over 2000 historical events that occurred on the BCM2 in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

▶ **To display the local log:**

1. Choose Maintenance > Event Log.

    Each event entry consists of:

    ▪ ID number of the event

    ▪ Date and time of the event

    ▪ Event type

    ▪ A description of the event

2. To view a specific type of events only, select the desired event type in the Filter Event Class field.

    ▪ To refresh the data, press F5 as needed.

3. To go to other pages of the log, click the pagination bar at the bottom of the page.

    ▪ If there are more than 5 pages and the page numbers displayed in the bar does not show the desired one, click [...] to have it show the next or previous five page numbers, if available.

First	Previous	1	2	3	4	5	...	Next	Last

4. If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

▶ **To clear the local log:**

1. Click 🗑 on the top-right corner.

2. Click Clear Log on the confirmation message.

Updating the BCM2 Firmware

Firmware files are available on Raritan website's *Support page* (*http://www.raritan.com/support/*).

When performing the firmware upgrade, the BCM2 keeps each outlet's power status unchanged so no server operation is interrupted. During and after the firmware upgrade, outlets that have been powered on prior to the firmware upgrade remain powered on and outlets that have been powered off remain powered off.

You must be the administrator or a user with the Firmware Update permission to update the BCM2 firmware.

Before starting the upgrade, read the release notes downloaded from the Raritan website's *Support page* (*http://www.raritan.com/support/*). If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

On a multi-inlet PDU (any model with X2 or X3 suffixes), all inlets must be connected to power for the PDU to successfully upgrade its firmware.

Note that firmware upgrade via some mobile devices, such as iPad, requires the use of a file manager app.

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

Important: If you are upgrading an existing USB-cascading chain from a firmware version older than 3.3.10, you must follow specific guidelines to avoid networking issues. See *Upgrade Guidelines for Existing USB-Cascading Chains* **(on page 255).**

▶ **To update the firmware:**

1. Choose Maintenance > Update Firmware.

2. Click **Browse...** to select an appropriate firmware file.

3. Click Upload. A progress bar appears to indicate the upload process.

4. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.

   ▪ If anything is incorrect, click Discard Upload.

5. To proceed with the update, click Update Firmware.

   Warning: Do NOT power off the BCM2 during the update.

6. During the firmware update:

   ▪ A progress bar appears on the web interface, indicating the update status.

   ▪ The front panel display shows the firmware upgrade message. See Showing the Firmware Upgrade Progress.

   ▪ The outlet LEDs flash if the relay boards are being updated. If the firmware update does not include the update of the relay board firmware, outlet LEDs do NOT flash.

   ▪ No users can successfully log in to the BCM2.

   ▪ Other users' operation, if any, is forced to suspend.

7. When the update is complete, the BCM2 resets, and the Login page re-appears.

   ▪ Other logged-in users are logged out when the firmware update is complete.

Important: If you are using the BCM2 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* **(on page 271).**

▶ **Alternatives:**

To use a different method to update the firmware, refer to:

- *Firmware Update via SCP* (on page 444)
- Bulk Configuration or Firmware Upgrade via DHCP/TFTP
- Firmware Upgrade via USB

Upgrade Guidelines for Existing USB-Cascading Chains

- Firmware version 3.3.10 is NOT compatible with old firmware versions in terms of the USB-cascading feature so all devices in a chain must be running version 3.3.10 or later. Otherwise, a networking issue occurs.

  Alternative: You can also choose to have an existing USB-cascading chain keep on running the old firmware without upgrading any device to 3.3.10 or later.

- When upgrading an existing USB-cascading chain from **any version prior to 3.3.10**, the upgrade must start from the last slave device, then the second to last, the third to last, and so on until the master device. Any upgrade without following this sequence results in the networking failure of some cascaded devices.

A Note about Firmware Upgrade Time

The PDU firmware upgrade time varies from unit to unit, depending on various external and internal factors.

External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require upgrade (which depends on the number of outlets). The microcontroller is upgraded only when required. Therefore, the length of firmware upgrade time ranges from approximately 3 minutes (without any microcontroller updated) to almost 7 minutes (with all microcontrollers for 48 outlets updated). Take the above factors into account when estimating the PDU's firmware upgrade time.

The time indicated in this note is for BCM2 web-interface-based upgrades. Upgrades through other management systems, such as Sunbird's Power IQ, may take additional time beyond the control of the PDU itself. This note does not address the upgrades using other management systems.

Full Disaster Recovery

If the firmware upgrade fails, causing the BCM2 device to stop working, you can recover it by using a special utility rather than returning the device to Raritan.

Contact Raritan Technical Support for the recovery utility, which works in Windows XP/Vista/7/10 and Linux. In addition, an appropriate BCM2 firmware file is required in the recovery procedure.

Note: All BCM2 PDUs, except for iX7™ PDUs, can be recovered via either a USB or serial RS-232 connection. For iX7™, disaster recovery can be performed via the USB connection only.

Viewing Firmware Update History

The firmware upgrade history is permanently stored on the BCM2. It remains available even though you perform a device reboot or any firmware update.

▶ **To view the firmware update history:**

1. Choose Maintenance > Firmware History.

   Each firmware update event consists of:

   - Update date and time
   - Previous firmware version
   - Update firmware version
   - Update result

2. If wanted, you can resort the list by clicking the desired column header. See Sorting a List.

Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured BCM2 device to your computer. You can use this configuration file to copy common settings to other BCM2 devices of the same model and firmware version. See *Bulk Configuration Restrictions* (on page 259).

Note that **NO device-specific data is saved** to the bulk configuration file, such as environmental sensors or certain network settings. For a list of device-specific settings that are *not* saved, see *Device-Specific Settings NOT Included* (on page 260).

Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the BCM2 devices in a different time zone than the source device.

Tip: To back up or restore "all" settings of a particular BCM2 device, use the Backup/Restore feature instead. See **Backup and Restore of Device Settings** *(on page 260).*

▶ **To save a bulk configuration file:**

You must have the Administrator Privileges or "Unrestricted View Privileges" to download the configuration.

1. Log in to the BCM2 whose settings you want to copy.
2. Choose Maintenance > Bulk Configuration.
3. Click Download Bulk Configuration.

4. When prompted to open or save the configuration file, click Save.

    ▪ The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

▶ **To perform bulk configuration:**

You must have the Administrator Privileges to upload the configuration.

1. Log in to another BCM2 of the same model running the same firmware.

2. Choose Maintenance > Bulk Configuration.

3. Click to to select the configuration file.

4. Click 'Upload & Restore Bulk Configuration' to copy it.

5. A message appears, prompting you to confirm the operation and enter the admin password.

    Enter the admin password, and click Restore.

6. Wait until the BCM2 device resets and the login page re-appears.

Note: On startup, the BCM2 performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

▶ **The last configuration-copying record:**

If you once copied any bulk configuration or device backup file to the BCM2, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last Restore: 2/24/2017, 6:05:53 PM, Status: OK

▶ **Alternatives:**

To use a different method to perform bulk configuration, refer to:

• *Bulk Configuration via SCP* (on page 445)

• Bulk Configuration or Firmware Upgrade via DHCP/TFTP

• Configuration or Firmware Upgrade with a USB Drive

Bulk Configuration Restrictions

A source device is the BCM2 device where the bulk configuration file is downloaded/saved.

A target device is the BCM2 device that loads this bulk configuration file.

▶ **Restrictions for bulk configuration:**

- The target device must be running the same firmware version as the source device.
- The target device must be of the same model type as the source device.
- Bulk configuration is permitted if the differences between the target and source devices are only "mechanical" designs which are indicated in a model name's suffix as listed below. In the following list, *n* represents a number.

  - PDU chassis color, which is indicated as *Kn*, such as K1 and K601

  - Line cord color, which is indicated as *Bn*, such as B2 and B5

  - Line cord length (meters), which is indicated as *An*, such as A0 and A14

  - Line cord length (centimeters), which is indicated as *Ln*

▶ **Example:**

You can perform bulk configuration between Raritan's PX2-4724-E2N1**K2** and PX2-4724-E2N1**K9**.

- Reason: The two models share the same technical specifications, and the only difference is their chassis colors represented by K2 (blue) and K9 (gray).

Device-Specific Settings NOT Included

The settings saved in the bulk configuration file include user and role configurations, thresholds, event rules, security settings, date/time and so on.

Note: Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the BCM2 devices in a different time zone than the source device.

The bulk configuration file does NOT contain device-specific information, including:

- Device name
- SNMP system name, contact and location
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Names, states and values of environmental sensors and actuators
- TLS certificate
- Server monitoring entries
- Asset strip names and rack unit names
- Outlet names and states

Backup and Restore of Device Settings

Unlike the bulk configuration file, the backup file contains ALL device settings, including device-specific data like device names and network settings. To back up or restore a BCM2 device's settings, you should perform the Backup/Restore feature.

All BCM2 information is captured in the XML backup file except for the device logs and TLS certificate.

Note: To perform bulk configuration among multiple BCM2 devices, use the Bulk Configuration feature instead. See **Bulk Configuration** *(on page 257).*

▶ **To download a backup BCM2 XML file:**

You must have the Administrator Privileges or "Unrestricted View Privileges" to download a backup file.

1. Choose Maintenance > Backup/Restore.
2. Click Download Device Settings. Save the file to your computer.
   - The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

▶ **To restore the BCM2 using a backup XML file:**

You must have the Administrator Privileges to restore the device settings.

1. Choose Maintenance > Backup/Restore.
2. Click [Browse...] to to select the backup file.
3. Click 'Upload & Restore Device Settings' to upload the file.
   ▪ A message appears, prompting you to confirm the operation and enter the admin password.
4. Enter the admin password, then click Restore.
5. Wait until the BCM2 device resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, the BCM2 performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

▶ **The last configuration-copying record:**

If you once copied any bulk configuration or device backup file to the BCM2, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last Restore: 2/24/2017, 6:05:53 PM, Status: OK

▶ **Alternative:**

To use a different method to perform backup/restore, refer to:

- *Backup and Restore via SCP* (on page 446)

Network Diagnostics

The BCM2 provides the following tools in the web interface for diagnosing potential networking issues.

- Ping: The tool is useful for checking whether a host is accessible through the network or Internet.
- Trace Route: The tool lets you find out the route over the network between two hosts or systems.
- List TCP Connections: You can use this function to display a list of TCP connections.

Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** *(on page 439).*

Choose Maintenance > Network Diagnostics, and then perform any function below.

▶ **Ping:**

1. Type values in the following fields.

Field	Description
Network Host	The name or IP address of the host that you want to check.
Number of Requests	A number up to 20. This determines how many packets are sent for pinging the host.

2. Click Run Ping to ping the host. The Ping results are then displayed.

▶ **Trace Route:**

1. Type values in the following fields.

Field/setting	Description
Host Name	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP Packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are then displayed.

▶ **List TCP Connections:**

1. Click the List TCP Connections title bar to show the list.

Downloading Diagnostic Information

Important: This function is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

You can download the diagnostic file from the BCM2 to a client machine. The file is compressed into a .tgz file   and should be sent to Raritan Technical Support for interpretation.

This feature is accessible only by users with Administrative Privileges or Unrestricted View Privileges.

▶ **To retrieve a diagnostic file:**

1. Choose Maintenance > Download Diagnostic >

   Download Diagnostic
   .

2. The system prompts you to save or open the file. Click Save.

3. E-mail this file as instructed by Raritan Technical Support.

Rebooting the BCM2 Device

You can remotely reboot the BCM2 device via the web interface.

Resetting the BCM2 does not interrupt the operation of connected servers because there is no loss of power to outlets. During and after the reboot, outlets that have been powered on prior to the reboot remain powered on, and outlets that have been powered off remain powered off.

> Warning: Rebooting the BCM2 deletes all webcam snapshots that are saved on the BCM2 locally. See *Viewing Saved Snapshots and Managing Storage* (on page 269).

▶ **To reboot the device:**

1. Choose Maintenance > Unit Reset >   **Reboot Unit**   .

2. Click Reboot to restart the BCM2.

3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.

4. When the restart is complete, the login page opens.

Note: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.
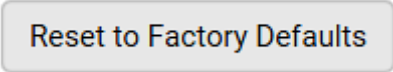
Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings of the BCM2 to factory defaults.

Important: Exercise caution before resetting the BCM2 to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only active energy data and firmware upgrade history are retained.

▶ **To reset the device to factory defaults:**

1. Choose Maintenance > Unit Reset >
    [Reset to Factory Defaults] .

[Factory Reset

Do you really want to reset the device to factory defaults? Saying yes will clear all settings, including the network setup.

Cancel   Factory Reset]
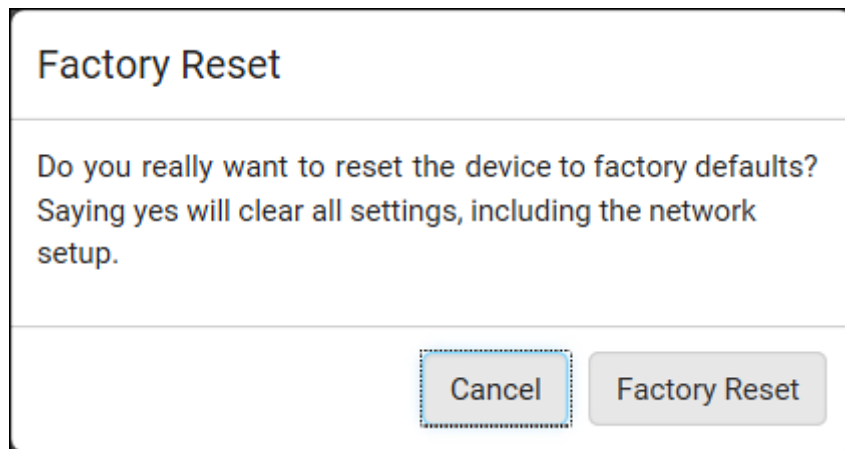
2. Click Factory Reset to reset the BCM2 to factory defaults.
3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.
4. When the reset is complete, the login page opens.

Note: If you are not redirected to the login page after the reset is complete, click the text "this link" in the countdown message.

▶ **Alternative:**

There are two more methods to reset the device to factory defaults.

● Use the "mechanical" reset button

● Perform the CLI command

For details, see *Resetting to Factory Defaults* (on page 449).

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the BCM2 device through the web interface.

▶ **To retrieve the embedded software packages information:**

1. Choose Maintenance > About iPDU. A list of open source packages is displayed.

2. You can click any link to access related information or download any software package.

Webcam Management

The webcam-related menu items appear only when there are webcam(s) connected to the BCM2. See Connecting a Logitech Webcam.

With a Logitech® webcam connected to the BCM2, you can visually monitor the environment around the BCM2 via snapshots or videos captured by the webcam.

- To view snapshots and videos, you need the permission of either "Change Webcam Configuration" or "View Webcam Sanpshots and Configuration."

- To configure webcam settings, you need the "Change Webcam Configuration" permission.

If your webcam supports audio transmission, audio will be available in live videos.

You can manually store snapshots taken from the webcam onto the BCM2 or a remote server. See *Viewing Saved Snapshots and Managing Storage* (on page 269).

Links to snapshots or videos being captured by a webcam can be sent via email or instant message. See *Sending Snapshots or Videos in an Email or Instant Message* (on page 268).

You can create event rules to trigger emails containing snapshots from a webcam. See *Available Actions* (on page 207).

For more information on the Logitech webcam, see the user documentation accompanying it.

Configuring Webcams and Viewing Live Images

To configure the webcam or view live snapshot/video sessions, choose Webcam in the Menu.

▶ **Live Preview:**

1. Click the Live Preview title bar to expand it.
2. The live snapshot/video session captured by the webcam is displayed.
   - The default is to show live snapshots. Interval time and the image captured time are displayed on the top of the image.
3. To save the current image, click Save Snapshot. See *Viewing Saved Snapshots and Managing Storage* (on page 269).
4. To have the live session also displayed in a Primary Standalone Live Preview window, click New Live Preview Window.
   - You can send out this window's URL to share the live image with other users. See *Sending Snapshots or Videos in an Email or Instant Message* (on page 268).
5. To switch between snapshot and video modes, see the *Settings* section below.
   - In the video mode, the number of frames to take per second (fps) and the captured time are displayed on the top of the image.

▶ **Image Controls:**

1. Click the Image Controls title bar to expand it.
2. Adjust the brightness, contrast and saturation by adjusting the corresponding slide bar.
   - Or click "Set to Webcam Defaults" to restore all settings to this webcam's factory defaults.

▶ **Settings:**

1. Click Edit Settings.
2. Enter a name for the webcam. Up to 64 characters are supported.
3. Type the location information in each location field if needed. Up to 63 characters are supported.
4. Select a resolution for the webcam.
   - If you connect two webcams to one USB-A port using a powered USB hub, set the resolution to 352x288 or lower for optimal performance.
5. Select the webcam mode.

- Video - the webcam enters the video mode. Set the Framerate (frames per second) rate.

- Snapshot - the webcam shows static images from the webcam. Set the "Time Between Snapshots" rate as measured in seconds.

6. Click Save. The changes made to the settings are applied to the live session. See the above *Live Preview* section.

Note: The settings changes do not apply to those images captured prior to the changes.

Sending Snapshots or Videos in an Email or Instant Message

Whenever you open a Primary Standalone Live Preview window, a unique URL is generated for this window session. A URL supports a maximum of three sessions. Therefore, you can email or instant message up to two persons this URL. Recipients can then click on the provided link and view live snapshots or videos simultaneously.

Tip: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window of the sender and two sessions of the remote recipients, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all of the three sessions of a specific URL. See **Viewing Connected Users** *(on page 252).*

For explanation of this topic, the message sender is User A and the two recipients are User B and C.

User C is able to access the snapshot or video image via the link in any of the following scenarios:

- The Primary Standalone Live Preview window remains open on User A's computer. If so, even though User A logs out of the web interface or the login session times out, the link remains available.
- Another recipient's live preview session based on the same URL remains open. That is, User B's session remains. If so, even though User A has closed the Primary Standalone Live Preview window, the link remains available.
- Neither User A's Primary Standalone Live Preview window nor User B's session based on the same URL remains open, but the idle timeout period has not expired yet since the last live preview window session was closed. For information on idle timeout, see *Configuring Login Settings* (on page 184).

Tip: When the idle timeout has not expired, the <webcam> user for that live preview URL remains shown on the Connected Users page.

Best Practice

As a best practice, User A should open the live snapshot or video session using a Primary Standalone Live Preview window and keep that window open at least until User C opens the live image session via the link.

Once User C opens the live session via the link, User A can close the Primary Standalone Live Preview window.

User C should let User A know that the link has been opened.

▶ **To send a snapshot or video link via email or instant message:**
1. Open the Webcam page by clicking it in the Menu.

2. Click Live Preview > New Live Preview Window. The live snapshot or video in a standalone live preview window opens. See *Configuring Webcams and Viewing Live Images* (on page 266).

3. Copy the URL from the live preview window, and send it through an email or instant message application.

4. Leave the live preview window open until the recipient opens the snapshot or video via the link.

Viewing Saved Snapshots and Managing Storage

Once a snapshot is saved, it is stored locally on the BCM2 by default. For instructions on saving snapshots, see *Configuring Webcams and Viewing Live Images* (on page 266).

Up to 10 images can be stored onto the BCM2 at once. Unless snapshots are deleted manually, the oldest snapshot is automatically overridden by the newest one when the total of snapshots exceeds 10.

To save more than 10 snapshots, you must save the images on a Common Internet File System (CIFS)/Samba.

Snapshots are saved as JPG files, and named based on the sequential numbers, such as 1.jpg, 2.jpg, 3.jpg and so on.

Warning: Rebooting the BCM2 deletes all webcam snapshots that are saved on the BCM2 locally. See *Viewing Saved Snapshots and Managing Storage* (on page 269).

To view saved images or configure the storage settings, choose Webcam Snapshots in the Menu.

▶ **To view and manage saved images:**

1. Click the snapshot you want to view from the list.

   ▪ If the list of snapshots saved in the specified CIFS/Samba server exceeds one page, you can switch between available pages by clicking the pagination bar on the top.

     If there are more than 5 pages and the page numbers displayed

     in the bar does not show the desired one, click [⋯] to have it show the next or previous five page numbers, if available.

First	Previous	1	2	3	4	5	...	Next	Last
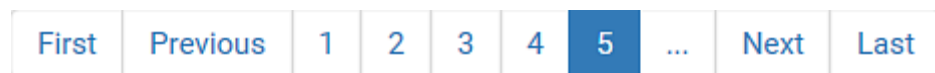
2. The selected snapshot as well as its information, such as captured time and resolution, is displayed on the same page.

3. If the latest saved snapshot is not listed yet, click ⋮ > Refresh on the top of the list.

4. To manually delete any images:

   a. Select the checkboxes of the images you want to remove.

      ▪ To select all images, select the top-most checkbox in the header row.

   b. On the top of the list, click ⋮ > Delete Selected.

   c. Click Delete on the confirmation message.

▶ **To configure the storage settings:**

1. Click ⋮ > Settings.

2. Click the Storage Type field to select the desired storage location and configure as needed.

Storage location	Description
Local	Local means the BCM2. This is default.
CIFS/Samba	Snapshots will be saved on a Common Internet File System/Samba. Configure the following fields for this server: ▪ Server - the desired CIFS/Samba server ▪ Share/Folder - this is the share drive/folder ▪ Username - for server access ▪ Password - for server access

3. In the Capacity field, type values to determine the maximum number of snapshots that can be saved on the selected storage location.

4. Click Save.

Raritan.
A brand of ☐ legrand

Chapter 5   Using SNMP

This SNMP section helps you set up the BCM2 for use with an SNMP manager. The BCM2 can be configured to send traps or informs to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

In This Chapter

Enabling and Configuring SNMP

To communicate with an SNMP manager, you must enable SNMP protocols on the BCM2. By default the "read-only" mode of SNMP v1/v2c is enabled.

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, you must configure the users with the SNMP v3 access permission and set Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between SNMP and the BCM2.

Important: You must download the SNMP MIB for your BCM2 to use with your SNMP manager. See *Downloading SNMP MIB* **(on page 274).**

▶ **To enable SNMP v1/v2c and/or v3 protocols:**

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3, and configure related fields, such as the community strings.
   - If SNMP v3 is enabled, you must determine which users shall have the SNMP v3 access permission. See below.

   For details, see *Configuring SNMP Settings* (on page 159).

▶ **To configure users for SNMP v3 access:**

1. Choose User Management > Users.
2. Create or modify users to enable their SNMP v3 access permission.
   - If authentication and privacy is enabled, configure the SNMP password(s) in the user settings.

   For details, see *Creating Users* (on page 123).

▶ **To enable SNMP notifications:**

1. Choose Device Settings > Network Services > SNMP.

2. In the SNMP Notifications section, enable the SNMP notification feature, and configure related fields. For details, refer to:

   ▪ *SNMPv2c Notifications* (on page 272)
   ▪ *SNMPv3 Notifications* (on page 273)

Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See **Available Actions** *(on page 207).*

SNMPv2c Notifications

1. Choose Device Settings > Network Services > SNMP.

2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.

3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.

4. Select SNMPv2c Trap or SNMPv2c Inform as the notification type.

5. Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of Retries	The number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the BCM2 and all SNMP management stations.

6. Click Save.

SNMPv3 Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.
4. Select SNMPv3 Trap or SNMPv3 Inform as the notification type.
5. For SNMP TRAPs, the engine ID is prepopulated.
6. Type values in the following fields.

Field	Description
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. ▪ Make sure the user has the SNMP v3 access permission.
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of Retries	Specify the number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Security Level	Three types are available. ▪ noAuthNoPriv - neither authentication nor privacy protocols are needed. ▪ AuthNoPriv - only authentication is required. ▪ authPriv - both authentication and privacy protocols are required.

Field	Description
Authentication Protocol, Authentication Passphrase, Confirm Authentication Passphrase	The three fields are available when the security level is set to AuthNoPriv or authPriv. ▪ Select the authentication protocol - MD5 or SHA ▪ Enter the authentication passphrase
Privacy Protocol, Privacy Passphrase, Confirm Privacy Passphrase	The three fields are available when the security level is set to authPriv. ▪ Select the Privacy Protocol - DES or AES ▪ Enter the privacy passphrase and then confirm the privacy passphrase

7. Click Save.

Downloading SNMP MIB

You must download an appropriate SNMP MIB file for successful SNMP communications. Always use the latest SNMP MIB downloaded from the current firmware of your BCM2.

You can download the MIBs from two different pages of the web interface.

▶ **MIB download via the SNMP page:**

1. Choose Device Settings > Network Services > SNMP.
2. Click the Download MIBs title bar.

Download MIBs   ⌄

3. Select the desired MIB file to download.
   ▪ EMD-MIB: The SNMP MIB file for BCM2 power management.
   ▪ ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
   ▪ LHX-MIB: The SNMP MIB file for managing the LHX/SHX heat exchanger(s).
4. Click Save to save the file onto your computer.

▶ **MIB download via the Device Information page:**

1. Choose Maintenance > Device Information.
2. In the Information section, click the desired download link:
   - EMD-MIB
   - ASSETMANAGEMENT-MIB
   - LHX MIB
3. Click Save to save the file onto your computer.

Note: LHX-MIB is available only after the LHX/SHX support has been enabled. See **Miscellaneous** *(on page 250).*

SNMP Gets and Sets

In addition to sending notifications, the BCM2 is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the BCM2, such as the system location, and the current on a specific outlet.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

  Note: The SNMP system name is the BCM2 device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

  The BCM2 does NOT support configuring IPv6-related parameters using the SNMP set requests.

Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom BCM2 MIB.
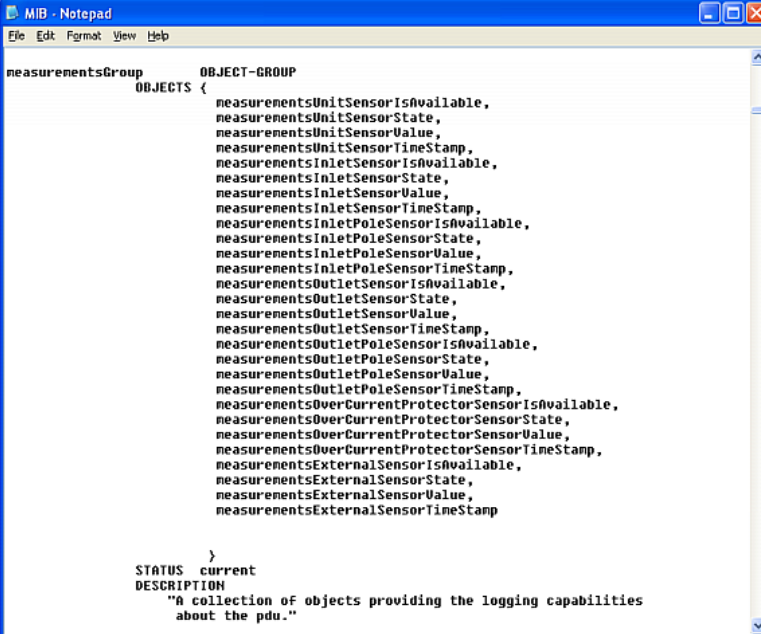
The BCM2 MIB

The SNMP MIB file is required for using your BCM2 device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Layout

Opening the MIB reveals the custom objects that describe the BCM2 system at the unit level as well as at the individual-outlet level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.

For example, the measurementsGroup group contains objects for sensor readings of BCM2 as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the PDU current rating.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which causes the BCM2 to generate a warning and send an SNMP notification when certain parameters are exceeded. See Sensor Threshold Settings for a description of how thresholds work.

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

Configuring NTP Server Settings

Using SNMP, you can change the following NTP server-related settings in the unitConfigurationTable:

- Enable or disable synchronization of the device's date and time with NTP servers (synchronizeWithNTPServer)
- Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer)
- Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (primaryNTPServerAddressType and primaryNTPServerAddress)
- Manually assign the secondary NTP server (optional) (secondaryNTPServerAddressType and secondaryNTPServerAddress)

Tip: To specify the time zone, use the CLI or web interface instead. For the CLI, see **Setting the Time Zone** *(on page 351). For the web interface, see* **Setting the Date and Time** *(on page 187).*

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset -v2c -c private 192.168.84.84
firstNTPServerAddressType = dns firstNTPServerAddress =
"angu.pep.com"
```

Retrieving Energy Usage

You can discover how much energy an IT device consumes by retrieving the Active Energy for the outlet this IT device is plugged into. The Active Energy values are included in the outletSensorMeasurementsTable, along with other outlet sensor readings.

A Note about Enabling Thresholds

When enabling previously disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Chapter 6   Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer a BCM2 device.

CLI commands are case sensitive.

In This Chapter

About the Interface

The BCM2 provides a command line interface that enables data center administrators to perform some basic management tasks.

Using this interface, you can do the following:

- Reset the BCM2 device
- Display the BCM2 and network information, such as the device name, firmware version, IP address, and so on
- Configure the BCM2 and network settings
- Troubleshoot network problems

You can access the interface over a local connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see **Changing Telnet Settings** *(on page 162).*

Logging in to CLI

Logging in via HyperTerminal over a local connection is a little different than logging in using SSH or Telnet.

If a security login agreement has been enabled, you must accept the agreement in order to complete the login. Users are authenticated first and the security banner is checked afterwards.

With HyperTerminal

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 log in using HyperTerminal:**

1. Connect your computer to the BCM2 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

    Tip: For a USB connection, you can determine the COM port by choosing Control Panel > System > Hardware > Device Manager, and locating the "Serial Console" under the Ports group.

3. In the communications program, press Enter to send a carriage return to the BCM2. The Username prompt appears.

    ```
    Username: _
    ```

4. Type a name and press Enter. The name is case sensitive. Then you are prompted to enter a password.

    ```
    Username: admin
    Password: _
    ```

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

Raritan.
A brand of Legrand

After properly entering the password, the # or > system prompt appears. See *Different CLI Modes and Prompts* (on page 283) 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 used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the BCM2.

With SSH or Telnet

You can remotely log in to the command line interface (CLI) 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 *Configuring Network Services* (on page 157) 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* (on page 283) 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 used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the BCM2.

With an Analog Modem

The BCM2 supports remote access to the CLI via a connected analog modem. This feature is especially useful when the LAN access is not available.

▶ **To connect to the BCM2 via the modem:**

1. Make sure the BCM2 has an analog modem connected. See *Connecting an Analog Modem* (on page 55).

2. Make sure the computer you are using has an appropriate modem connected.

3. Launch a terminal emulation program, and configure its baud rate settings according to the baud rate set for the analog modem connected to the BCM2. See *Configuring the Serial Port* (on page 243).

4. Type the following AT command to make a connection with the BCM2.

   ATD<modem phone number>

5. The CLI login prompt appears after the connection is established successfully. Then type the user name and password to log in to the CLI.

▶ **To disconnect from the BCM2:**

1. Return to the modem's command mode using the escape code +++.

2. After the OK prompt appears, type the following AT command to disconnect from the BCM2.

   ATH

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

- User Mode: When you log in as a normal user, who may not have full permissions to configure the BCM2 device, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the BCM2 device, the **#** prompt appears.
- Configuration Mode: You can enter the configuration mode from the administrator or user mode. In this mode, the prompt changes to **config:#** or **config:>** and you can change BCM2 device and network configurations. See *Entering Configuration Mode* (on page 315).
- Diagnostic Mode: You can enter the diagnostic mode from the administrator or user mode. In this mode, the prompt changes to **diag:#** or **diag:>** and you can perform the network troubleshooting commands, such as the ping command. See *Entering Diagnostic Mode* (on page 439).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing a BCM2 device over the local connection.

> When accessing or upgrading multiple BCM2 devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

Help Command

The help (?) command shows a list of main CLI commands available for the current mode. This is helpful when you are not familiar with CLI commands.

▶ **Help command under the administrator mode:**

```
#          ?
```

▶ **Help command under the configuration mode:**

```
config:#    ?
```

▶ **Help command under the diagnostic mode:**

```
diag:#      ?
```

Press Enter after typing the help command, and a list of main commands for the current mode is displayed.

Tip: You can check what parameters are available for a specific CLI command by adding the help command to the end of the queried command. See **Querying Available Parameters for a Command** *(on page 285).*

Querying Available Parameters for a Command

If you are not sure what commands or parameters are available for a particular type of CLI command or its syntax, you can have the CLI show them by adding a space and the help command (?) to the end of that command. A list of available parameters and their descriptions will be displayed.

The following shows a few query examples.

▶ **To query available parameters for the "show" command:**

```
#          show ?
```

▶ **To query available parameters for the "show user" command:**

```
#          show user ?
```

▶ **To query available network configuration parameters:**

```
config:#    network ?
```

▶ **To query available role configuration parameters:**

```
config:#    role ?
```

▶ **To query available parameters for the "role create" command:**

```
config:#    role create ?
```

Showing Information

You can use the show commands to view current settings or the status of the BCM2 device or part of it, such as the IP address, networking mode, firmware version, states or readings of internal or external sensors, user profiles, and so on.

Some "show" commands have two formats: one with the parameter "details" and the other without. The difference is that the command without the parameter "details" displays a shortened version of information while the other displays in-depth information.

After typing a "show" command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt. See **Different CLI Modes and Prompts** *(on page 283).*

Network Configuration

This command shows all network configuration and all network interfaces' information, such as the IP address, MAC address, the Ethernet interface's duplex mode, and the wireless interface's status/settings.

```
#        show network
```

IP Configuration

This command shows the IP-related configuration only, such as IPv4 and IPv6 configuration, address(es), gateway, and subnet mask.

Tip: To show IPv4-only and IPv6-only configuration data, see **IPv4-Only or IPv6-Only Configuration** *(on page 287).*

```
#        show network ip common
```

To show the IP-related configuration of a specific network interface, use the following command.

```
#        show network ip interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Option	Description
ethernet	Show the IP-related configuration of the ETHERNET interface.
wireless	Show the IP-related configuration of the WIRELESS interface.
bridge	Show the IP-related configuration of the BRIDGE interface.

Option	Description
all	Show the IP-related configuration of all interfaces. You can type the CLI command without the word 'all.' For example, *show network ip interface*.

IPv4-Only or IPv6-Only Configuration

To show IPv4-only configuration or IPv6-only configuration, use any of the following commands.

Tip: To show both IPv4 and IPv6 configuration data, see **IP Configuration** *(on page 286).*

▶ **To show all IPv4 configuration:**

```
#      show network ipv4 common
```

▶ **To show all IPv6 configuration:**

```
#      show network ipv6 common
```

▶ **To show the IPv4 configuration of a specific network interface:**

```
#      show network ipv4 interface <ETH>
```

▶ **To show the IPv6 configuration of a specific network interface:**

```
#      show network ipv6 interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Option	Description
ethernet	Show the IPv4 or IPv6 configuration of the ETHERNET interface.
wireless	Show the IPv4 or IPv6 configuration of the WIRELESS interface.
bridge	Show the IPv4 or IPv6 configuration of the BRIDGE interface.
all	Show the IPv4 or IPv6 configuration of all interfaces. You can type the CLI command without the word 'all.' For example, *show network ipv4 interface*.

Network Interface Settings

This command shows the specified network interface's information which is NOT related to IP configuration. For example, the Ethernet port's LAN interface speed and duplex mode, or the wireless interface's SSID parameter and authentication protocol.

```
#       show network interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Option	Description
ethernet	Show the ETHERNET interface's non-IP settings.
wireless	Show the WIRELESS interface's non-IP settings.
bridge	Show the BRIDGE interface's non-IP settings.
all	Show the non-IP settings of all interfaces. You can type the CLI command without the word 'all.' For example, *show network interface*.

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, SSH and Modbus/TCP services, and SNMP settings.

```
#        show network services <option>
```

Variables:

- <option> is one of the options: *all*, *http*, *https*, *telnet*, *ssh*, *snmp*, *modbus* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. *Tip: You can also type the command without adding this option "all" to get the same data.*
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

PDU Configuration

This command shows the PDU configuration, such as the device name, firmware version and model type.

```
#        show pdu
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show pdu details
```

Outlet Information

This command syntax shows the outlet information.

```
#        show outlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show outlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all outlets.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific outlet number	Displays the information for the specified outlet only.

Displayed information:

- Without the parameter "details," only the outlet name is displayed. For PX-2000 series, the outlet state is also displayed.
- With the parameter "details," more outlet information is displayed in addition to the outlet name, such as the outlet rating.

Inlet Information

This command syntax shows the inlet information.

```
#       show inlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show inlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all inlets.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific inlet number	Displays the information for the specified inlet only.
	An inlet number needs to be specified only when there are more than 1 inlet on your PDU.

Displayed information:

- Without the parameter "details," only the inlet's name and RMS current are displayed.
- With the parameter "details," more inlet information is displayed in addition to the inlet name and RMS current, such as the inlet's RMS voltage, active power and active energy.

Overcurrent Protector Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the overcurrent protector information, such as a circuit breaker or a fuse.

```
#        show ocp <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show ocp <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all overcurrent protectors.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific overcurrent protector number	Displays the information for the specified overcurrent protector only.

Displayed information:

- Without the parameter "details," only the overcurrent protector status and name are displayed.
- With the parameter "details," more overcurrent protector information is displayed in addition to status, such as the rating and RMS current value.

Date and Time Settings

This command shows the current date and time settings on the BCM2 device.

```
#       show time
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show time details
```

Default Measurement Units

This command shows the default measurement units applied to the BCM2 web and CLI interfaces across all users, especially those users authenticated through remote authentication servers.

```
#       show user defaultPreferences
```

Note: If a user has set his/her own preferred measurement units or the administrator has changed any user's preferred units, the web and CLI interfaces show the preferred measurement units for that user instead of the default ones after that user logs in to the BCM2. See **Existing User Profiles** *(on page 303) for the preferred measurement units for a specific user.*

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
#       show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show externalsensors <n> details
```

```
External sensor 3 ('Temperature 1')
Sensor type: Temperature
Reading:     31.8 deg C (normal)

Serial number:          AEI0950133
Description:             Not configured
Location:                X Not configured
                         Y Not configured
                         Z Not configured
Position:                Port 1
Using default thresholds: yes
```

Variables:

* <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information of all environmental sensors.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the BCM2 web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

   Note: A state sensor displays the sensor state instead of the reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number, sensor position, and X, Y, and Z coordinates.

Note: DPX sensor packages do not provide chain position information.

Environmental Sensor Package Information

Different from the "`show externalsensors`" commands, which show the reading, status and configuration of an individual environmental sensor, the following command shows the information of all connected environmental sensor packages, each of which may contain more than one sensor or actuator.

```
#      show peripheralDevicePackages
```

Information similar to the following is displayed. An environmental sensor package is a peripheral device package.

```
Peripheral Device Package 1
Serial Number:    AEI7A00022
Package Type:     DPX-T1H1
Position:         Port 1
Package State:    operational
Firmware Version: Not available

Peripheral Device Package 2
Serial Number:    AEI7A00021
Package Type:     DPX-T3H1
Position:         Port 1
Package State:    operational
Firmware Version: Not available
```

Actuator Information

This command syntax shows an actuator's information.

```
#        show actuators <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show actuators <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all actuators.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific actuator number*	Displays the information for the specified actuator only.

* The actuator number is the ID number assigned to the actuator. The ID number can be found using the BCM2 web interface or CLI. It is an integer starting at 1.

Displayed information:

- Without the parameter "details," only the actuator ID, type and state are displayed.
- With the parameter "details," more information is displayed in addition to the ID number and actuator state, such as the serial number and X, Y, and Z coordinates.

Inlet Sensor Threshold Information

This command syntax shows the specified inlet sensor's threshold-related information.

```
#       show sensor inlet <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor inlet <n> <sensor type> details
```

Variables:

- <n> is the number of the inlet whose sensors you want to query. For a single-inlet PDU, <n> is always the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor
lineFrequency	Line frequency sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified inlet sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

Inlet Pole Sensor Threshold Information

This command is only available for a three-phase PDU except for an in-line monitor (PX-3000 series).

This command syntax shows the specified inlet pole sensor's threshold-related information.

```
#       show sensor inletpole <n> <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor inletpole <n> <p> <sensor type> details
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to query. For a single-inlet PDU, <n> is always the number 1.
- <p> is the label of the inlet pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified inlet pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

Overcurrent Protector Sensor Threshold Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the specified overcurrent protector sensor's threshold-related information.

```
#        show sensor ocp <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show sensor ocp <n> <sensor type> details
```

Variables:

- <n> is the number of the overcurrent protector whose sensors you want to query.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified overcurrent protector sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
#        show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show sensor externalsensor <n> details
```

```
External sensor 3 (Temperature):
Reading: 31.8 deg C
State:   normal

Active Thresholds: Sensor specific thresholds

Default Thresholds for Temperature sensors:
Lower critical threshold: 10.0 deg C
Lower warning threshold:  15.0 deg C
Upper warning threshold:  30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples

Sensor Specific Thresholds:
Lower critical threshold: 8.0 deg C
Lower warning threshold:  13.0 deg C
Upper warning threshold:  28.0 deg C
Upper critical threshold: 33.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the BCM2 web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Note: For a state sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
#       show defaultThresholds <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show defaultThresholds <sensor type> details
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors
all	All of the above numeric sensors
	Tip: You can also type the command without adding this option "all" to get the same data.

Displayed information:

- Without the parameter "details," only the default upper and lower thresholds, deassertion hysteresis and assertion timeout settings of the specified sensor type are displayed.
- With the parameter "details," the threshold range is displayed in addition to default thresholds settings.

Security Settings

This command shows the security settings of the BCM2.

```
#       show security
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show security details
```

Displayed information:

- Without the parameter "details," the information including IP access control, role-based access control, password policy, and HTTPS encryption is displayed.
- With the parameter "details," more security information is displayed, such as user blocking time, user idle timeout and front panel permissions (if supported by your model).

Existing User Profiles

This command shows the data of one or all existing user profiles.

```
#       show user <user_name>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show user <user_name> details
```

Variables:

- <user_name> is the name of the user whose profile you want to query. The variable can be one of the options: *all* or a user's name.

Option	Description
all	This option shows all existing user profiles.
	Tip: You can also type the command without adding this option "all" to get the same data.
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

- Without the parameter "details," only four pieces of user information are displayed: user name, user "Enabled" status, SNMP v3 access privilege, and role(s).
- With the parameter "details," more user information is displayed, such as the telephone number, e-mail address, preferred measurement units and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
#       show roles <role_name>
```

Variables:

- <role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles.
	Tip: You can also type the command without adding this option "all" to get the same data.
a specific role's name	This option shows the data of the specified role only.

Displayed information:

- Role settings are displayed, including the role description and privileges.

Load Shedding Settings

This section applies to outlet-switching capable models only.

This command shows the load shedding settings.

```
#       show loadshedding
```

Displayed information:

- The load shedding state is displayed along with non-critical outlets.

Note: The load shedding mode is associated with critical and non-critical outlets. To specify critical and non-critical outlets through CLI, see **Specifying Non-Critical Outlets** *(on page 320).*

Serial Port Settings

This command shows the baud rate setting of the serial port labeled CONSOLE / MODEM on the BCM2 device.

```
#       show serial
```

EnergyWise Settings

This command shows the BCM2 device's current configuration for Cisco® EnergyWise.

```
#       show energywise
```

Asset Strip Settings

This command shows the asset strip settings, such as the total number of rack units (tag ports), asset strip state, numbering mode, orientation, available tags and LED color settings.

```
#       show assetStrip <n>
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays all asset strip information.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific asset strip number	Displays the settings of the asset strip connected to the specified FEATURE port number.
	For the BCM2 device with only one FEATURE port, the valid number is always 1.

Rack Unit Settings of an Asset Strip

A rack unit refers to a tag port on the asset strips. This command shows the settings of a specific rack unit or all rack units on an asset strip, such as a rack unit's LED color and LED mode.

```
#       show rackUnit <n> <rack_unit>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is one of the options: *all* or a specific rack unit's index number.

Option	Description
all	Displays the settings of all rack units on the specified asset strip.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific number	Displays the settings of the specified rack unit on the specified asset strip.
	Use the index number to specify the rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.

Blade Extension Strip Settings

This command shows the information of a blade extension strip, including the total number of tag ports, and if available, the ID (barcode) number of any connected tag.

```
#        show bladeSlot <n> <rack_unit> <slot>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit (tag port) on the selected asset strip. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <slot> is one of the options: *all* or a specific number of a tag port on the blade extension strip.

Option	Description
all	Displays the information of all tag ports on the specified blade extension strip connected to a particular rack unit.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific number	Displays the information of the specified tag port on the blade extension strip connected to a particular rack unit.
	The number of each tag port on the blade extension strip is available on the Asset Strip page.

Event Log

The command used to show the event log begins with `show eventlog`. You can add either the *limit* or *class* parameters or both to show specific events.

▶ **Show the last 30 entries:**

```
#       show eventlog
```

▶ **Show a specific number of last entries in the event log:**

```
#       show eventlog limit <n>
```

▶ **Show a specific type of events only:**

```
#       show eventlog class <event_type>
```

▶ **Show a specific number of last entries associated with a specific type of events only:**

```
#       show eventlog limit <n> class <event_type>
```

Variables:

- `<n>` is one of the options: *all* or a number.

Option	Description
all	Displays all entries in the event log.
An integer number	Displays the specified number of last entries in the event log. The number ranges between 1 to 10,000.

- `<event_type>` is one of the following event types.

Event type	Description
all	All events.
device	Device-related events, such as system starting or firmware upgrade event.
userAdministration	User management events, such as a new user profile or a new role.
userActivity	User activities, such as login or logout.
pdu	Displays PDU-related events, such as entry or exit of the load shedding mode.

Event type	Description
sensor	Internal or external sensor events, such as state changes of any sensors.
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
assetManagement	Raritan asset management events, such as asset tag connections or disconnections.
lhx	Schroff® LHX/SHX heat exchanger events.
modem	Modem-related events.
timerEvent	Scheduled action events.
webcam	Events for webcam management, if available.
cardReader	Events for card reader management, if available.
energywise	Cisco EnergyWise-related events, such as enabling the support of the EnergyWise function.

Wireless LAN Diagnostic Log

This command shows the diagnostic log for the wireless LAN connection.

```
#        show wlanlog
```

Server Reachability Information

This command shows all server reachability information with a list of monitored servers and status.

```
#        show serverReachability
```

Server Reachability Information for a Specific Server

To show the server reachability information for a certain IT device only, use the following command.

```
#       show serverReachability server <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show serverReachability server <n> details
```

Variables:

- <n> is a number representing the sequence of the IT device in the monitored server list.

  You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

```
_____
#  IP address       Enabled  Status
_____
1  192.168.84.126   Yes      Waiting for reliable connection
2  www.raritan.com  Yes      Waiting for reliable connection
```

Displayed information:

- Without the parameter "details," only the specified device's IP address, monitoring enabled/disabled state and current status are displayed.
- With the parameter "details," more settings for the specified device are displayed, such as number of pings and wait time prior to the next ping.

Command History

This command syntax shows the command history for current connection session.

```
#        show history
```

Displayed information:

- A list of commands that were previously entered in the current session is displayed.

History Buffer Length

This command syntax shows the length of the history buffer for storing history commands.

```
#        show history bufferlength
```

Displayed information:

- The current history buffer length is displayed.

Reliability Data

This command shows the reliability data.

```
#        show reliability data
```

Reliability Error Log

This command shows the reliability error log.

```
#        show reliability errorlog <n>
```

Variables:

- <n> is one of the options: *0* (zero) or any other integer number.

Option	Description
0	Displays all entries in the reliability error log.
	Tip: You can also type the command without adding this option "0" to get all data.

Option	Description
A specific integer number	Displays the specified number of last entries in the reliability error log.

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IPv4 access control: Disabled

IPv6 access control: Disabled


Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:    No
Maximum number of failed logins: 3
User block time:                   10 minutes

User idle timeout: 1440 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitly authori
zed by management are unauthorized. All activities are monitored and logged. The
re is no privacy on this system. Unauthorized access and activities or any crimi
nal activity will be reported to appropriate authorities.
```

Example 3 - Basic PDU Information

The diagram shows the output of the *show pdu* command.

```
# show pdu
PDU 'my PX'
Model:             PX3-XXXX
Firmware Version: 2.X.0.5-40956
```

Example 4 - In-Depth PDU Information

More information is displayed when typing the *show pdu details* command. Displayed information varies depending on the model you purchased.

```
# show pdu details
PDU 'my PX'
Model:             PX3-XXXX
Firmware Version:  2.X.0.5-40956
Serial Number:     QGZ3792136
Board Revision:    0x01

Voltage rating:    200-240V
Current rating:    16A
Frequency rating:  50/60Hz
Power rating:      3.2-3.8kVA

Sensor data retrieval:      Enabled
Measurements per log entry: 60

External sensor Z coordinate format: Rack units
Device altitude:                     0 m
```

Clearing Information

You can use the clear commands to remove unnecessary data from the BCM2.

After typing a "clear" command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt. See **Different CLI Modes and Prompts** *(on page 283).*

Clearing Event Log

This command removes all data from the event log.

clear eventlog

    -- OR --

clear eventlog /y

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the event log or n to abort the operation.

If you type y, a message "Event log was cleared successfully" is displayed after all data in the event log is deleted.

Clearing WLAN Log

This command removes all data from the diagnostic log for the wireless LAN (WLAN) connection.

```
#        clear wlanlog
```

-- OR --

```
#        clear wlanlog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the WLAN log or n to abort the operation.

If you type y, a message "WLAN log was cleared successfully" is displayed to indicate all data in the WLAN log has been deleted.

Configuring the BCM2 Device and Network

To configure the BCM2 device or network settings through the CLI, it is highly recommended to log in as the administrator so that you have full permissions.

To configure any settings, enter the configuration mode. Configuration commands are case sensitive so ensure you capitalize them correctly.

Entering Configuration Mode

Configuration commands function in configuration mode only.

▶ **To enter configuration mode:**

1. Ensure you have entered administrator mode and the # prompt is displayed.

   Note: If you enter configuration mode from user mode, you may have limited permissions to make configuration changes. See **Different CLI Modes and Prompts** *(on page 283).*

2. Type config and press Enter.
3. The config:# prompt appears, indicating that you have entered configuration mode.

   `config:# _`
4. Now you can type any configuration command and press Enter to change the settings.

Important: To apply new configuration settings, you must issue the

"apply" command before closing the terminal emulation program. Closing the program does not save any configuration changes. See *Quitting Configuration Mode* (on page 316).

Quitting Configuration Mode

Both of "apply" and "cancel" commands let you quit the configuration mode. The difference is that "apply" saves all changes you made in the configuration mode while "cancel" aborts all changes.

▶ **To quit the configuration mode, use either command:**

```
config:#    apply
    -- OR --
config:#    cancel
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode. See *Different CLI Modes and Prompts* (on page 283).

PDU Configuration Commands

A PDU configuration command begins with *pdu*. You can use the PDU configuration commands to change the settings that apply to the whole BCM2 device.

Changing the PDU Name

This command changes the BCM2 device's name.

```
config:#    pdu name "<name>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Setting the Outlet Power-On Sequence

This section applies to outlet-switching capable models only.

This command sets the outlet power-on sequence when the PDU powers up.

```
config:#   pdu outletSequence <option>
```

Variables:

- <option> is one of the options: *default*, or a comma-separated list of outlet numbers.

Option	Description
default	All outlets are switched ON in the ASCENDING order (from outlet 1 to the final outlet) when the BCM2 device powers up.
A comma-separated list of outlet numbers	All outlets are switched ON in the order you specify using the comma-separated list. The list must include all outlets on the PDU.

Setting the Outlet Power-On Sequence Delay

This section applies to outlet-switching capable models only.

This command sets the delays (in seconds) for outlets when turning on all outlets in sequence.

```
config:#    pdu outletSequenceDelay <outlet1>:<delay1>;<outlet2>:<delay2>;
            <outlet3>:<delay3>;...
```

Separate outlet numbers and their delay settings with a colon. Outlets followed by delays are separated with a semicolon.

Variables:

- <outlet1>, <outlet2>, <outlet3> and the like are individual outlet numbers or a range of outlets using a dash. For example, *3-8* represents outlets 3 to 8.
- <delay1>, <delay2>, <delay3> and the like are the delay time in seconds.

Setting the PDU-Defined Default Outlet State

This section applies to outlet-switching capable models only.

This command determines the initial power condition of all outlets after powering up the PDU.

```
config:#    pdu outletStateOnDeviceStartup <option>
```

Variables:

- <option> is one of the options: *off*, *on* or *lastKnownState*.

Option	Description
off	Switches OFF all outlets when the BCM2 device powers up.
on	Switches ON all outlets when the BCM2 device powers up.
lastKnownState	Restores all outlets to the previous status before powering down the BCM2 device when the PDU powers up again.

Raritan.
A brand of legrand

Setting the PDU-Defined Cycling Power-Off Period

This section applies to outlet-switching capable models only.

This command sets the power-off period of the power cycling operation for all outlets.

```
config:#   pdu cyclingPowerOffPeriod <timing>
```

Variables:

- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600, or *pduDefined* for following the PDU-defined timing.

Setting the Inrush Guard Delay Time

This section applies to outlet-switching capable models only.

This command sets the inrush guard delay.

```
config:#   pdu inrushGuardDelay <timing>
```

Variables:

- <timing> is a delay time between 100 and 100000 milliseconds.

Setting the Outlet Initialization Delay

This section applies to outlet-switching capable models only.

This command determines the outlet initialization delay timing on device startup. See PDU for information on outlet initialization delay.

```
config:#   pdu outletInitializationDelayOnDeviceStartup <timing>
```

Variables:

- <timing> is a delay time between 1 and 3600 seconds.

Specifying Non-Critical Outlets

This section applies to outlet-switching capable models only.

This command determines critical and non-critical outlets. It is associated with the load shedding mode. See Load Shedding Mode.

```
config:#    pdu nonCriticalOutlets <outlets1>:false;<outlets2>:true
```

Separate outlet numbers and their settings with a colon. Separate each "false" and "true" setting with a semicolon.

Variables:

- <outlets1> is one or multiple outlet numbers to be set as critical outlets. Use commas to separate outlet numbers.

  Use a dash for a range of consecutive outlets. For example, *3-8* represents outlets 3 to 8.

- <outlets2> is one or multiple outlet numbers to be set as NON-critical outlets. Use commas to separate outlet numbers.

  Use a dash for a range of consecutive outlets. For example, *3-8* represents outlets 3 to 8.

Enabling or Disabling Data Logging

This command enables or disables the data logging feature.

```
config:#    pdu dataRetrieval <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the data logging feature.
disable	Disables the data logging feature.

For more information, see *Setting Data Logging* (on page 235).

Raritan.
A brand of **legrand**

Setting Data Logging Measurements Per Entry

This command defines the number of measurements accumulated per log entry.

```
config:#   pdu measurementsPerLogEntry <number>
```

Variables:

- <number> is an integer between 1 and 600. The default is 60 samples per log entry.

For more information, see *Setting Data Logging* (on page 235).

Specifying the Device Altitude

This command specifies your BCM2 device's altitude above sea level (in meters). You must specify the BCM2 device's altitude above sea level if a Raritan's DPX differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See *Altitude Correction Factors* (on page 479).

```
config:#   pdu deviceAltitude <altitude>
```

Variables:

- <altitude> is an integer between 1 and 3000 meters.

Setting the Z Coordinate Format for Environmental Sensors

This command enables or disables the use of rack units for specifying the height (Z coordinate) of environmental sensors.

```
config:#   pdu externalSensorsZCoordinateFormat <option>
```

Variables:

- <option> is one of the options: *rackUnits* or *freeForm*.

Option	Description
rackUnits	The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors or actuators.
freeForm	Any alphanumeric string can be used for specifying the Z coordinate.

Note: After determining the format for the Z coordinate, you can set a value for it. See **Setting the Z Coordinate** *(on page 400).*

Enabling or Disabling Peripheral Device Auto Management

This command enables or disables the Peripheral Device Auto Management feature.

```
config:#   pdu peripheralDeviceAutoManagement <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the automatic management feature for environmental sensor packages.
disable	Disables the automatic management feature for environmental sensor packages.

For more information, see How the Automatic Management Function Works.

Examples

This section illustrates several PDU configuration examples.

Example 1 - PDU Naming

The following command assigns the name "my px12" to the PDU.

```
config:#    pdu name "my px12"
```

Example 2 - Outlet Sequence

The following command causes a 10-outlet PDU to first power on the 8th to 6th outlets and then the rest of outlets in the ascending order after the PDU powers up.

```
config:#    pdu outletSequence 8-6,1-5,9,10
```

Example 3 - Outlet Sequence Delay

The following command determines that the outlet 1's delay is 2.5 seconds, outlet 2's delay is 3 seconds, and the delay for outlets 3 through 5 is 10 seconds.

```
config:#    pdu outletSequenceDelay 1:2.5;2:3;3-5:10
```

Example 4 - Non-Critical Outlets

The following command sets outlets 1, 2, 3, 7, and 9 to be critical outlets, and 4, 5, 6, 8, 10, 11 and 12 to be non-critical outlets on a 12-outlet BCM2.

```
config:#    pdu nonCriticalOutlets 1-3,7,9:false;4-6,8,10-12:true
```

Network Configuration Commands

A network configuration command begins with *network*. A number of network settings can be changed through the CLI, such as the IP address, transmission speed, duplex mode, and so on.

Configuring IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

Setting the IPv4 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv4 interface <ETH> configMethod <mode>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv4 configuration mode of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv4 configuration mode of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 configuration mode of the BRIDGE interface (that is, bridging mode).

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

Setting the IPv4 Preferred Host Name

After selecting DHCP as the IPv4 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv4 interface <ETH> preferredHostName <name>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv4 preferred host name of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv4 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 preferred host name of the BRIDGE interface (that is, bridging mode).

- <name> is a host name which:
    - Consists of alphanumeric characters and/or hyphens
    - Cannot begin or end with a hyphen
    - Cannot contain more than 63 characters
    - Cannot contain punctuation marks, spaces, and other symbols

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the BCM2 device.

```
config:#   network ipv4 interface <ETH> address <ip address>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv4 address of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv4 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 address of the BRIDGE interface (that is, the bridging mode).

- <ip address> is the IP address being assigned to your BCM2 device. Its format is "IP address/prefix". For example, *192.168.84.99/32*.

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:#   network ipv4 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting IPv4 Static Routes

If the IPv4 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the BCM2 and devices in the other subnet.

These commands are prefixed with *network ipv4 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see *Static Route Examples* (on page 145).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv4 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv4 staticRoutes modify <route_ID> <dest-2> <hop>
```

-- OR --

```
config:#   network ipv4 staticRoutes modify <route_ID> <dest-2> interface <ETH>
```

Variables:

- <dest-1> is a combination of the IP address and subnet mask of the other subnet. The format is *IP address/subnet mask*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ethernet*, *wireless* and *bridge*. Type "bridge" only when your BCM2 is in the bridging mode.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/subnet mask*. You can modify either the IP address or the subnet mask or both.

Configuring IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

Setting the IPv6 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv6 interface <ETH> configMethod <mode>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv6 configuration mode of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv6 configuration mode of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 configuration mode of the BRIDGE interface (that is, bridging mode).

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

Setting the IPv6 Preferred Host Name

After selecting DHCP as the IPv6 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv6 interface <ETH> preferredHostName <name>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv6 preferred host name of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv6 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 preferred host name of the BRIDGE interface (that is, bridging mode).

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
- Cannot contain punctuation marks, spaces, and other symbols

Setting the IPv6 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the BCM2 device.

```
config:#   network ipv6 interface <ETH> address <ip
           address>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv6 address of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv6 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 address of the BRIDGE interface (that is, the bridging mode).

- <ip address> is the IP address being assigned to your BCM2 device. This value uses the IPv6 address format. Note that you must add */xx*, which indicates a prefix length of bits such as /64, to the end of this IPv6 address.

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:#   network ipv6 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Setting IPv6 Static Routes

If the IPv6 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the BCM2 and devices in the other subnet.

These commands are prefixed with *network ipv6 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see *Static Route Examples* (on page 145).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv6 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv6 staticRoutes modify <route_ID> <dest-2> <hop>
```

-- OR --

```
config:#    network ipv6 staticRoutes modify <route_ID> <dest-2> interface <ETH>
```

Variables:

- <dest-1> is the IP address and prefix length of the subnet where the BCM2 belongs. The format is *IP address/prefix length*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ethernet*, *wireless* and *bridge*. Type "bridge" only when your BCM2 is in the bridging mode.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/prefix length*. You can modify either the IP address or the prefix length or both.

Configuring DNS Parameters

Use the following commands to configure DNS-related settings.

▶ **Specify the primary DNS server:**

```
config:#   network dns firstServer <ip address>
```

▶ **Specify the secondary DNS server:**

```
config:#   network dns secondServer <ip address>
```

▶ **Specify the third DNS server:**

```
config:#   network dns thirdServer <ip address>
```

▶ **Determine which IP address is used when the DNS server returns both IPv4 and IPv6 addresses:**

```
config:#   network dns resolverPreference <resolver>
```

Variables:
- <ip address> is the IP address of the DNS server.
- <resolver> is one of the options: *preferV4* or *preferV6.*

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.
preferV6	Use the IPv6 addresses returned by the DNS server.

Setting LAN Interface Parameters

A LAN interface configuration command begins with *network ethernet*.

Enabling or Disabling the LAN Interface

This command enables or disables the LAN interface.

```
config:#   network ethernet ETHERNET enabled <option>
```

Variables:

- <option> is one of the options: *true or false*.

Option	Description
true	The specified network interface is enabled.
false	The specified network interface is disabled.

Changing the LAN Interface Speed

This command determines the LAN interface speed.

```
config:#   network ethernet ETHERNET speed <option>
```

Variables:

- <option> is one of the options: *auto*, *10Mbps*, and *100Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.

Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

config:# network ethernet ETHERNET duplexMode <mode>

Variables:

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The BCM2 selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the BCM2 device) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Setting Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), authentication method, Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *network wireless*.

Note: If current networking mode is not wireless, the SSID, PSK and BSSID values are not applied until the networking mode is changed to "wireless." In addition, a message appears, indicating that the active network interface is not wireless.

Setting the SSID

This command specifies the SSID string.

config:# network wireless SSID <ssid>

Variables:

- <ssid> is the name of the wireless access point, which consists of:
    - Up to 32 ASCII characters
    - No spaces

- ASCII codes 0x20 ~ 0x7E

Setting the Authentication Method

This command sets the wireless authentication method to either PSK or Extensible Authentication Protocol (EAP).

```
config:#   network wireless authMethod <method>
```

Variables:

- <method> is one of the authentication methods: *PSK* or *EAP*.

Method	Description
PSK	The wireless authentication method is set to PSK.
EAP	The wireless authentication method is set to EAP.

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command.

```
config:#   network wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
    - 8 to 63 characters
    - No spaces
    - ASCII codes 0x20 ~ 0x7E

Setting EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, password, and CA certificate.

▶ **Determine the outer authentication protocol:**

config:#   network wireless eapOuterAuthentication <outer_auth>

▶ **Determine the inner authentication protocol:**

config:#   network wireless eapInnerAuthentication <inner_auth>

▶ **Set the EAP identity:**

config:#   network wireless eapIdentity <identity>

▶ **Set the EAP password:**

config:#   network wireless eapPassword

After performing the above command, the BCM2 prompts you to enter the password. Then type the password and press Enter.

▶ **Provide a CA TLS certificate:**

config:#   network wireless eapCACertificate

After performing the above command, the system prompts you to enter the CA certificate's contents. For details, see *EAP CA Certificate Example* (on page 339).

▶ **Enable or disable verification of the TLS certificate chain:**

config:#   network wireless enableCertVerification <option1>

▶ **Allow expired and not yet valid TLS certificates:**

config:#   network wireless allowOffTimeRangeCerts <option2>

▶ **Allow wireless network connection with incorrect system time:**

```
config:#    network wireless allowConnectionWithIncorrectClock <option3>
```

Variables:

- The value of <outer_auth> is *PEAP* because BCM2 only supports Protected Extensible Authentication Protocol (PEAP) as the outer authentication.
- The value of <inner_auth> is *MSCHAPv2* because BCM2 only supports Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) as the inner authentication.
- <identity> is your user name for the EAP authentication.
- <option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the verification of the TLS certificate chain.
false	Disables the verification of the TLS certificate chain.

- <option2> is one of the options: *true* or *false*.

Option	Description
true	Always make the wireless network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The wireless network connection is NOT successfully established when the TLS certificate chain contains any certificate which is outdated or not valid yet.

- <option3> is one of the options: *true* or *false*.

Option	Description
true	Make the wireless network connection successful when the BCM2 system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.

Option	Description
false	The wireless network connection is NOT successfully established when the BCM2 finds that the TLS certificate is not valid due to incorrect system time.

EAP CA Certificate Example

This section provides a CA certificate example only. Your CA certificate contents should be different from the contents displayed in this example.

▶ **To provide a CA certificate:**

1. Make sure you have entered the configuration mode. See *Entering Configuration Mode* (on page 315).

2. Type the following command and press Enter.

   ```
   config:#   network wireless eapCACertificate
   ```

3. The system prompts you to enter the contents of the CA certificate.

4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbHz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents as illustrated below, excluding the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. Paste the contents in the terminal.

7. Press Enter.

8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.
   ```
   config:#
   ```

Setting the BSSID

This command specifies the BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables:

- <bssid> is either the MAC address of the wireless access point or *none* for automatic selection.

Configuring the Cascading Mode

This command determines the cascading mode.

```
config:#   network <mode> enabled <option1>
```

Variables:

- <mode> is one of the following cascading modes.

Important: When enabling either cascading mode, you must make sure the other cascading mode is disabled, or the preferred

cascading mode may not be enabled successfully.

Mode	Description
bridge	The network bridging mode, where each cascaded device is assigned a unique IP address.
portForwarding	The port forwarding mode, where every cascaded device in the chain shares the same IP address, with diverse port numbers assigned.

- <option1> is one of the following options:

Option	Description
true	The selected cascading mode is enabled.
false	The selected cascading mode is disabled.

▶ **If Port Forwarding mode is enabled, you must configure two more settings to finish the configuration:**

On ALL cascaded devices, you must configure the 'role' setting one by one.

```
config:#   network portForwarding role <option2>
```

On the master device, you must configure the 'downstream interface' setting.

```
config:#   network portForwarding
           masterDownstreamInterface <option3>
```

Variables:

- <option2> is one of the following cascading roles:

Role	Description
master	The device is a master device.
slave	The device is a slave device.

- <option3> is one of the following options:

Option	Description
Ethernet	Ethernet port is the port where the 1st slave device is connected.
Usb	USB port is the port where the 1st slave device is connected.

Setting Network Service Parameters

A network service command begins with *network services*.

Setting the HTTP Port

The commands used to configure the HTTP port settings begin with *network services http*.

▶ **Change the HTTP port:**

```
config:#    network services http port <n>
```

▶ **Enable or disable the HTTP port:**

```
config:#    network services http enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.
- <option> is one of the options: *true* or *false*.

Option	Description
true	The HTTP port is enabled.
false	The HTTP port is disabled.

Setting the HTTPS Port

The commands used to configure the HTTPS port settings begin with *network services https*.

▶ **Change the HTTPS port:**

```
config:#   network services https port <n>
```

▶ **Enable or disable the HTTPS access:**

```
config:#   network services https enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Forces any access to the BCM2 via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

Enabling or Disabling Telnet

This command enables or disables the Telnet service.

```
config:#   network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.

Option	Description
false	The Telnet service is disabled.

Changing the Telnet Port

This command changes the Telnet port.

```
config:#   network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command enables or disables the SSH service.

```
config:#   network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Changing the SSH Port

This command changes the SSH port.

```
config:#   network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Raritan.
A brand of legrand

Determining the SSH Authentication Method

This command syntax determines the SSH authentication method.

```
config:#   network services ssh authentication <auth_method>
```

Variables:

- <option> is one of the options: *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

Option	Description
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

If the public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connection. See *Specifying the SSH Public Key* (on page 387).

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

An SNMP command begins with *network services snmp*.

Enabling or Disabling SNMP v1/v2c

This command enables or disables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v1/v2c protocol is enabled.
disable	The SNMP v1/v2c protocol is disabled.

Enabling or Disabling SNMP v3

This command enables or disables the SNMP v3 protocol.

```
config:#   network services snmp v3 <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v3 protocol is enabled.
disable	The SNMP v3 protocol is disabled.

Setting the SNMP Read Community

This command sets the SNMP read-only community string.

```
config:#   network services snmp readCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the SNMP Write Community

This command sets the SNMP read/write community string.

```
config:#   network services snmp writeCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the sysContact Value

This command sets the SNMP MIB-II sysContact value.

```
config:#   network services snmp sysContact <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysName Value

This command sets the SNMP MIB-II sysName value.

```
config:#   network services snmp sysName <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysLocation Value

This command sets the SNMP MIB-II sysLocation value.

```
config:#   network services snmp sysLocation <value>
```

Variables:

<value> is a string comprising 0 to 255 alphanumeric characters.

Changing the Modbus Configuration

You can enable or disable the Modbus agent, configure its read-only capability, or change its TCP port.

A Modbus command begins with *network services modbus*.

Enabling or Disabling Modbus

This command enables or disables the Modbus protocol.

```
config:#   network services modbus enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Modbus agent is enabled.
false	The Modbus agent is disabled.

Enabling or Disabling the Read-Only Mode

This command enables or disables the read-only mode for the Modbus agent.

```
config:#   network services modbus readonly <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The read-only mode is enabled.
false	The read-only mode is disabled.

Changing the Modbus Port

This command changes the Modbus port.

```
config:#   network services modbus port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Modbus port is 502.

Enabling or Disabling Service Advertising

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See *Enabling Service Advertising* (on page 164) for details.

```
config:#   network services zeroconfig enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The zero configuration protocol is enabled.
false	The zero configuration protocol is disabled.

Raritan.
A brand of legrand

Examples

This section illustrates several network configuration examples.

Example 1 - Networking Mode

The following command enables the wired networking mode.

```
config:#   network mode wired
```

Example 2 - Enabling Both IP Protocols

The following command determines that both IPv4 and IPv6 protocols are enabled.

```
config:#   network ip proto both
```

Example 3 - Wireless Authentication Method

The following command sets the wireless authentication method to PSK.

```
config:#   network wireless authMethod PSK
```

Example 4 - Static IPv4 Configuration

The following command enables the Static IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode static
```

Time Configuration Commands

A time configuration command begins with *time*.

Determining the Time Setup Method

This command determines the method to configure the system date and time.

```
config:#   time method <method>
```

Variables:

- <method> is one of the time setup options: *manual* or *ntp*.

Mode	Description
manual	The date and time settings are customized.
ntp	The date and time settings synchronize with a specified NTP server.

Setting NTP Parameters

A time configuration command that is used to set the NTP parameters begins with *time ntp*.

Specifying the Primary NTP Server

This command specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#   time ntp firstServer <first_server>
```

Variables:

- The <first_server> is the IP address or host name of the primary NTP server.

Specifying the Secondary NTP Server

This command specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#   time ntp secondServer <second_server>
```

Variables:

- The <second_server> is the IP address or host name of the secondary NTP server.

Overriding DHCP-Assigned NTP Servers

This command determines whether the customized NTP server settings override the DHCP-specified NTP servers.

```
config:#   time ntp overrideDHCPProvidedServer <option>
```

Variables:

- <option> is one of these options: *true* or *false*.

Mode	Description
true	Customized NTP server settings override the DHCP-specified NTP servers.
false	Customized NTP server settings do NOT override the DHCP-specified NTP servers.

Deleting an NTP Server

The following commands delete the primary and/or secondary time server(s).

▶ **To delete the primary time server:**

```
config:#   time ntp firstServer ""
```

▶ **To delete the secondary time server:**

```
config:#   time ntp secondServer ""
```

Setting the Time Zone

The CLI has a list of time zones to configure the date and time for the BCM2.

```
config:#   time zone
```

After a list of time zones is displayed, type the index number of the time zone or press Enter to cancel.

Example

▶ **To set the time zone:**

1. Type the time zone command as shown below and press Enter.

    ```
    config:#    time zone
    ```

2. The system shows a list of time zones. Type the index number of the desired time zone and press Enter.

3. Type `apply` for the selected time zone to take effect.

Customizing the Date and Time

If intending to manually configure the date and time, use the following CLI commands to specify them.

Note: You shall set the time configuration method to "manual" prior to customizing the date and time. See **Determining the Time Setup Method** *(on page 350).*

▶ **Assign the date:**

```
config:#    time set date <yyyy-mm-dd>
```

▶ **Assign the time:**

```
config:#    time set time <hh:mm:ss>
```

Variables:

Variable	Description
<yyyy-mm-dd>	Type the date in the format of yyyy-mm-dd. For example, type *2015-11-30* for November 30, 2015.
<hh:mm:ss>	Type the time in the format of hh:mm:ss in the 24-hour format. For example, type *13:50:20* for 1:50:20 pm.

Setting the Automatic Daylight Savings Time

This command determines whether the daylight savings time is applied to the time settings.

```
config:#   time autoDST <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Mode	Description
enable	Daylight savings time is enabled.
disable	Daylight savings time is disabled.

Examples

This section illustrates several time configuration examples.

Example 1 - Time Setup Method

The following command sets the date and time settings by using the NTP servers.

```
config:#   time method ntp
```

Example 2 - Primary NTP Server

The following command sets the primary time server to 192.168.80.66.

```
config:#   time ntp firstServer 192.168.80.66
```

Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually on your BCM2 and then shows the result. For instructions on specifying NTP servers via CLI, see *Setting NTP Parameters* (on page 350).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See *Setting NTP Parameters* (on page 350).
- Make the customized NTP servers override the DHCP-assigned ones. See *Overriding DHCP-Assigned NTP Servers* (on page 351).

This command is available either in the administrator/user mode or in the configuration mode. See *Different CLI Modes and Prompts* (on page 283).

▶ **In the administrator/user mode:**

```
#          check ntp
```

▶ **In the configuration mode:**

```
config#    check ntp
```

Security Configuration Commands

A security configuration command begins with *security*.

Firewall Control

You can manage firewall control features through the CLI. The firewall control lets you set up rules that permit or disallow access to the BCM2 device from a specific or a range of IP addresses.

- An IPv4 firewall configuration command begins with *security ipAccessControl ipv4*.
- An IPv6 firewall configuration command begins with *security ipAccessControl ipv6*.

Modifying Firewall Control Parameters

There are different commands for modifying firewall control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 firewall control feature:**

```
config:#    security ipAccessControl ipv4 enabled <option>
```

▶ **Determine the default IPv4 firewall control policy for inbound traffic:**

```
config:#    security ipAccessControl ipv4 defaultPolicyIn <policy>
```

▶ **Determine the default IPv4 firewall control policy for outbound traffic:**

```
config:#    security ipAccessControl ipv4 defaultPolicyOut <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 firewall control feature:**

```
config:#    security ipAccessControl ipv6 enabled <option>
```

▶ **Determine the default IPv6 firewall control policy for inbound traffic:**

```
config:#    security ipAccessControl ipv6 defaultPolicyIn <policy>
```

▶ **Determine the default IPv6 firewall control policy for outbound traffic:**

```
config:#    security ipAccessControl ipv6 defaultPolicyOut <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.

355

Option	Description
false	Disables the IP access control feature.

- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

Tip: You can combine both commands to modify all firewall control parameters at a time. See **Multi-Command Syntax** *(on page 429).*

Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands.

- An IPv4 firewall control rule command begins with *security ipAccessControl ipv4 rule*.
- An IPv6 firewall control rule command begins with *security ipAccessControl ipv6 rule*.

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command for adding a rule varies.

- *IPv4 commands*

▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
config:#   security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
config:#   security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy>
           <insert> <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv4 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

- *IPv6 commands*

▶ **Add a new rule to the bottom of the IPv6 rules list:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv6 rule by inserting it above or below a specific rule:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy>
            <insert> <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv6 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Policy	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command varies.

- *IPv4 commands*

▶ **Modify an IPv4 rule's IP address and/or subnet mask:**

```
config:#    security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
            <ip_mask>
```

▶ **Modify an IPv4 rule's policy:**

```
config:#    security ipAccessControl ipv4 rule modify <direction> <rule_number> policy
            <policy>
```

▶ **Modify all contents of an existing IPv4 rule:**

```
config:#    security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
            <ip_mask> policy <policy>
```

- *IPv6 commands*

▶ **Modify an IPv6 rule's IP address and/or prefix length:**

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
            <ip_mask>
```

▶ **Modify an IPv6 rule's policy:**

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> policy
            <policy>
```

▶ **Modify all contents of an IPv6 existing rule:**

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
            <ip_mask> policy <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

▶ **IPv4 commands**

```
config:#    security ipAccessControl ipv4 rule delete <direction> <rule_number>
```

▶ IPv6 commands

```
config:#    security ipAccessControl ipv6 rule delete <direction> <rule_number>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to remove.

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement`,

Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

```
config:#    security restrictedServiceAgreement enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed in the login screen.

Do either of the following, or the login fails:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

  Tip: To select the agreement checkbox using the keyboard, first press Tab to go to the checkbox and then Enter.

- In the CLI, type `y` when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Specifying the Agreement Contents

This command allows you to create or modify contents of the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement bannerContent
```

After performing the above command, do the following:

1. Type the text comprising up to 10,000 ASCII characters when the CLI prompts you to enter the content.
2. To end the content:
   a. Press Enter.
   b. Type `--END--` to indicate the end of the content.
   c. Press Enter again.

If the content is successfully entered, the CLI displays this message "Successfully entered Restricted Service Agreement" followed by the total number of entered characters in parentheses.

Note: The new content of Restricted Service Agreement is saved only after typing the `apply` command. See **Quitting Configuration Mode** *(on page 316).*

Example

The following example illustrates how to specify the content of the Restricted Service Agreement.

1. Type the following command and press Enter to start entering the content.

   ```
   config:#   security restrictedServiceAgreement bannerContent
   ```

2. Type the following content when the CLI prompts you to enter the content.

```
IMPORTANT!! You are accessing a PDU. If you are not the
system administrator, do NOT power off or power cycle
any outlet without the permission of the system
administrator.
```

3. Press Enter.

4. Type the following:

   `--END--`

5. Press Enter again.

6. Verify that the message "Successfully entered Restricted Service Agreement" is displayed, indicating that the content input is successful.

Login Limitation

The login limitation feature controls login-related limitations, such as password aging, simultaneous logins using the same user name, and the idle time permitted before forcing a user to log out.

A login limitation command begins with *security loginLimits*.

You can combine multiple commands to modify various login limitation parameters at a time. See *Multi-Command Syntax* (on page 429).

Single Login Limitation

This command enables or disables the single login feature, which controls whether multiple logins using the same login name simultaneously is permitted.

```
config:#   security loginLimits singleLogin <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the single login feature.
disable	Disables the single login feature.

Password Aging

This command enables or disables the password aging feature, which controls whether the password should be changed at a regular interval:

```
config:#    security loginLimits passwordAging <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the password aging feature.
disable	Disables the password aging feature.

Password Aging Interval

This command determines how often the password should be changed.

```
config:#    security loginLimits passwordAgingInterval <value>
```

Variables:

- <value> is a numeric value in days set for the password aging interval. The interval ranges from 7 to 365 days.

Idle Timeout

This command determines how long a user can remain idle before that user is forced to log out of the BCM2 web interface or CLI.

```
config:#    security loginLimits idleTimeout <value>
```

Variables:

- <value> is a numeric value in minutes set for the idle timeout. The timeout ranges from 1 to 1440 minutes (24 hours).

User Blocking

There are different commands for changing different user blocking parameters. These commands begin with `security userBlocking`.

You can combine multiple commands to modify the user blocking parameters at a time. See *Multi-Command Syntax* (on page 429).

▶ **Determine the maximum number of failed logins before blocking a user:**

```
config:#    security userBlocking maximumNumberOfFailedLogins <value1>
```

▶ **Determine how long a user is blocked:**

```
config:#    security userBlocking blockTime <value2>
```

Variables:

- <value1> is an integer between 3 and 10, or *unlimited*, which sets no limit on the maximum number of failed logins and thus disables the user blocking function.
- <value2> is a numeric value ranging from 1 to 1440 minutes (one day), or *infinite*, which blocks the user all the time until the user is unblocked manually.

Strong Passwords

The strong password commands determine whether a strong password is required for login, and what a strong password should contain at least.

A strong password command begins with `security strongPasswords`.

You can combine multiple strong password commands to modify different parameters at a time. See *Multi-Command Syntax* (on page 429).

Enabling or Disabling Strong Passwords

This command enables or disables the strong password feature.

```
config:#   security strongPasswords enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

Minimum Password Length

This command determines the minimum length of the password.

```
config:#   security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Maximum Password Length

This command determines the maximum length of the password.

```
config:#   security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Lowercase Character Requirement

This command determines whether a strong password includes at least a lowercase character.

```
config:#   security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.

Option	Description
disable	No lowercase character is required.

Uppercase Character Requirement

This command determines whether a strong password includes at least a uppercase character.

```
config:#   security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Numeric Character Requirement

This command determines whether a strong password includes at least a numeric character.

```
config:#   security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.
disable	No numeric character is required.

Special Character Requirement

This command determines whether a strong password includes at least a special character.

```
config:#   security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Maximum Password History

This command determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:#   security strongPasswords passwordHistoryDepth <value>
```

Variables:

- <value> is an integer between 1 and 12.

Role-Based Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

- An IPv4 role-based access control command begins with *security roleBasedAccessControl ipv4*.
- An IPv6 role-based access control command begins with *security roleBasedAccessControl ipv6*.

Modifying Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 role-based access control feature:**

```
config:#   security roleBasedAccessControl ipv4 enabled <option>
```

▶ **Determine the IPv4 role-based access control policy:**

```
config:#    security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 role-based access control feature:**

```
config:#    security roleBasedAccessControl ipv6 enabled <option>
```

▶ **Determine the IPv6 role-based access control policy:**

```
config:#    security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time. See **Multi-Command Syntax** *(on page 429).*

Managing Role-Based Access Control Rules

You can add, delete or modify role-based access control rules.

- An IPv4 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv4 rule*.
- An IPv6 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv6 rule*.

Adding a Role-Based Access Control Rule

Depending on where you want to add a new rule in the list, the command syntax for adding a rule varies.

- *IPv4 commands*

▶ Add a new rule to the bottom of the IPv4 rules list:

```
config:#   security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
           <policy>
```

▶ Add a new IPv4 rule by inserting it above or below a specific rule:

```
config:#   security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
           <policy> <insert>  <rule_number>
```

- *IPv6 commands*

▶ Add a new rule to the bottom of the IPv6 rules list:

```
config:#   security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
           <policy>
```

▶ Add a new IPv6 rule by inserting it above or below a specific rule:

```
config:#   security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
           <policy> <insert>  <rule_number>
```

Variables:

- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is the role for which you want to create an access control rule.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Role-Based Access Control Rule

Depending on what to modify in an existing rule, the command syntax varies.

- *IPv4 commands*

▶ **Modify a rule's IPv4 address range:**

```
config:#   security roleBasedAccessControl ipv4 rule modify <rule_number>
           startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ **Modify an IPv4 rule's role:**

```
config:#   security roleBasedAccessControl ipv4 rule modify <rule_number> role
           <role>
```

▶ **Modify an IPv4 rule's policy:**

```
config:#   security roleBasedAccessControl ipv4 rule modify <rule_number> policy
           <policy>
```

▶ **Modify all contents of an existing IPv4 rule:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy
            <policy>
```

- *IPv6 commands*

▶ **Modify a rule's IPv6 address range:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ **Modify an IPv6 rule's role:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> role
            <role>
```

▶ **Modify an IPv6 rule's policy:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> policy
            <policy>
```

▶ **Modify all contents of an existing IPv6 rule:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy
            <policy>
```

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is one of the existing roles.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role

Policy	Description
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

Deleting a Role-Based Access Control Rule

These commands remove a specific rule from the list.

▶ **IPv4 commands**

```
config:#    security roleBasedAccessControl ipv4 rule delete <rule_number>
```

▶ **IPv6 commands**

```
config:#    security roleBasedAccessControl ipv6 rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Enabling or Disabling Front Panel Outlet Switching

This section applies to outlet-switching capable models only.

The following CLI commands control whether you can turn on or off an outlet by operating the front panel display.

▶ **To enable the front panel outlet control feature:**

```
config:#    security frontPanelPermissions add switchOutlet
```

▶ **To disable the front panel outlet control feature:**

```
config:#    security frontPanelPermissions remove switchOutlet
```

Examples

This section illustrates several security configuration examples.

Example 1 - IPv4 Firewall Control Configuration

The following command sets up two parameters of the IPv4 access control feature.

```
config:#    security ipAccessControl ipv4 enabled true defaultPolicyIn accept
            defaultPolicyOut accept
```

Results:

- The IPv4 access control feature is enabled.
- The default policy for inbound traffic is set to "accept."
- The default policy for outbound traffic is set to "accept."

Example 2 - Adding an IPv4 Firewall Rule

The following command adds a new IPv4 access control rule and specifies its location in the list.

```
config:#    security ipAccessControl ipv4 rule add 192.168.84.123/24 accept
            insertAbove 5
```

Results:

- A new IPv4 firewall control rule is added to accept all packets sent from the IPv4 address 192.168.84.123.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Example 3 - User Blocking

The following command sets up two user blocking parameters.

```
config:#    security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

Example 4 - Adding an IPv4 Role-based Access Control Rule

The following command creates a newIPv4   role-based access control rule and specifies its location in the list.

```
config:#    security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100
            admin deny insertAbove 3
```

Results:

- A new IPv4 role-based access control rule is added, dropping all packets from any IPv4 address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin."
- The newly-added IPv4 rule is inserted above the 3rd rule. That is, the new rule becomes the 3rd rule, and the original 3rd rule becomes the 4th rule.

Outlet Configuration Commands

An outlet configuration command begins with *outlet*. Such a command allows you to configure an individual outlet.

Changing the Outlet Name

This command names an outlet.

```
config:#    outlet <n> name "<name>"
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Changing an Outlet's Default State

This section applies to outlet-switching capable models only.

This command determines the initial power condition of an outlet after the BCM2 powers up.

```
config:#   outlet <n> stateOnDeviceStartup <option>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <option> is one of the options: *off*, *on, lastKnownState* and *pduDefined.*

Option	Description
off	Turn off the outlet.
on	Turn on the outlet.
lastKnownState	Restore the outlet to the state prior to last PDU power down.
pduDefined	PDU-defined setting.

Note: Setting the outlet's default state to an option other than pduDefined *overrides the PDU-defined default state on that outlet. See* **Setting the PDU-Defined Default Outlet State** *(on page 318).*

Setting an Outlet's Cycling Power-Off Period

This section applies to outlet-switching capable models only.

This command determines the power-off period of the power cycling operation for a specific outlet.

```
config:#   outlet <n> cyclingPowerOffPeriod <timing>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600, or *pduDefined* for following the PDU-defined timing.

Note: This setting overrides the PDU-defined cycling power-off period on a particular outlet. See **Setting the PDU-Defined Cycling Power-Off Period** *(on page 319).*

Example - Outlet Naming

The following command assigns the name "Win XP" to outlet 8.

```
config:#   outlet 8 name "Win XP"
```

Inlet Configuration Commands

An inlet configuration command begins with *inlet*. You can configure an inlet by using the inlet configuration command.

Raritan.
A brand of ◻ legrand

Changing the Inlet Name

This command syntax names an inlet.

```
config:#    inlet <n> name "<name>"
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1. The value is an integer between 1 and 50.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Enabling or Disabling an Inlet (for Multi-Inlet PDUs)

Enabling or disabling an inlet takes effect on a multi-inlet PDU only.

This command enables or disables an inlet.

```
config:#    inlet <n> enabled <option>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1. The value is an integer between 1 and 50.
- <option> is one of the options: *true* or *false*.

Option	Description
true	The specified inlet is enabled.
false	The specified inlet is disabled.

Note: If performing this command causes all inlets to be disabled, a warning message appears, prompting you to confirm. When this occurs, press y to confirm or n to cancel the operation.

Example - Inlet Naming

The following command assigns the name "AC source" to the inlet 1. If your BCM2 device contains multiple inlets, this command names the 1st inlet.

```
config:#   inlet 1 name "AC source"
```

Overcurrent Protector Configuration Commands

An overcurrent protector configuration command begins with *ocp.* The command configures an individual circuit breaker or fuse which protects outlets.

Changing the Overcurrent Protector Name

This command names a circuit breaker or a fuse which protects outlets on your BCM2.

```
config:#   ocp <n> name "<name>"
```

Variables:

- <n> is the number of the overcurrent protector that you want to configure. The value is an integer between 1 and 50.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example - OCP Naming

The command assigns the name "Email servers CB" to the overcurrent protector labeled 2.

```
config:#   ocp 2 name "Email servers CB"
```

User Configuration Commands

Most user configuration commands begin with *user* except for the password change command.

Creating a User Profile

This command creates a new user profile.

```
config:#   user create <name> <option> <roles>
```

After performing the user creation command, the BCM2 prompts you to assign a password to the newly-created user. Then:

1. Type the password and press Enter.

2. Re-type the same password for confirmation and press Enter.

Variables:

*   <name> is a string comprising up to 32 ASCII printable characters. The <name> variable CANNOT contain spaces.

*   <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the newly-created user profile.
disable	Disables the newly-created user profile.

*   <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Modifying a User Profile

A user profile contains various parameters that you can modify.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** *(on page 429).*

Changing a User's Password

This command allows you to change an existing user's password if you have the Administrator Privileges.

```
config:#   user modify <name> password
```

After performing the above command, BCM2 prompts you to enter a new password. Then:

1. Type a new password and press Enter.

2. Re-type the new password for confirmation and press Enter.

Variables:

- <name> is the name of the user whose settings you want to change.

Example

The following procedure illustrates how to change the password of the user "May."

1. Verify that you have entered the configuration mode. See *Entering Configuration Mode* (on page 315).

2. Type the following command to change the password for the user profile "May."

```
config:#   user modify May password
```

3. Type a new password when prompted, and press Enter.

4. Type the same new password and press Enter.

5. If the password change is completed successfully, the config:# prompt appears.

Modifying a User's Personal Data

You can change a user's personal data, including the user's full name, telephone number, and email address.

Various commands can be combined to modify the parameters of a specific user profile at a time. See *Multi-Command Syntax* (on page 429).

▶ **Change a user's full name:**

```
config:#   user modify <name> fullName "<full_name>"
```

▶ **Change a user's telephone number:**

```
config:#   user modify <name> telephoneNumber "<phone_number>"
```

▶ **Change a user's email address:**

```
config:#   user modify <name> eMailAddress <email_address>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <full_name> is a string comprising up to 32 ASCII printable characters. The <full_name> variable must be enclosed in quotes when it contains spaces.
- <phone_number> is the phone number that can reach the specified user. The <phone_number> variable must be enclosed in quotes when it contains spaces.
- <email_address> is the email address of the specified user.

Enabling or Disabling a User Profile

This command enables or disables a user profile. A user can log in to the BCM2 device only after that user's user profile is enabled.

```
config:#   user modify <name> enabled <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the specified user profile.
false	Disables the specified user profile.

Forcing a Password Change

This command determines whether the password change is forced when a user logs in to the specified user profile next time.

```
config:#   user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	A password change is forced on the user's next login.
false	No password change is forced on the user's next login.

Modifying SNMPv3 Settings

There are different commands to modify the SNMPv3 parameters of a specific user profile. You can combine all of the following commands to modify the SNMPv3 parameters at a time. See *Multi-Command Syntax* (on page 429).

▶ **Enable or disable the SNMP v3 access to BCM2 for the specified user:**

```
config:#   user modify <name> snmpV3Access <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the SNMP v3 access permission for the specified user.
disable	Disables the SNMP v3 access permission for the specified user.

▶ **Determine the security level:**

```
config:#   user modify <name> securityLevel <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

▶ **Determine whether the authentication passphrase is identical to the password:**

```
config:#    user modify <name> userPasswordAsAuthenticationPassphrase <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

▶ **Determine the authentication passphrase:**

```
config:#    user modify <name> authenticationPassPhrase <authentication_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <authentication_passphrase> is a string used as an authentication passphrase, comprising 8 to 32 ASCII printable characters.

▶ **Determine whether the privacy passphrase is identical to the authentication passphrase:**

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase
            <option4>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option4> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.
false	Privacy passphrase is different from the authentication passphrase.

► **Determine the privacy passphrase:**

```
config:#   user modify <name> privacyPassPhrase <privacy_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <privacy_passphrase> is a string used as a privacy passphrase, comprising 8 to 32 ASCII printable characters.

► **Determine the authentication protocol:**

```
config:#   user modify <name> authenticationProtocol <option5>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option5> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

► **Determine the privacy protocol:**

```
config:#   user modify <name> privacyProtocol <option6>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.

Changing the Role(s)

This command changes the role(s) of a specific user.

```
config:#   user modify <name> roles <roles>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <roles> is a role or a list of comma-separated roles assigned to the specified user profile. See *All Privileges* (on page 392).

Changing Measurement Units

You can change the measurement units displayed for temperatures, length, and pressure for a specific user profile. Different measurement unit commands can be combined so that you can set all measurement units at a time. To combine all commands, see *Multi-Command Syntax* (on page 429).

Note: The measurement unit change only applies to the web interface and command line interface.

Tip: To set the default measurement units applied to the BCM2 user interfaces for all users via CLI, see **Setting Default Measurement Units** *(on page 389).*

▶ **Set the preferred temperature unit:**

```
config:#   user modify <name> preferredTemperatureUnit <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

► **Set the preferred length unit:**

```
config:#   user modify <name> preferredLengthUnit <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

► **Set the preferred pressure unit:**

```
config:#   user modify <name> preferredPressureUnit <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Specifying the SSH Public Key

If the SSH key-based authentication is enabled, specify the SSH public key for each user profile using the following procedure.

► **To specify or change the SSH public key for a specific user:**

1. Type the SSH public key command as shown below and press Enter.

```
config:#   user modify <name> sshPublicKey
```

2. The system prompts you to enter the contents of the SSH public key. Do the following to input the contents:

   a. Open your SSH public key with a text editor.

   b. Copy all contents in the text editor.

   c. Paste the contents into the terminal.

     d.   Press Enter.

▶ **To remove an existing SSH public key:**

1. Type the same command as shown above.
2. When the system prompts you to input the contents, press Enter without typing or pasting anything.

Example

The following procedure illustrates how to change the SSH public key for the user "assistant."

1. Verify that you have entered the configuration mode. See *Entering Configuration Mode* (on page 315).
2. Type the following command and press Enter.

```
config:#   user modify assistant sshPublicKey
```

3. You are prompted to enter a new SSH public key.
4. Type the new key and press Enter.

Deleting a User Profile

This command deletes an existing user profile.

```
config:#   user delete <name>
```

Changing Your Own Password

Every user can change their own password via this command if they have the Change Own Password privilege. Note that this command does not begin with *user*.

```
config:#   password
```

After performing this command, the BCM2 prompts you to enter both current and new passwords respectively.

Important: After the password is changed successfully, the new password is effective immediately no matter you type the command "apply" or not to save the changes.

Example

This procedure changes your own password:

1. Verify that you have entered the configuration mode. See *Entering Configuration Mode* (on page 315).
2. Type the following command and press Enter.

```
config:#    password
```

3. Type the existing password and press Enter when the following prompt appears.

```
Current password:
```

4. Type the new password and press Enter when the following prompt appears.

```
Enter new password:
```

5. Re-type the new password for confirmation and press Enter when the following prompt appears.

```
Re-type new password:
```

Setting Default Measurement Units

Default measurement units, including temperature, length, and pressure units, apply to the BCM2 user interfaces across all users except for those whose preferred measurement units are set differently by themselves or the administrator. Diverse measurement unit commands can be combined so that you can set all default measurement units at a time. To combine all commands, see *Multi-Command Syntax* (on page 429).

Note: The measurement unit change only applies to the web interface and command line interface.

Tip: To change the preferred measurement units displayed in the BCM2 user interfaces for a specific user via CLI, see **Changing Measurement Units** *(on page 386).*

▶ **Set the default temperature unit:**

```
config:#    user defaultpreferences preferredTemperatureUnit <option1>
```

Variables:

- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

▶ **Set the default length unit:**

```
config:#    user defaultpreferences preferredLengthUnit <option2>
```

Variables:

- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

▶ **Set the default pressure unit:**

```
config:#    user defaultpreferences preferredPressureUnit <option3>
```

Variables:

- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Examples

This section illustrates several user configuration examples.

Example 1 - Creating a User Profile

The following command creates a new user profile and sets two parameters for the new user.

```
config:#   user create May enable admin
```

Results:

- A new user profile "May" is created.
- The new user profile is enabled.
- The **admin** role is assigned to the new user profile.

Example 2 - Modifying a User's Roles

The following command assigns two roles to the user "May."

```
config:#   user modify May roles admin,tester
```

Results:

- The user May has the union of all privileges of "admin" and "tester."

Example 3 - Default Measurement Units

The following command sets all default measurement units at a time.

```
config:#   user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet
           preferredPressureUnit psi
```

Results:

- The default temperature unit is set to Fahrenheit.
- The default length unit is set to feet.
- The default pressure unit is set to psi.

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command creates a new role, with a list of semicolon-separated privileges assigned to the role.

```
config:#    role create <name> <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, that privilege should be followed by a colon and the argument(s).

```
config:#    role create <name> <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See *All Privileges* (on page 392).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

All Privileges

This table lists all privileges. Note that available privileges vary according to the model you purchased. For example, a PDU without the outlet switching function does not have the privilege "switchOutlet."

Privilege	Description
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration

Privilege	Description
changeAuthSettings	Change Authentication Settings
changeDataTimeSettings	Change Date/Time Settings
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeLhxConfiguration	Change LHX/SHX Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
switchOutlet*	Switch Outlet
switchActuator**	Switch Actuator
switchTransferSwitch	Switch Transfer Switch
viewEventSetup	View Event Settings
viewEverything	Unrestricted View Privileges
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Snapshots and Configuration

* The "switchOutlet" privilege requires an argument that is separated with a colon. The argument could be:

- All outlets, that is,
  ```
  switchOutlet:all
  ```

- An outlet number. For example:
  ```
  switchOutlet:1
  switchOutlet:2
  switchOutlet:3
  ```

- A list of comma-separated outlets. For example:
  ```
  switchOutlet:1,3,5,7,8,9
  ```

** The "switchActuator" privilege requires an argument that is separated with a colon. The argument could be:

- All actuators, that is,
  ```
  switchActuator:all
  ```

- An actuator's ID number. For example:
  ```
  switchActuator:1
  switchActuator:2
  switchActuator:3
  ```

- A list of comma-separated ID numbers of different actuators. For example:
  ```
  switchActuator:1,3,6
  ```

Note: The ID number of each actuator is shown in the BCM2 web interface. It is an integer between 1 and 32.

Modifying a Role

You can modify diverse parameters of an existing role, including its privileges.

▶ **Modify a role's description:**

```
config:#   role modify <name> description "<description>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

▶ **Add more privileges to a specific role:**

```
config:#   role modify <name> addPrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#   role modify <name> addPrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See *All Privileges* (on page 392).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

▶ **Remove specific privileges from a role:**

```
config:#   role modify <name> removePrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#   role modify <name> removePrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See *All Privileges* (on page 392).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

Deleting a Role

This command deletes an existing role.

```
config:#    role delete <name>
```

Example - Creating a Role

The following command creates a new role and assigns privileges to the role.

```
config:#    role create tester firmwareUpdate;viewEventSetup
```

Results:

• A new role "tester" is created.
• Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

Environmental Sensor Configuration Commands

An environmental sensor configuration command begins with *externalsensor*. You can configure the name and location parameters of an individual environmental sensor.

Note: To configure an actuator, see **Actuator Configuration Commands** *(on page 413).*

Changing the Sensor Name

This command names an environmental sensor.

```
config:#   externalsensor <n> name "<name>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Note: To name an actuator, see **Actuator Configuration Commands** *(on page 413).*

Specifying the CC Sensor Type

Raritan's contact closure sensor (DPX-CC2-TR) supports the connection of diverse third-party or Raritan's detectors/switches. You must specify the type of connected detector/switch for proper operation. Use this command when you need to specify the sensor type.

```
config:#   externalsensor <n> sensorSubType <sensor_type>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <sensor_type> is one of these types: *contact*, *smokeDetection*, *waterDetection* or *vibration*.

Type	Description
contact	The connected detector/switch is for detection of door lock or door closed/open status.
smokeDetection	The connected detector/switch is for detection of the smoke presence.
waterDetection	The connected detector/switch is for detection of the water presence.

Type	Description
vibration	The connected detector/switch is for detection of the vibration.

Setting the X Coordinate

This command specifies the X coordinate of an environmental sensor.

```
config:#    externalsensor <n> xlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Y Coordinate

This command specifies the Y coordinate of an environmental sensor.

```
config:#    externalsensor <n> ylabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Z Coordinate

This command specifies the Z coordinate of an environmental sensor.

```
config:#   externalsensor <n> zlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- Depending on the Z coordinate format you set, there are two types of values for the <coordinate> variable:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Note: To specify the Z coordinate using the rack units, see **Setting the Z Coordinate Format for Environmental Sensors** *(on page 322).*

Changing the Sensor Description

This command provides a description for a specific environmental sensor.

```
config:#   externalsensor <n> description "<description>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Using Default Thresholds

This command determines whether default thresholds, including the deassertion hysteresis and assertion timeout, are applied to a specific environmental sensor.

```
config:#   externalsensor <n> useDefaultThresholds <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Default thresholds are selected as the threshold option for the specified sensor.
false	Sensor-specific thresholds are selected as the threshold option for the specified sensor.

Setting the Alarmed to Normal Delay for DX-PIR

This command determines the value of the Alarmed to Normal Delay setting for a DX-PIR presence detector.

```
config:#   externalsensor <n> alarmedToNormalDelay <time>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <time> is an integer number in seconds, ranging between 0 and 300.

Examples

This section illustrates several environmental sensor configuration examples.

Example 1 - Environmental Sensor Naming

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 name "Cabinet humidity"
```

Example 2 - Sensor Threshold Selection

The following command sets the environmental sensor #1 to use the default thresholds, including the deassertion hysteresis and assertion timeout, as its threshold settings.

```
config:#   externalsensor 1 useDefaultThresholds true
```

Configuring Environmental Sensors' Default Thresholds

You can set the default values of upper and lower thresholds, deassertion hysteresis and assertion timeout on a sensor type basis, including temperature, humidity, air pressure and air flow sensors. The default thresholds automatically apply to all environmental sensors that are newly detected or added.

A default threshold configuration command begins with *defaultThresholds*.

You can configure various default threshold settings for the same sensor type at a time by combining multiple commands. See *Multi-Command Syntax* (on page 429).

▶ **Set the Default Upper Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperCritical <value>
```

▶ **Set the Default Upper Warning Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperWarning <value>
```

▶ **Set the Default Lower Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> lowerCritical <value>
```

▶ **Set the Default Lower Warning Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> lowerWarning <value>
```

▶ **Set the Default Deassertion Hysteresis for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> hysteresis <hy_value>
```

▶ **Set the Default Assertion Timeout for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> assertionTimeout <as_value>
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

- <value> is the value for the specified threshold of the specified sensor type. Note that diverse sensor types use different measurement units.

Sensor types	Measurement units
absoluteHumidity	g/m^3 (that is, g/m³)
relativeHumidity	%
temperature	Degrees Celsius ($°C$) or Fahrenheit ($°F$), depending on your measurement unit settings.
airPressure	Pascal (Pa) or psi, depending on your measurement unit settings.
airFlow	m/s

Sensor types	Measurement units
vibration	g

- <hy_value> is the deassertion hysteresis value applied to the specified sensor type.
- <as_value> is the assertion timeout value applied to the specified sensor type. It ranges from 0 to 100 (samples).

Example - Default Upper Thresholds for Temperature

It is assumed that your preferred measurement unit for temperature is set to degrees Celsius. Then the following command sets the default Upper Warning threshold to 20 $^{\circ}C$ and Upper Critical threshold to 24 $^{\circ}C$ for all temperature sensors.

```
config:#   defaultThresholds temperature upperWarning 20
           upperCritical 24
```

Sensor Threshold Configuration Commands

A sensor configuration command begins with *sensor*. You can use the commands to configure the threshold, hysteresis and assertion timeout values for any sensor associated with the following items:

- Inlets
- Inlet poles (for three-phase PDUs only)
- Overcurrent protectors
- Environmental sensors

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold has been enabled.

Commands for Inlet Sensors

A sensor configuration command for inlets begins with *sensor inlet*.

You can configure various inlet sensor threshold settings at a time by combining multiple commands. See *Multi-Command Syntax* (on page 429).

▶ **Set the Upper Critical threshold for an inlet sensor:**

```
config:#    sensor inlet <n> <sensor type> upperCritical <option>
```

▶ Set the Upper Warning threshold for an inlet sensor:

```
config:#    sensor inlet <n> <sensor type> upperWarning <option>
```

▶ Set the Lower Critical threshold for an inlet sensor:

```
config:#    sensor inlet <n> <sensor type> lowerCritical <option>
```

▶ Set the Lower Warning threshold for an inlet sensor:

```
config:#    sensor inlet <n> <sensor type> lowerWarning <option>
```

▶ Set the deassertion hysteresis for an inlet sensor:

```
config:#    sensor inlet <n> <sensor type> hysteresis <hy_value>
```

▶ Set the assertion timeout for an inlet sensor:

```
config:#    sensor inlet <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
peakCurrent	Peak current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Sensor type	Description
unbalancedCurrent	Unbalanced load sensor
lineFrequency	Line frequency sensor
residualCurrent	Residual current sensor
phaseAngle	Inlet phase angle sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific inlet sensor.
disable	Disables the specified threshold for a specific inlet sensor.
A numeric value	Sets a value for the specified threshold of a specific inlet sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified inlet sensor. See *"To De-assert" and Deassertion Hysteresis* (on page 86).
- <as_value> is a numeric value that is assigned to the assertion timeout for the specified inlet sensor. See *"To Assert" and Assertion Timeout* (on page 84).

Commands for Inlet Pole Sensors

A sensor configuration command for inlet poles begins with *sensor inletpole*. This type of command is available on a three-phase PDU only.

You can configure various inlet pole sensor threshold settings at a time by combining multiple commands. See *Multi-Command Syntax* (on page 429).

▶ **Set the Upper Critical Threshold for an Inlet Pole:**

```
config:#   sensor inletpole <n> <p> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning Threshold for an Inlet Pole:**

```
config:#   sensor inletpole <n> <p> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical Threshold for an Inlet Pole:**

```
config:#   sensor inletpole <n> <p> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning Threshold for an Inlet Pole:**

```
config:#   sensor inletpole <n> <p> <sensor type> lowerWarning <option>
```

▶ **Set the Inlet Pole's Deassertion Hysteresis:**

```
config:#   sensor inletpole <n> <p> <sensor type> hysteresis <hy_value>
```

▶ **Set the Inlet Pole's Assertion Timeout:**

```
config:#   sensor inletpole <n> <p> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 – L2
2	**L2**	L2	L2 – L3
3	**L3**	L3	L3 – L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for the specified inlet pole sensor.
disable	Disables the specified threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the specified threshold of the specified inlet pole sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified inlet pole sensor. See *"To De-assert" and Deassertion Hysteresis* (on page 86).
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified inlet pole sensor. See *"To Assert" and Assertion Timeout* (on page 84).

Commands for Overcurrent Protector Sensors

A sensor configuration command for overcurrent protectors begins with *sensor ocp*.

You can configure various overcurrent protector threshold settings at a time by combining multiple commands. See *Multi-Command Syntax* (on page 429).

▶ **Set the Upper Critical threshold for an overcurrent protector:**

```
config:#   sensor ocp <n> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning threshold for an overcurrent protector:**

```
config:#   sensor ocp <n> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical threshold for an overcurrent protector:**

```
config:#    sensor ocp <n> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning threshold for an overcurrent protector:**

```
config:#    sensor ocp <n> <sensor type> lowerWarning <option>
```

▶ **Set the deassertion hysteresis for an overcurrent protector:**

```
config:#    sensor ocp <n> <sensor type> hysteresis <hy_value>
```

▶ **Set the assertion timeout for an overcurrent protector:**

```
config:#    sensor ocp <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the number of the overcurrent protector that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for the overcurrent protector sensor.
disable	Disables the specified threshold for the overcurrent protector sensor.
A numeric value	Sets a value for the specified threshold of the overcurrent protector sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified overcurrent protector sensor. See *"To De-assert" and Deassertion Hysteresis* (on page 86).
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified overcurrent protector sensor. See *"To Assert" and Assertion Timeout* (on page 84).

Commands for Environmental Sensors

A sensor threshold configuration command for environmental sensors begins with *sensor externalsensor*.

You can configure various environmental sensor threshold settings at a time by combining multiple commands. See *Multi-Command Syntax* (on page 429).

▶ **Set the Upper Critical threshold for an environmental sensor:**

```
config:#   sensor externalsensor <n> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning threshold for an environmental sensor:**

```
config:#   sensor externalsensor <n> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical threshold for an environmental sensor:**

```
config:#   sensor externalsensor <n> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning threshold for an environmental sensor:**

```
config:#   sensor externalsensor <n> <sensor type> lowerWarning <option>
```

▶ **Set the deassertion hysteresis for an environmental sensor:**

```
config:#   sensor externalsensor <n> <sensor type> hysteresis <hy_value>
```

▶ **Set the assertion timeout for an environmental sensor:**

```
config:#    sensor externalsensor <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <sensor type> is one of these sensor types: *temperature, absoluteHumidity, relativeHumidity, airPressure, airFlow* or *vibration*.

  Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable, disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific environmental sensor.
disable	Disables the specified threshold for a specific environmental sensor.
A numeric value	Sets a value for the specified threshold of a specific environmental sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See *"To De-assert" and Deassertion Hysteresis* (on page 86).
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified environmental sensor. It ranges between 1 and 100. See *"To Assert" and Assertion Timeout* (on page 84).

Examples

This section illustrates several environmental sensor threshold configuration examples.

Example 1 - Upper Critical Threshold for a Temperature Sensor

The following command sets the Upper Critical threshold of the environmental "temperature" sensor with the ID number 2 to 40 degrees Celsius. It also enables the upper critical threshold if this threshold has not been enabled yet.

```
config:#    sensor externalsensor 2 temperature upperCritical 40
```

Example 2 - Warning Thresholds for Inlet Sensors

The following command sets both the Upper Warning and Lower Warning thresholds for the inlet 1 RMS current.

```
config:#    sensor inlet 1 current upperWarning 20 lowerWarning 12
```

Results:

- The Upper Warning threshold for the inlet 1 RMS current is set to 20A. It also enables the upper warning threshold if this threshold has not been enabled yet.
- The Lower Warning threshold for the inlet 1 RMS current is set to 12A. It also enables the lower warning threshold if this threshold has not been enabled yet.

Example 3 - Upper Thresholds for Overcurrent Protector Sensors

The following command sets both the Upper Critical and Upper Warning thresholds for the 2nd overcurrent protector.

```
config:#    sensor ocp 2 current upperWarning enable upperCritical 16
```

Results:

- The Upper Critical threshold for the 2nd overcurrent protector's RMS current is set to 16A. It also enables the upper critical threshold if this threshold has not been enabled yet.
- The Upper Warning threshold for the 2nd overcurrent protector's RMS current is enabled.

Actuator Configuration Commands

An actuator configuration command begins with *actuator*. You can configure the name and location parameters of an individual actuator.

You can configure various parameters for one actuator at a time. See *Multi-Command Syntax* (on page 429).

▶ **Change the name:**

```
config:#    actuator <n> name "<name>"
```

▶ **Set the X coordinate:**

```
config:#    actuator <n> xlabel "<coordinate>"
```

▶ **Set the Y coordinate:**

```
config:#    actuator <n> ylabel "<coordinate>"
```

▶ **Set the Z coordinate:**

```
config:#    actuator <n> zlabel "<z_label>"
```

▶ **Modify the actuator's description:**

```
config:#    actuator <n> description "<description>"
```

Variables:

- <n> is the ID number assigned to the actuator. The ID number can be found using the BCM2 web interface or CLI. It is an integer starting at 1.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
- There are two types of values for the <z_label> variable, depending on the Z coordinate format you set:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

413

Note: *To specify the Z coordinate using the rack units, see* **Setting the Z Coordinate Format for Environmental Sensors** *(on page 322).*

- <description> is a sentence or paragraph comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Example - Actuator Naming

The following command assigns the name "Door lock" to the actuator whose ID number is 9.

```
config:#   actuator 9 name "Door lock"
```

Server Reachability Configuration Commands

You can use the CLI to add or delete an IT device, such as a server, from the server reachability list, or modify the settings for a monitored IT device. A server reachability configuration command begins with *serverReachability*.

Adding a Monitored Device

This command adds a new IT device to the server reachability list.

```
config:#   serverReachability add <IP_host> <enable> <succ_ping>
           <fail_ping> <succ_wait> <fail_wait> <resume> <disable_count>
```

Variables:

- <IP_host> is the IP address or host name of the IT device that you want to add.
- <enable> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the newly added device.
false	Disables the ping monitoring feature for the newly added device.

- <succ_ping> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_ping> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the BCM2 resumes pinging after declaring the monitored device "Unreachable." Valid range is 5 to 120 (seconds).
- <disable_count> is the number of consecutive "Unreachable" declarations before the BCM2 disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

Deleting a Monitored Device

This command removes a monitored IT device from the server reachability list.

```
config:#   serverReachability delete <n>
```

Variables:

- <n> is a number representing the sequence of the IT device in the monitored server list.

  You can find each IT device's sequence number using the CLI command of show serverReachability as illustrated below.

```
   _____
   #  IP address       Enabled  Status
   --------------------------------------------------------------
   1  192.168.84.126    Yes      Waiting for reliable connection
   2  www.raritan.com   Yes      Waiting for reliable connection
```

Modifying a Monitored Device's Settings

The command to modify a monitored IT device's settings begins with *serverReachability modify*.

You can modify various settings for a monitored device at a time. See *Multi-Command Syntax* (on page 429).

▶ **Modify a device's IP address or host name:**

```
config:#    serverReachability modify <n> ipAddress <IP_host>
```

▶ **Enable or disable the ping monitoring feature for the device:**

```
config:#    serverReachability modify <n> pingMonitoringEnabled <option>
```

▶ **Modify the number of successful pings for declaring "Reachable":**

```
config:#    serverReachability modify <n> numberOfSuccessfulPingsToEnable
            <succ_number>
```

▶ **Modify the number of unsuccessful pings for declaring "Unreachable":**

```
config:#    serverReachability modify <n> numberOfUnsuccessfulPingsForFailure
            <fail_number>
```

▶ **Modify the wait time after a successful ping:**

```
config:#    serverReachability modify <n> waitTimeAfterSuccessfulPing
            <succ_wait>
```

▶ **Modify the wait time after a unsuccessful ping:**

```
config:#    serverReachability modify <n> waitTimeAfterUnsuccessfulPing
            <fail_wait>
```

▶ **Modify the wait time before resuming pinging after declaring "Unreachable":**

```
config:#    serverReachability modify <n> waitTimeBeforeResumingPinging
            <resume>
```

▶ **Modify the number of consecutive "Unreachable" declarations before disabling the ping monitoring feature:**

```
config:#    serverReachability modify <n> numberOfFailuresToDisable
            <disable_count>
```

Variables:

- <n> is a number representing the sequence of the IT device in the server monitoring list.
- <IP_host> is the IP address or host name of the IT device whose settings you want to modify.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the monitored device.
false	Disables the ping monitoring feature for the monitored device.

- <succ_number> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_number> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the BCM2 resumes pinging after declaring the monitored device "Unreachable." Valid range is 5 to 120 (seconds).
- <disable_count> is the number of consecutive "Unreachable" declarations before the BCM2 disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

Example - Server Settings Changed

The following command modifies several ping monitoring settings for the second server in the server reachability list.

```
config:#    serverReachability modify 2 numberOfSuccessfulPingsToEnable 10
            numberOfUnsuccessfulPingsForFailure 8
            waitTimeAfterSuccessfulPing 30
```

EnergyWise Configuration Commands

An EnergyWise configuration command begins with *energywise*.

Enabling or Disabling EnergyWise

This command syntax determines whether the Cisco® EnergyWise endpoint implemented on the BCM2 device is enabled.

```
config:#   energywise enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Cisco EnergyWise feature is enabled.
false	The Cisco EnergyWise feature is disabled.

Specifying the EnergyWise Domain

This command syntax specifies to which Cisco® EnergyWise domain the BCM2 device belongs.

```
config:#   energywise domain <name>
```

Variables:

- <name> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Raritan.
A brand of legrand

Specifying the EnergyWise Secret

This command syntax specifies the password (secret) to enter the Cisco®
EnergyWise domain.

```
config:#    energywise secret <password>
```

Variables:

- <password> is a string comprising up to 127 ASCII printable
  characters. Spaces and asterisks are NOT acceptable.

Changing the UDP Port

This command syntax specifies the UDP port for communications in the
Cisco® EnergyWise domain.

```
config:#    energywise port <port>
```

Variables:

- <port> is the UDP port number ranging between 1 and 65535.

Setting the Polling Interval

This command syntax determines the polling interval at which the Cisco®
EnergyWise domain queries the BCM2 device.

```
config:#    energywise polling <timing>
```

Variables:

- <timing> is an integer number in seconds. It ranges between 30 and
  600 seconds.

Example - Setting Up EnergyWise

The following command sets up two Cisco® EnergyWise-related features.

```
config:#   energywise enabled true port 10288
```

Results:

- The EnergyWise feature implemented on the BCM2 is enabled.
- The UDP port is set to 10288.

Asset Management Commands

You can use the CLI commands to change the settings of the connected asset strip (if any) or the settings of LEDs on the asset strip.

Asset Strip Management

An asset strip management configuration command begins with `assetStrip`.

Naming an Asset Strip

This command syntax names or changes the name of an asset strip connected to the BCM2 device.

```
config:#   assetStrip <n> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Specifying the Number of Rack Units

This command syntax specifies the total number of rack units on an asset strip connected to the BCM2 device.

```
config:#    assetStrip <n> numberOfRackUnits <number>
```

Note: A rack unit refers to a tag port on the asset strips.

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <number> is the total number of rack units available on the connected asset strip. This value ranges from 8 to 64.

Specifying the Rack Unit Numbering Mode

This command syntax specifies the numbering mode of rack units on the asset strips connected to the BCM2 device. The numbering mode changes the rack unit numbers.

```
config:#    assetStrip <n> rackUnitNumberingMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <mode> is one of the numbering modes: *topDown* or *bottomUp*.

Mode	Description
topDown	The rack units are numbered in the ascending order from the highest to the lowest rack unit.
bottomUp	The rack units are numbered in the descending order from the highest to the lowest rack unit.

Specifying the Rack Unit Numbering Offset

This command syntax specifies the starting number of rack units on the asset strips connected to the BCM2 device.

```
config:#   assetStrip <n> rackUnitNumberingOffset <number>
```

Variables:

* <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
* <number> is a starting number for numbering rack units on the connected asset strip. This value is an integer number.

Specifying the Asset Strip Orientation

This command syntax specifies the orientation of the asset strips connected to the BCM2 device. Usually you do not need to perform this command unless your asset strips do NOT come with the tilt sensor, causing the BCM2 unable to detect the asset strips' orientation.

```
config:#   assetStrip <n> assetStripOrientation <orientation>
```

Variables:

* <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
* <orientation> is one of the options: *topConnector* or *bottomConnector*.

Orientation	Description
topConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
bottomConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom.

Setting LED Colors for Connected Tags

This command syntax sets the LED color for all rack units on the asset strip #1 to indicate the presence of a connected asset tag.

```
config:#   assetStrip <n> LEDColorForConnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Setting LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the connected asset strip(s) to indicate the absence of a connected asset tag.

```
config:#   assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Rack Unit Configuration

A rack unit refers to a tag port on the asset strips. A rack unit configuration command begins with `rackUnit`.

Naming a Rack Unit

This command syntax assigns or changes the name of the specified rack unit on the specified asset strip.

```
config:#   rackUnit <n> <rack_unit> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Setting the LED Operation Mode

This command syntax determines whether a specific rack unit on the specified asset strip follows the global LED color settings.

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *automatic* or *manual*.

Mode	Description
automatic	This option makes the LED of the specified rack unit follow the global LED color settings. See *Setting LED Colors for Connected Tags* (on page 423) and *Setting LED Colors for Disconnected Tags* (on page 423). This is the default.

Mode	Description
manual	This option enables selection of a different LED color and LED mode for the specified rack unit.
	When this option is selected, see *Setting an LED Color for a Rack Unit* (on page 425) and *Setting an LED Mode for a Rack Unit* (on page 426) to set different LED settings.

Setting an LED Color for a Rack Unit

This command syntax sets the LED color for a specific rack unit on the specified asset strip. You need to set a rack unit's LED color only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Note: A rack unit's LED color setting overrides the global LED color setting on it. See **Setting LED Colors for Connected Tags** *(on page 423) and* **Setting LED Colors for Disconnected Tags** *(on page 423).*

Setting an LED Mode for a Rack Unit

This command syntax sets the LED mode for a specific rack unit on the specified asset strip. You need to set a rack unit's LED mode only when the LED operation mode of this rack unit has been set to "manual."

```
config:#    rackUnit <n> <rack_unit> LEDMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *on*, *off*, *blinkSlow* or *blinkFast*.

Mode	Description
on	This mode has the LED stay lit permanently.
off	This mode has the LED stay off permanently.
blinkSlow	This mode has the LED blink slowly.
blinkFast	This mode has the LED blink quickly.

Examples

This section illustrates several asset management examples.

Example 1 - Asset Strip LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the asset sensor #1 to BLACK (that is, 000000) to indicate the absence of a connected asset tag.

```
config:#    assetStrip 1 LEDColorForDisconnectedTags #000000
```

Note: Black color causes the LEDs to stay off.

Example 2 - Rack Unit Naming

The following command assigns the name "Linux server" to the rack unit whose index number is 25 on the asset sensor#1.

```
config:#   rackUnit 1 25 name "Linux server"
```

Serial Port Configuration Commands

A serial port configuration command begins with *serial*.

Setting the Baud Rates

The following commands set the baud rate (bps) of the serial port labeled CONSOLE / MODEM on the BCM2 device. Change the baud rate before connecting it to the desired device, such as a computer, a Raritan's P2CIM-SER, or a modem, through the serial port, or there are communications errors. If you change the baud rate dynamically after the connection has been made, you must reset the BCM2 or power cycle the connected device for proper communications.

▶ **Determine the CONSOLE baud rate:**

```
config:#   serial consoleBaudRate <baud_rate>
```

Note: The serial port bit-rate change is required when the BCM2 works in conjunction with Raritan's Dominion LX KVM switch. Dominion LX only supports 19200 bps for communications over the serial interface.

▶ **Determine the MODEM baud rate:**

```
config:#   serial modemBaudRate <baud_rate>
```

Variables:

- <baud_rate> is one of the baud rate options: *1200*, *2400*, *4800*, *9600*, *19200*, *38400*, *57600*, *115200*.

Forcing the Device Detection Mode

This command forces the serial port on the BCM2 to enter a specific device detection mode.

```
config:#   serial deviceDetectionType <mode>
```

Variables:

- <mode> is one of the detection modes: *automatic*, *forceConsole*, *forceAnalogModem,* or *forceGsmModem*.

Option	Description
automatic	The BCM2 automatically detects the type of the device connected to the serial port. Select this option unless your BCM2 cannot correctly detect the device type.
forceConsole	The BCM2 attempts to recognize that the connected device is set for the console mode.
forceAnalogModem	The BCM2 attempts to recognize that the connected device is an analog modem.
forceGsmModem	The BCM2 attempts to recognize that the connected device is a GSM modem.

Example

The following command sets the CONSOLE baud rate of the BCM2 device's serial port to 9600 bps.

```
config:#   serial consoleBaudRate 9600
```

Setting the History Buffer Length

This command syntax sets the history buffer length, which determines the amount of history commands that can be retained in the buffer. The default length is 25.

```
config:#   history length <n>
```

Variables:

- <n> is an integer number between 1 and 250.

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command to perform all of them at a time. All combined commands must belong to the same configuration type, such as commands prefixed with *network*, *user modify*, *sensor externalsensor* and so on.

A multi-command syntax looks like this:

```
<configuration type> <setting 1> <value 1> <setting 2>
<value 2> <setting 3> <value 3> ...
```

Example 1 - Combination of IP, Subnet Mask and Gateway Parameters

The following multi-command syntax configures IPv4 address, subnet mask and gateway for the network connectivity simultaneously.

```
config:#   network ipv4 ipAddress 192.168.84.225 subnetMask
           255.255.255.0 gateway 192.168.84.0
```

Results:

- The IP address is set to 192.168.84.225.
- The subnet mask is set to 255.255.255.0.
- The gateway is set to 192.168.84.0.

Example 2 - Combination of Upper Critical and Upper Warning Settings

The following multi-command syntax simultaneously configures Upper Critical and Upper Warning thresholds for the RMS current of the 2nd overcurrent protector.

```
config:#   sensor ocp 2 current upperCritical disable upperWarning 15
```

Results:

- The Upper Critical threshold of the 2nd overcurrent protector's RMS current is disabled.
- The Upper Warning threshold of the 2nd overcurrent protector's RMS current is set to 15A and enabled at the same time.

Example 3 - Combination of SSID and PSK Parameters

This multi-command syntax configures both SSID and PSK parameters simultaneously for the wireless feature.

```
config:#   network wireless SSID myssid PSK encryp_key
```

Results:

- The SSID value is set to myssid.
- The PSK value is set to encryp_key.

Load Shedding Configuration Commands

This section applies to outlet-switching capable models only.

A load shedding configuration command begins with *loadshedding*.

Unlike other CLI configuration commands, the load shedding configuration command is performed in the *administrator mode* rather than the configuration mode. See *Different CLI Modes and Prompts* (on page 283).

Enabling or Disabling Load Shedding

This section applies to outlet-switching capable models only.

This command determines whether to enter or exit from the load shedding mode.

```
#            loadshedding <option>
```

After performing the above command, BCM2 prompts you to confirm the operation. Press y to confirm or n to abort the operation.

To skip the confirmation step, you can add the "/y" parameter to the end of the command so that the operation is executed immediately.

```
#            loadshedding <option> /y
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
start	Enter the load shedding mode.
stop	Quit the load shedding mode.

Example

The following command has the BCM2 enter the load shedding mode.

```
config:#   loadshedding start
```

Power Control Operations

> This section applies to outlet-switching capable models only.

Outlets on the BCM2 device can be turned on or off or power cycled through the CLI.

Besides, you can cancel the power-on process while the BCM2 is powering on ALL outlets.

You must perform this operation in the *administrator mode*. See *Different CLI Modes and Prompts* (on page 283).

Turning On the Outlet(s)

> This section applies to outlet-switching capable models only.

This command turns on one or multiple outlets.

```
#       power outlets <numbers> on
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power outlets <numbers> on /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches ON all outlets.
A specific outlet number	Switches ON the specified outlet.
A comma-separated list of outlets	Switches ON multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Switches ON multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Turning Off the Outlet(s)

This section applies to outlet-switching capable models only.

This command turns off one or multiple outlets.

```
#        power outlets <numbers> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#        power outlets <numbers> off /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches OFF all outlets.
A specific outlet number	Switches OFF the specified outlet.
A comma-separated list of outlets	Switches OFF multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Switches OFF multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Power Cycling the Outlet(s)

This section applies to outlet-switching capable models only.

This command power cycles one or multiple outlets.

```
#       power outlets <numbers> cycle
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power outlets <numbers> cycle /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Power cycles all outlets.
A specific outlet number	Power cycles the specified outlet.
A comma-separated list of outlets	Power cycles multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type outlets 2,4,9,11-13,15.
A range of outlets with an en dash in between	Power cycles multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type outlets 3-8.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Canceling the Power-On Process

> This section applies to outlet-switching capable models only.

After issuing the command to power on ALL outlets, you can use the following command to stop the power-on process.

```
#       power cancelSequence
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power cancelSequence /y
```

Example - Power Cycling Specific Outlets

The following command power cycles these outlets: 2, 6, 7, 8, 10, 13, 14, 15 and 16.

```
#    power outlets 2,6-8,10,13-16 cycle
```

Actuator Control Operations

An actuator, which is connected to a dry contact signal channel of a DX sensor, can control a mechanism or system. You can switch on or off that mechanism or system through the actuator control command in the CLI.

Perform these commands in the administrator or user mode. See *Different CLI Modes and Prompts* (on page 283).

Switching On an Actuator

This command syntax turns on one actuator.

```
#       control actuator <n> on
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       control actuator <n> on /y
```

Variables:

- <n> is an actuator's ID number.

  The ID number is available in the BCM2 web interface or using the show command in the CLI. It is an integer between 1 and 32.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Switching Off an Actuator

This command syntax turns off one actuator.

```
#       control actuator <n> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       control actuator <n> off /y
```

Variables:

- <n> is an actuator's ID number.

  The ID number is available in the BCM2 web interface or using the show command in the CLI. It is an integer between 1 and 32.

Raritan.
A brand of legrand

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Example - Turning On a Specific Actuator

The following command turns on the actuator whose ID number is 8.

```
#     control actuator 8 on
```

Unblocking a User

If any user is blocked from accessing the BCM2, you can unblock them at the local console.

▶ **To unblock a user:**

1. Log in to the CLI interface using any terminal program via a local connection. See *With HyperTerminal* (on page 280).

2. When the Username prompt appears, type unblock and press Enter.

Username: unblock

3. When the "Username to unblock" prompt appears, type the name of the blocked user and press Enter.

Username to unblock:

4. A message appears, indicating that the specified user was unblocked successfully.

Resetting the BCM2

You can reset the BCM2 device to factory defaults or simply restart it using the CLI commands.

Restarting the PDU

This command restarts the BCM2 device. It is not a factory default reset.

▶ **To restart the BCM2 device:**

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the BCM2 device.

       #   `reset unit`

            -- OR --

       #   `reset unit /y`

3. If you entered the command without "`/y`" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the Username prompt appears, indicating the reset is complete.

Note: If you are performing this command over a USB connection, re-connect the USB cable after the reset is completed, or the CLI communications are lost.

Resetting Active Energy Readings

You can reset either one active energy sensor or all active energy sensors at a time to restart the energy accumulation process. Only users with the "Admin" role assigned can reset active energy readings.

▶ **To reset all active energy readings of the BCM2:**

    #   `reset activeEnergy pdu`

         -- OR --

    #   `reset activeEnergy pdu /y`

▶ **To reset one inlet's active energy readings:**

    #   `reset activeEnergy inlet <n>`

         -- OR --

    #   `reset activeEnergy inlet <n> /y`

If you entered the command without "/y", a message appears prompting you to confirm the operation. Type y to confirm the reset or n to abort it.

Variables:

- <n> is the inlet number.

Resetting to Factory Defaults

The following commands restore all settings of the BCM2 device to factory defaults.

▶ **To reset BCM2 settings after login, use either command:**

```
#      reset factorydefaults
```
        -- OR --
```
#      reset factorydefaults /y
```

▶ **To reset BCM2 settings before login:**

```
Username:    factorydefaults
```

See *Using the CLI Command* (on page 450) for details.

Network Troubleshooting

The BCM2 provides 4 diagnostic commands for troubleshooting network problems: *nslookup*, *netstat*, *ping*, and *traceroute*. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

Entering Diagnostic Mode

Diagnostic commands function in the diagnostic mode only.

▶ **To enter the diagnostic mode:**

1. Enter either of the following modes:
   - Administrator mode: The # prompt is displayed.
   - User mode: The > prompt is displayed.
2. Type `diag` and press Enter. The diag# or diag> prompt appears, indicating that you have entered the diagnostic mode.
3. Now you can type any diagnostic commands for troubleshooting.

Quitting Diagnostic Mode

▶ **To quit the diagnostic mode, use this command:**

```
diag>       exit
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode. See *Different CLI Modes and Prompts* (on page 283).

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag>       nslookup <host>
```

Variables:

- <host> is the name or IP address of the host whose DNS information you want to query.

Showing Network Connections

This command syntax displays network connections and/or status of ports.

```
diag>       netstat <option>
```

Variables:

- <option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

Testing the Network Connectivity

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.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds ranging from 1 to 600.

The command looks like the following when it includes all options:

```
diag>    ping <host> count <number1> size <number2> timeout <number3>
```

Tracing the Route

This command syntax traces the network route between your BCM2 device and a network host.

```
diag>        traceroute <host>
```

Variables:

- <host> is the name or IP address of the host you want to trace.

Example - Ping Command

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag>        ping 192.168.84.222 count 5
```

Retrieving Previous Commands

If you would like to retrieve any command that was previously typed in the same connection session, press the Up arrow (↑) on the keyboard until the desired command is displayed.

Automatically Completing a Command

A CLI command always consists of several words. You can easily enter a command by typing first word(s) or letter(s) and then pressing Tab or Ctrl+i instead of typing the whole command word by word.

▶ **To have a command completed automatically:**

1. Type initial letters or words of the desired command. Make sure the letters or words you typed are unique so that the CLI can identify the command you want.
2. Press Tab or Ctrl+i until the complete command appears.

Example 1:

Type the first word and the first letter of the second word of the "`reset factorydefaults`" command, that is, `reset f`. Then press Tab or Ctrl+i to complete the second word.

Example 2:

Type the first word and initial letters of the second word of the "`security enforceHttpsForWebAccess`" command, that is, `security enf`. Then press Tab or Ctrl+i to complete the second word.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

▶ **To log out of the CLI:**

1. Ensure you have entered administrator mode and the # prompt is displayed.

2. Type `exit` and press Enter.

Chapter 7   Using SCP Commands

You can perform a Secure Copy (SCP) command to update the BCM2 firmware, do bulk configuration, or back up and restore the configuration.

In This Chapter

Firmware Update via SCP

Same as any BCM2 firmware update, all user management operations are suspended and all login attempts fail during the SCP firmware update. For details, see *Updating the BCM2 Firmware* (on page 254).

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

▶ **To update the firmware via SCP:**

1. Type the following SCP command and press Enter.

   `scp <firmware file> <user name>@<device ip>:/fwupdate`

   - *<firmware file>* is the BCM2 firmware's filename. If the firmware file is not in the current directory, you must include the path in the filename.
   - *<user name>* is the "admin" or any user profile with the Firmware Update permission.
   - *<device ip>* is the IP address of the BCM2 that you want to update.

2. When the system prompts you to enter the password for the specified user profile, type it and press Enter.

3. The system transmits the specified firmware file to the BCM2, and shows the transmission speed and percentage.

4. When the transmission is complete, it shows the following message, indicating that the BCM2 starts to update its firmware now. Wait until the upgrade completes.

   `Starting firmware update. The connection will be closed now.`

▶ **SCP example:**

```
scp  pdu-px2-030000-41270.bin
admin@192.168.87.50:/fwupdate
```

▶ **Windows PSCP command:**

PSCP in Windows works in a similar way to the SCP.

- `pscp <firmware file> <user name>@<device ip>:/fwupdate`

Bulk Configuration via SCP

Like performing bulk configuration via the web interface, there are two steps with the bulk configuration using the SCP commands:

a. Save a configuration from a source BCM2.

b. Copy the configuration file to one or multiple destination BCM2.

For detailed information on the bulk configuration requirements, see *Bulk Configuration* (on page 257).

▶ **To save the configuration via SCP:**

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/bulk_config.xml
```

- *<user name>* is the "admin" or any user profile with the administrator privileges.
- *<device ip>* is the IP address of the BCM2 whose configuration you want to save.

2. Type the user password when prompted.

3. The system saves the configuration from the BCM2 to a file named "bulk_config.xml."

▶ **To copy the configuration via SCP:**

1. Type the following SCP command and press Enter.

```
scp bulk_config.xml <user name>@<device ip>:/bulk_restore
```

- *<user name>* is the "admin" or any user profile with the administrator privileges.
- *<device ip>* is the IP address of the BCM2 whose configuration you want to copy.

2. Type the user password when prompted.

3. The system copies the configuration included in the file "bulk_config.xml" to another BCM2, and displays the following message.

```
Starting restore operation. The connection will be
closed now.
```

▶ **SCP examples:**

- Save operation:

```
scp  admin@192.168.87.50:/bulk_config.xml
```

- Copy operation:

```
scp  bulk_config.xml
admin@192.168.87.47:/bulk_restore
```

▶ **Windows PSCP commands:**

PSCP in Windows works in a similar way to the SCP.

- Save operation:

```
pscp <user name>@<device ip>:/bulk_config.xml
```

- Copy operation:

```
pscp bulk_config.xml <user name>@<device
ip>:/bulk_restore
```

Backup and Restore via SCP

To back up ALL settings of a BCM2, including device-specific settings, you should perform the backup operation instead of the bulk configuration.

You can restore all settings to previous ones after a backup file is available.

▶ **To back up the settings via SCP:**

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/backup_settings.xml
```

- *<user name>* is the "admin" or any user profile with the administrator privileges.
- *<device ip>* is the IP address of the BCM2 whose settings you want to back up.

2. Type the user password when prompted.

3. The system saves the settings from the BCM2 to a file named "backup_settings.xml."

Raritan.
A brand of legrand

▶ **To restore the settings via SCP:**

1. Type the following SCP command and press Enter.

   `scp backup_settings.xml <user name>@<device ip>:/settings_restore`

   - *<user name>* is the "admin" or any user profile with the administrator privileges.
   - *<device ip>* is the IP address of the BCM2 whose settings you want to restore.

2. Type the user password when prompted.
3. The system copies the configuration included in the file "backup_settings.xml" to the BCM2, and displays the following message.

   `Starting restore operation. The connection will be closed now.`

▶ **SCP examples:**

- Backup operation:

  `scp admin@192.168.87.50:/backup_settings.xml`

- Restoration operation:

  `scp backup_settings.xml admin@192.168.87.50:/settings_restore`

▶ **Windows PSCP commands:**

PSCP in Windows works in a similar way to the SCP.

- Backup operation:

  `pscp <user name>@<device ip>:/backup_settings.xml`

- Restoration operation:

  `pscp backup_settings.xml <user name>@<device ip>:/settings_restore`

Downloading Diagnostic Data via SCP

You can download the diagnostic data via SCP.

▶ **To download the diagnostic data via SCP:**

1. Type the following SCP command and press Enter.
   `scp <user name>@<device ip>:/diag-data.tgz`

   - *<user name>* is the "admin" or any user profile with the Administrator or "Unrestricted View Privileges" privileges.

- *<device ip>* is the IP address of the BCM2 whose diagnostic data you want to download.

2. Type the password when the system prompts you to type it.

3. The system saves the diagnostic data from the BCM2 to a file named "diag-data.tgz."

▶ **SCP example:**

```
scp  admin@192.168.87.50:/diag-data.tgz
```

▶ **Windows PSCP command:**

PSCP in Windows works in a similar way to the SCP.

- `pscp <user name>@<device ip>:/diag-data.tgz`

Raritan.
A brand of legrand

Appendix A Resetting to Factory Defaults

You can use either the reset button or the command line interface (CLI) to reset the BCM2.

Important: Exercise caution before resetting the BCM2 to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only active energy data and firmware upgrade history are retained.

▶ **Alternative:**

Another method to reset it to factory defaults is to use the web interface. See *Resetting All Settings to Factory Defaults* (on page 264).

In This Chapter

Using the Reset Button

An RS-232 serial connection to a computer is required for using the reset button.

▶ **To reset to factory defaults using the reset button:**

1. Connect a computer to the BCM2 device via RS-232. See Making an RS-232 or USB Connection.

2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the BCM2. For information on the serial port configuration, see step 2 of *With HyperTerminal* (on page 280).

3. Press (and release) the Reset button of the BCM2 device while pressing the Esc key of the keyboard several times in rapid succession. A prompt (=>) should appear after about one second.

4. Type *defaults* to reset the BCM2 to its factory defaults.

5. Wait until the Username prompt appears, indicating the reset is complete.

Note: HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring the BCM2 to factory defaults. For information on CLI, see *Using the Command Line Interface* (on page 279).

▶ **To reset to factory defaults after logging in to the CLI:**

1. Connect to the BCM2 device. See *Logging in to CLI* (on page 280) or Making an RS-232 or USB Connection.

2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the BCM2. For information on the serial port configuration, see step 2 of *With HyperTerminal* (on page 280).

3. Log in to the CLI by typing the user name "admin" and its password.

4. After the # system prompt appears, type either of the following commands and press Enter.

   ```
   #      reset factorydefaults
   ```
   -- OR --
   ```
   #      reset factorydefaults /y
   ```

5. If you entered the command without "`/y`" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.

6. Wait until the Username prompt appears, indicating the reset is complete.

▶ **To reset to factory defaults without logging in to the CLI:**

The BCM2 provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the BCM2 and launch a terminal emulation program as described in the above procedure.

2. At the Username prompt in the CLI, type "factorydefaults" and press Enter.

   ```
   Username:  factorydefaults
   ```

3. Type `y` on a confirmation message to perform the reset.

Raritan.
A brand of 🔲legrand

Appendix B LDAP Configuration Illustration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP authentication, four main steps are required:

a. Determine user accounts and roles (groups) intended for the BCM2
b. Create user groups for the BCM2 on the AD server
c. Configure LDAP authentication on the BCM2 device
d. Configure roles on the BCM2 device

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

In This Chapter

Step A. Determine User Accounts and Groups

Determine the user accounts and roles (groups) that are authenticated for accessing the BCM2. In this example, we will create two user roles with different permissions. Each role (group) will consist of two user accounts available on the AD server.

User groups	User accounts (members)
BCM_User	usera
	bcmuser2
BCM_Admin	userb
	bcmuser

Group permissions:

*   The BCM_User group will only have read-only permissions.
*   The BCM_Admin group will have full system permissions.

Step B. Configure User Groups on the AD Server

You must create the groups (roles) for the BCM2 on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups for the BCM2 are named *BCM_Admin* and *BCM_User*.
- User accounts *bcmuser*, *bcmuser2*, *usera* and *userb* already exist on the AD server.

▶ **To configure the user groups on the AD server:**

1. On the AD server, create new groups -- *BCM_Admin* and *BCM_User*.

   Note: See the documentation or online help accompanying Microsoft AD for detailed instructions.

2. Add the *bcmuser2* and *usera* accounts to the BCM_User group.
3. Add the *bcmuser* and *userb* accounts to the BCM_Admin group.
4. Verify whether each group comprises correct users.

Step C. Configure LDAP Authentication on the BCM2 Device

You must enable and set up LDAP authentication properly on the BCM2 device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See *Wired Network Settings* (on page 137) and Role of a DNS Server.
- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.
- The AD protocol is NOT encrypted over TLS.
- The AD server uses the default TCP port *389*.
- Anonymous bind is used.

▶ **To configure LDAP authentication:**

1. Choose Device Settings > Security > Authentication.
2. In the LDAP Servers section, click New to add an LDAP/LDAPS server.
3. Provide the BCM2 with the information about the AD server.

Field/setting	Do this...
IP Address / Hostname	Type the domain name `techadssl.com` or IP address `192.168.56.3`.

Field/setting	Do this...
	Important: Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	Leave the checkbox deselected unless the new LDAP server's settings are similar to any existing LDAP settings.
Type of LDAP Server	Select "Microsoft Active Directory."
Security	Select "None" since the TLS encryption is not applied in this example.
Port (None/StartTLS)	Ensure the field is set to 389.
Port (TLS), CA Certificate	Skip the two fields since the TLS encryption is not enabled.
Anonymous Bind	Select this checkbox because anonymous bind is used.
Bind DN, Bind Password, Confirm Bind Password	Skip the three fields because of anonymous bind.
Base DN for Search	Type dc=techadssl,dc=com as the starting point where your search begins on the AD server.
Login Name Attribute	Ensure the field is set to sAMAccountName because the LDAP server is Microsoft Active Directory.
User Entry Object Class	Ensure the field is set to user because the LDAP server is Microsoft Active Directory.
User Search Subfilter	The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
Active Directory Domain	Type techadssl.com.

4. Click Add Server.The LDAP server is saved.
5. In the Authentication Type field, select LDAP.
6. Click Save. The LDAP authentication is activated.

Note: If the BCM2 clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the BCM2 and the LDAP server to use the same NTP server(s).

Step D. Configure Roles on the BCM2

A role on the BCM2 determines the system permissions. You must create the roles whose names are identical to the user groups created for the BCM2 on the AD server or authorization will fail. Therefore, we will create the roles named *BCM_User* and *BCM_Admin* on the BCM2.

In this illustration, we assume:

- Users assigned to the *BCM_User* role can only access the BCM2 and view settings.
- Users assigned to the *BCM_Admin* role can both access and configure the BCM2 because they have the Administrator permissions.

▶ **To create the BCM_User role with appropriate permissions assigned:**

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type `BCM_User` in the Role Name field.
4. Type a description for the BCM_User role in the Description field. For example, "The role can only view BCM settings".
5. Click the Privileges tab to select "Unrestricted View Privileges," which includes all View permissions. The "Unrestricted View Privileges" permission lets users view all settings without the capability to configure or change them.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission "Unrestricted View Privileges" from the Privileges list.
   c. Click Add.
6. Click OK. The BCM_User role is created.
7. Keep the Manage Roles dialog opened to continue creating the BCM_Admin role.

▶ **To create the BCM_Admin role with full permissions assigned:**

1. Click New. The Create New Role dialog appears.
2. Type `BCM_Admin` in the Role Name field.

Raritan.
A brand of ☐legrand

3. Type a description for the BCM_Admin role in the Description field. In this example, we type "The role includes all privileges" to describe the role.

4. Click the Privileges tab to select the Administrator permission. The Administrator permission allows users to configure or change all BCM2 settings.

   a. Click Add. The "Add Privileges to new Role" dialog appears.

   b. Select the permission named Administrator Privileges from the Privileges list.

   c. Click Add.

5. Click OK. The BCM_Admin role is created.

6. Click Close to quit the dialog.

Appendix C   RADIUS Configuration Illustration

This section provides illustrations for configuring RADIUS authentication. One illustration is based on the Microsoft® Network Policy Server (NPS), and the other is based on a FreeRADIUS server.

The following steps are required for any RADIUS authentication:

1. Configure RADIUS authentication on the BCM2. See *Adding Radius Servers* (on page 181).
2. Configure roles on the BCM2. See *Creating Roles* (see "*Creating a Role*" on page 132, on page 128).
3. Configure BCM2 user credentials and roles on your RADIUS server.
    - To configure using standard attributes, see Standard Attributes.
    - To configure using vendor-specific attributes, see Vendor-Specific Attributes.

Note that we assume that the NPS is running on a Windows 2008 system in the NPS illustrations.

In This Chapter

NPS VSA Illustration

To configure Windows 2008 NPS with the *vendor-specific attribute*, you must:

a. Add your BCM2 to NPS. See *Step A: Add Your BCM2 as a RADIUS Client* (on page 457).
b. On the NPS, configure connection request policies and the vendor-specific attribute. See Step B: Configure Connection Policies and Vendor-Specific Attributes.

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See *AD-Related Configuration* (on page 474).

Step A: Add Your BCM2 as a RADIUS Client

The RADIUS implementation on a BCM2 follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

▶ **Presumptions in the illustration:**

- IP address of your BCM2 = `192.168.56.29`
- RADIUS authentication port specified for BCM2: *1812*
- RADIUS accounting port specified for BCM2: *1813*

▶ **To add your BCM2 to the RADIUS NPS:**

1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.
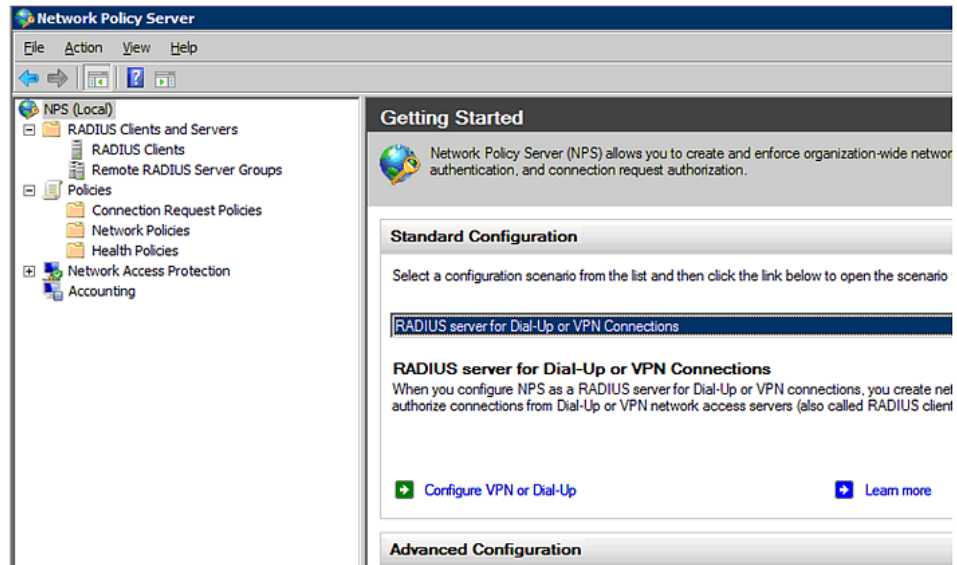
2. Right-click NPS (Local), and select Properties.
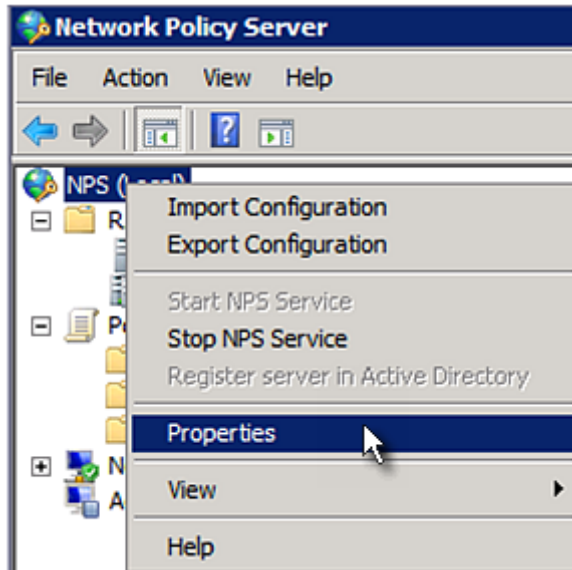
Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your BCM2. In this example, they are 1812 and 1813. Then close this dialog.
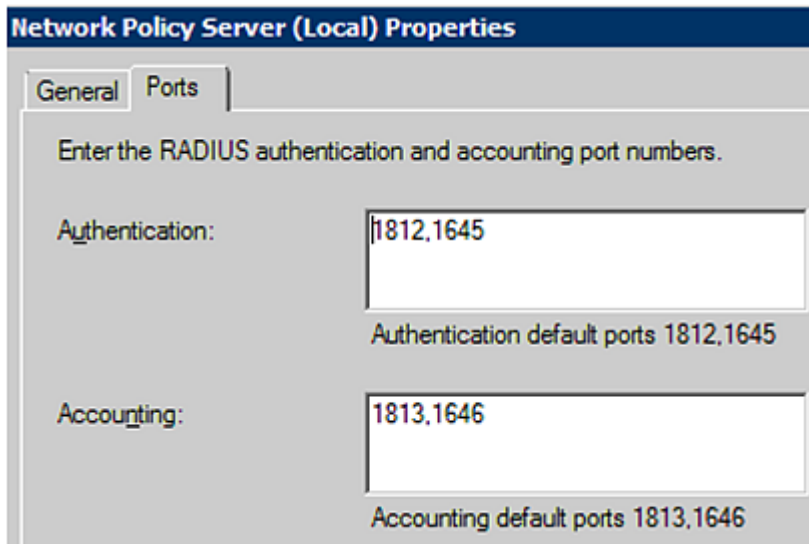
3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.
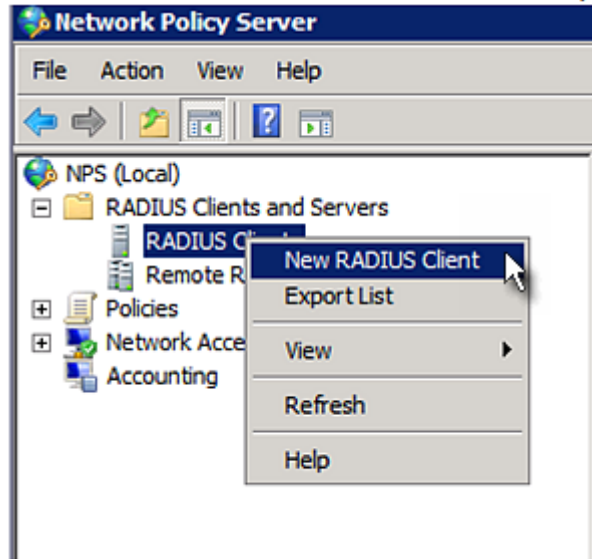
4. Do the following to add your BCM2 to NPS:

    a. Verify the "Enable this RADIUS client" checkbox is selected.

    b. Type a name for identifying your BCM2 in the "Friendly name" field.

    c. Type *192.168.56.29* in the "Address (IP or DNS)" field.

    d. Select *RADIUS Standard* in the "Vendor name" field.

    e. Select the *Manual* radio button.

f. Type the shared secret in the "Shared secret" and "Confirm shared secret" fields. The shared secret must be the same as the one specified on your BCM2.

5. Click OK.

Step B: Configure Connection Policies and Standard Attributes

You need to configure the following for connection request policies:

- IP address or host name of the BCM2
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

▶ **Presumptions in the illustration:**

- IP address of your BCM2 = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your BCM2 = `CHAP`
- Existing role of your BCM2 = `Admin`

▶ **Illustration:**

1. Open the NPS console, and expand the Policies folder.
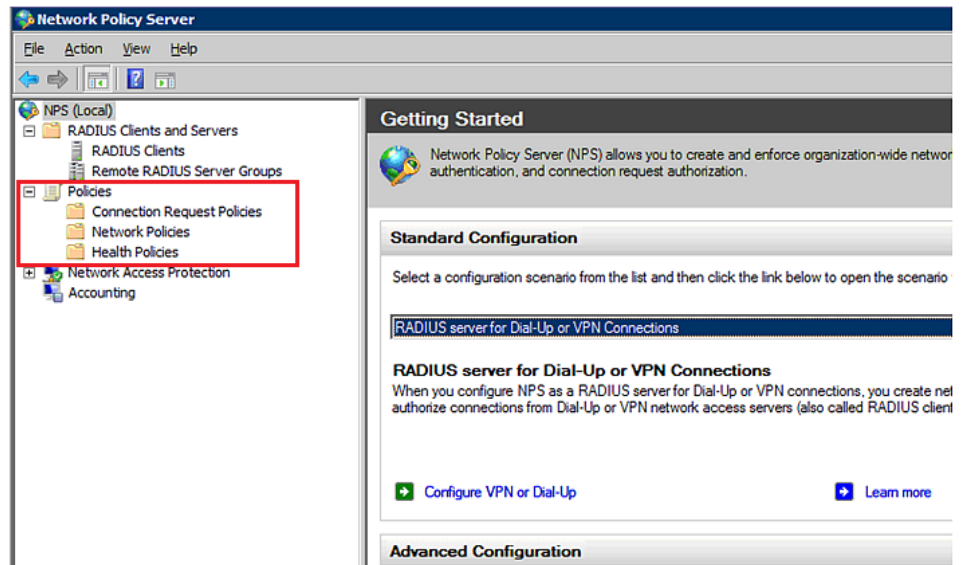
2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.
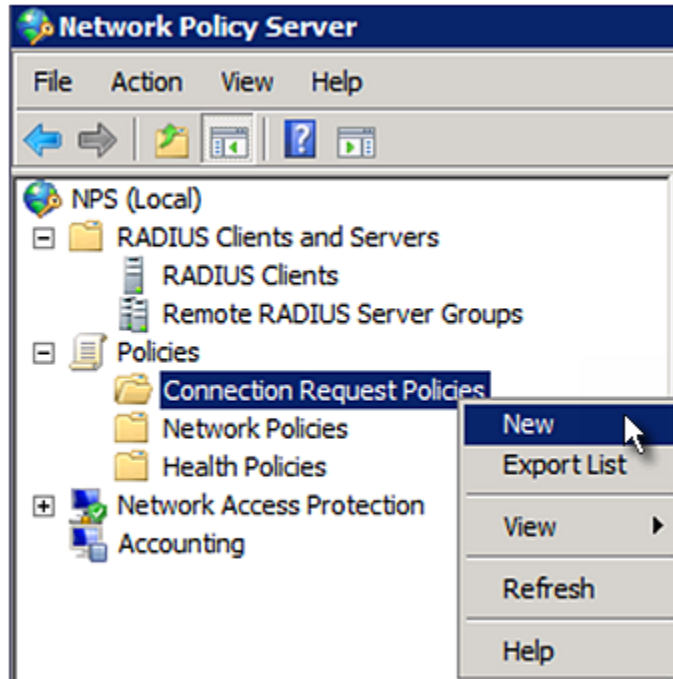
3. Type a descriptive name for identifying this policy in the "Policy name" field.

- You can leave the "Type of network access server" field to the default -- Unspecified.

4. Click Next to show the "Specify Conditions" screen. Click Add.
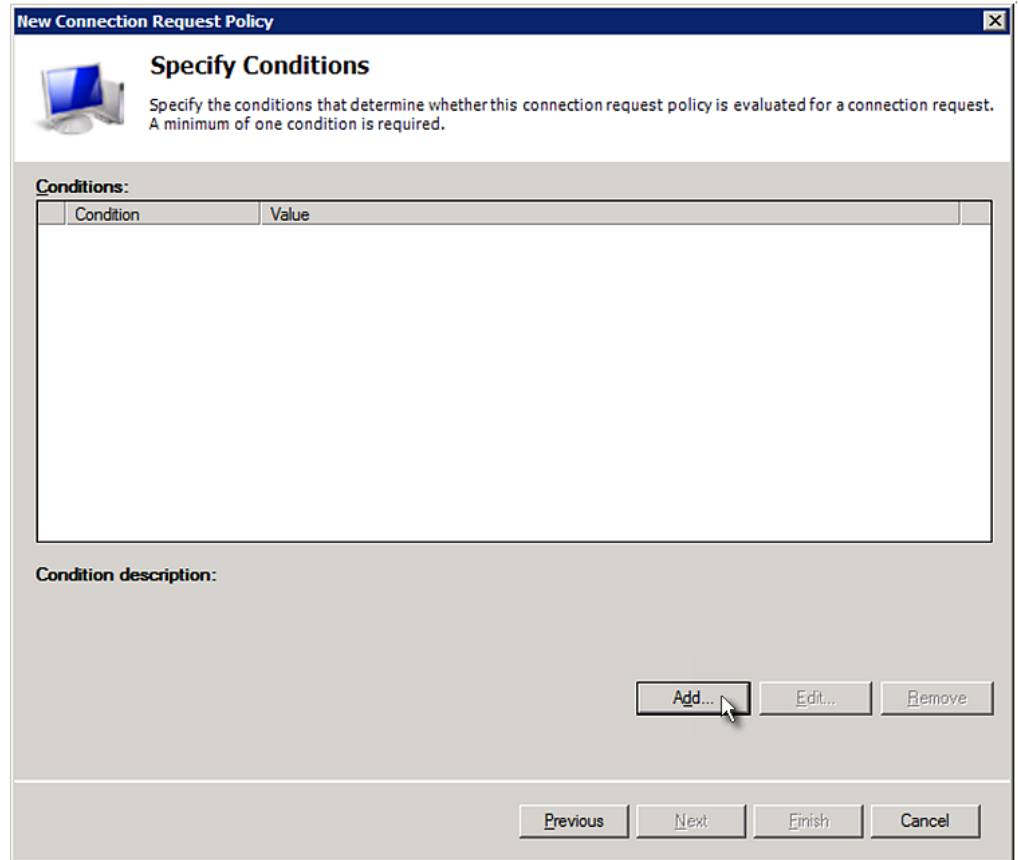
5. The "Select condition" dialog appears. Click Add.
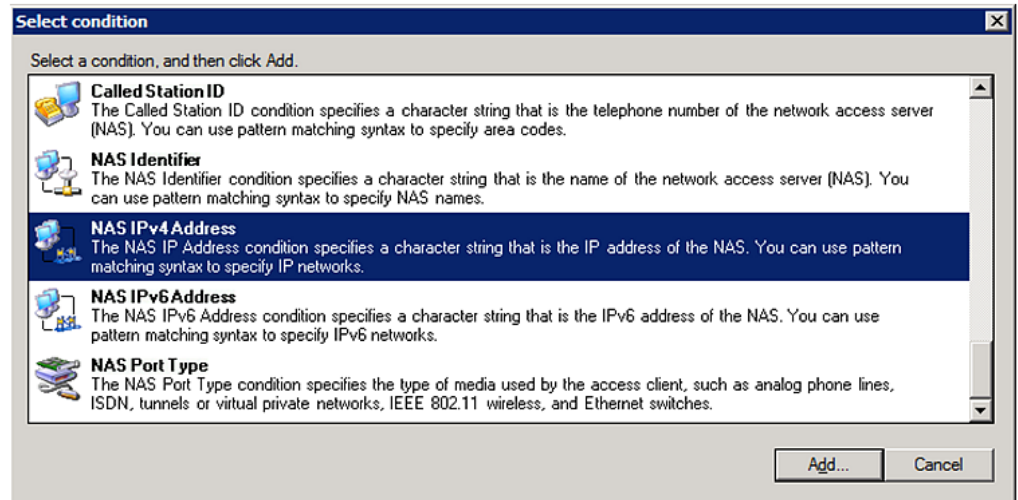
6. The NAS IPv4 Address dialog appears. Type the BCM2 IP address --
    192.168.56.29, and click OK.
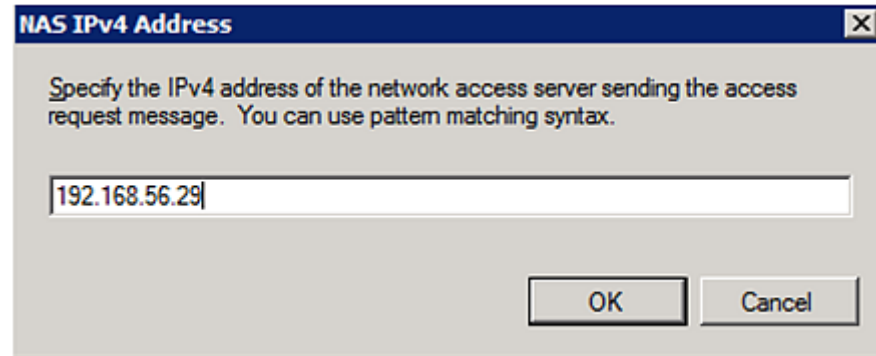
7. Click Next in the New Connection Request Policy dialog.
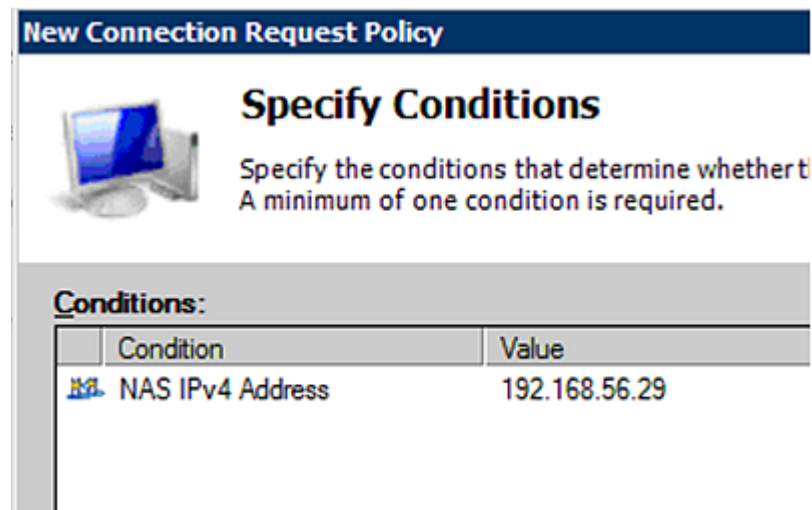
8. Select "Authenticate requests on this server" because a local NPS
    server is used in this example. Then click Next.

465

Note: Connection Request Forwarding options must match your environment.
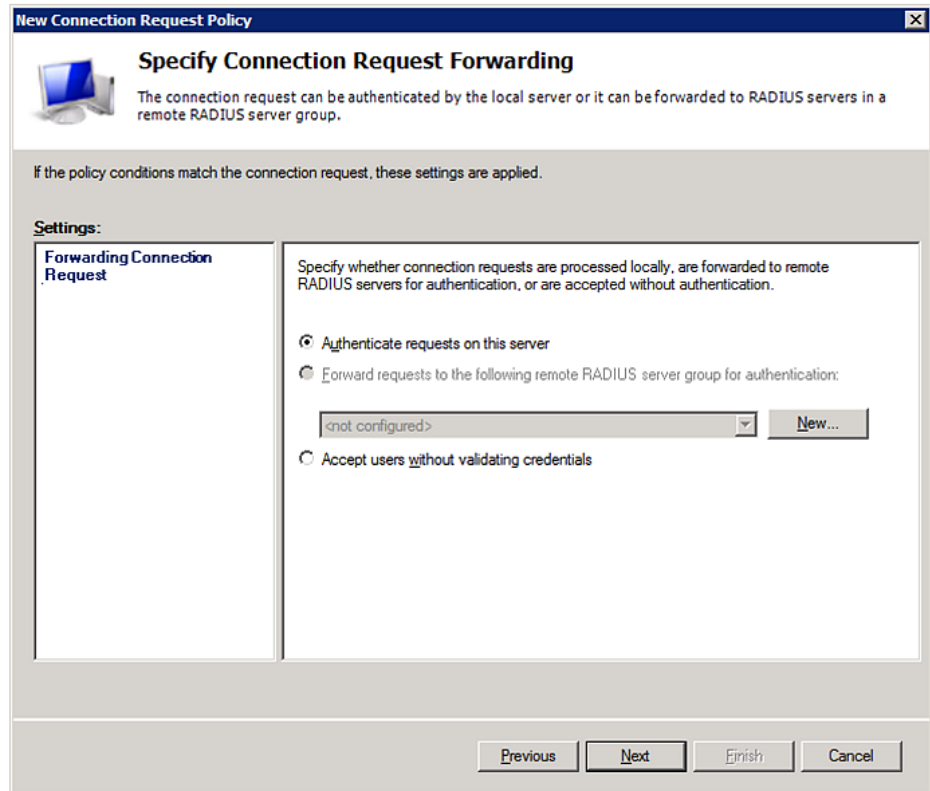
9. When the system prompts you to select the authentication method, select the following two options:

    ▪ Override network policy authentication settings

    ▪ CHAP -- the BCM2 uses "CHAP" in this example

Note: If your BCM2 uses PAP, then select "PAP."

10. Select Standard to the left of the dialog and then click Add.
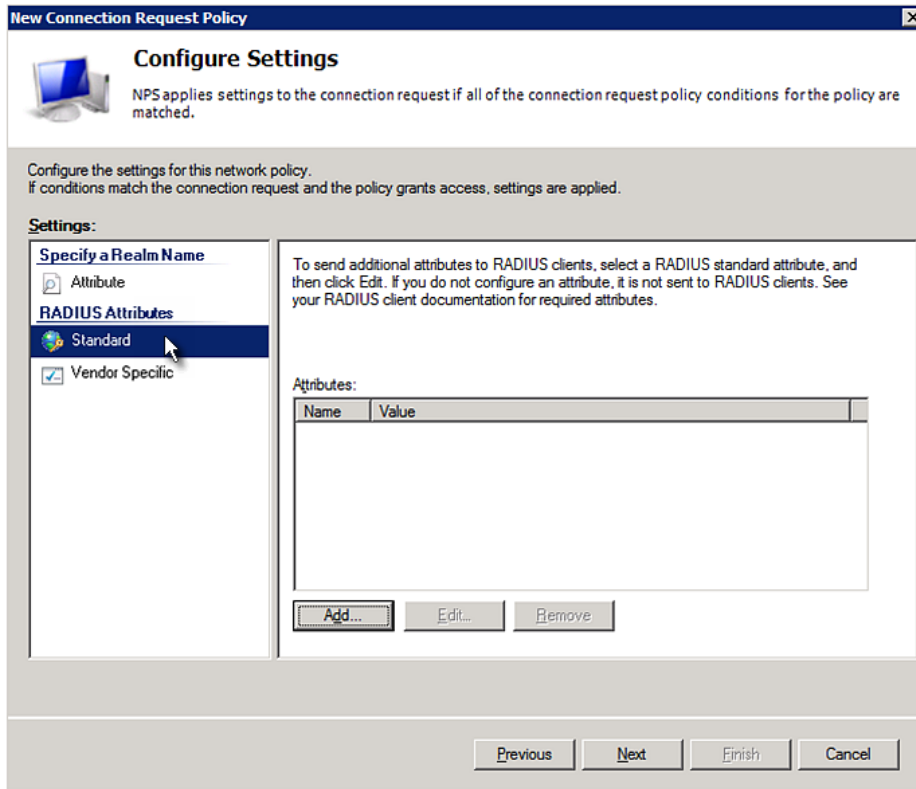
11. Select Filter-Id from the list of attributes and click Add.
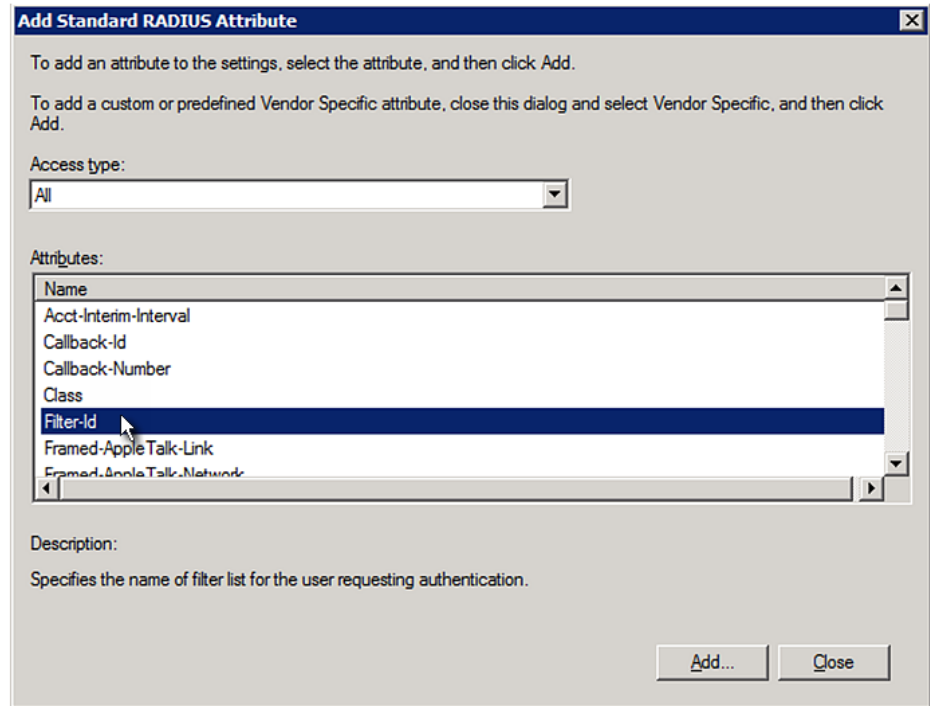
12. In the Attribute Information dialog, click Add.
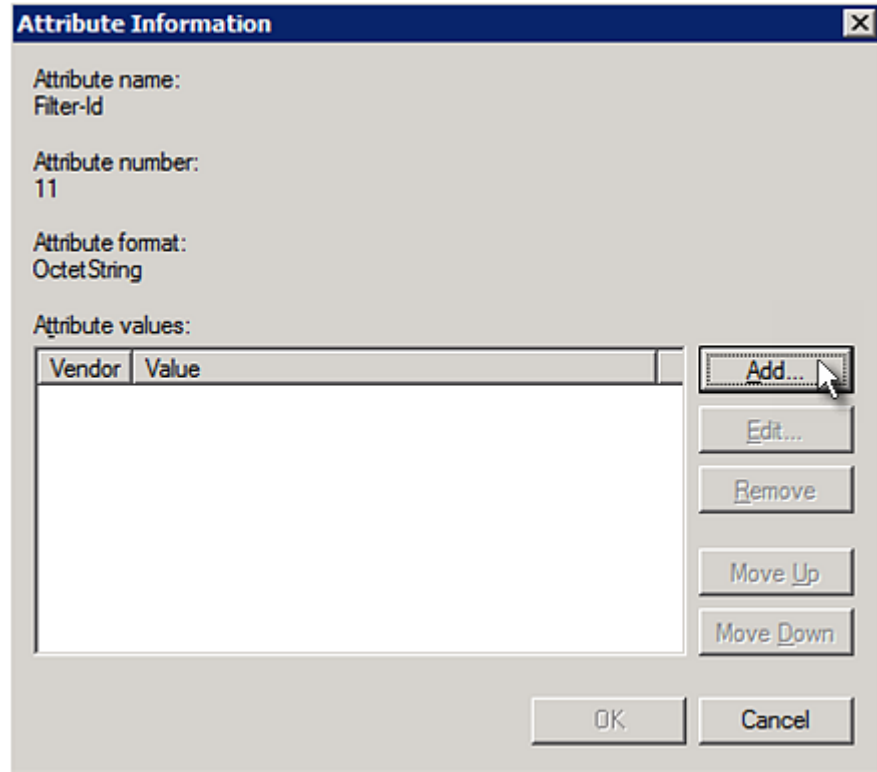
13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

Admin inside the curved brackets {} is the existing role on the BCM2. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.
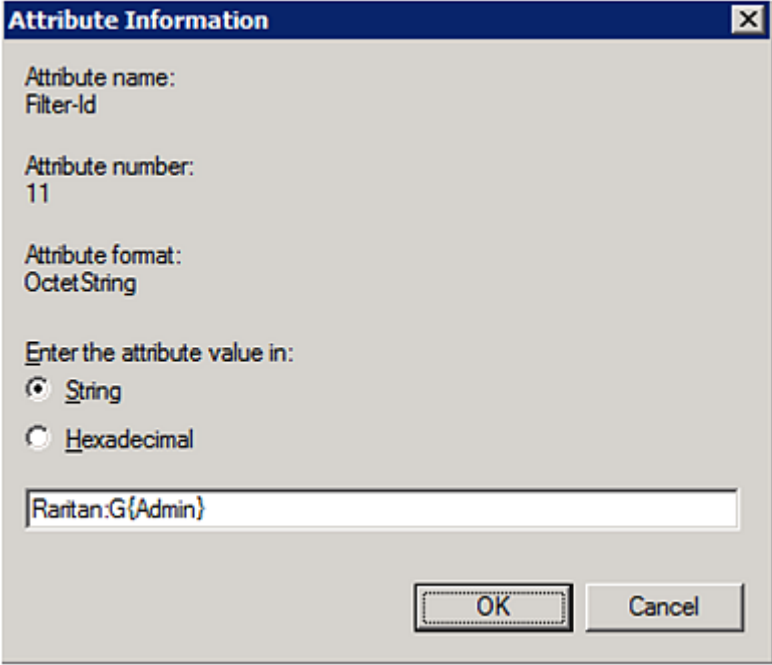
14. The new attribute is added. Click OK.
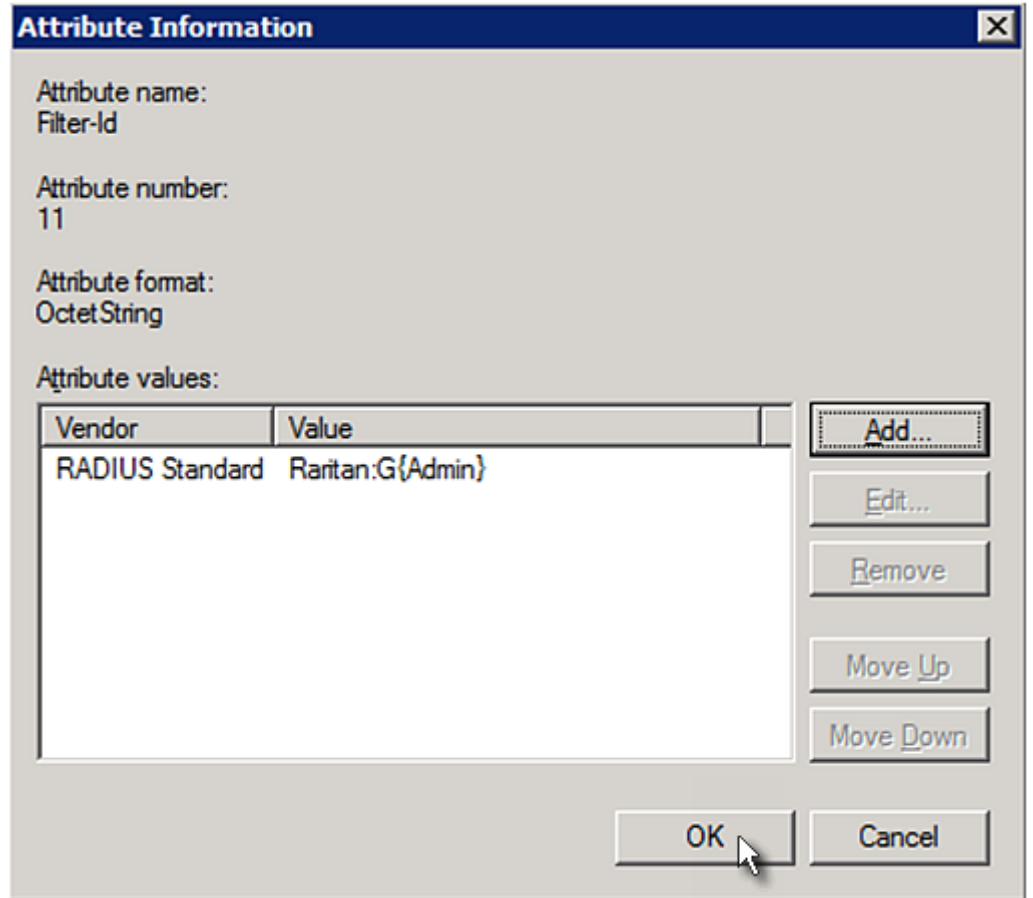
15. Click Next to continue.

16. A summary showing connection request policy settings is displayed. Click Finish to close the dialog.
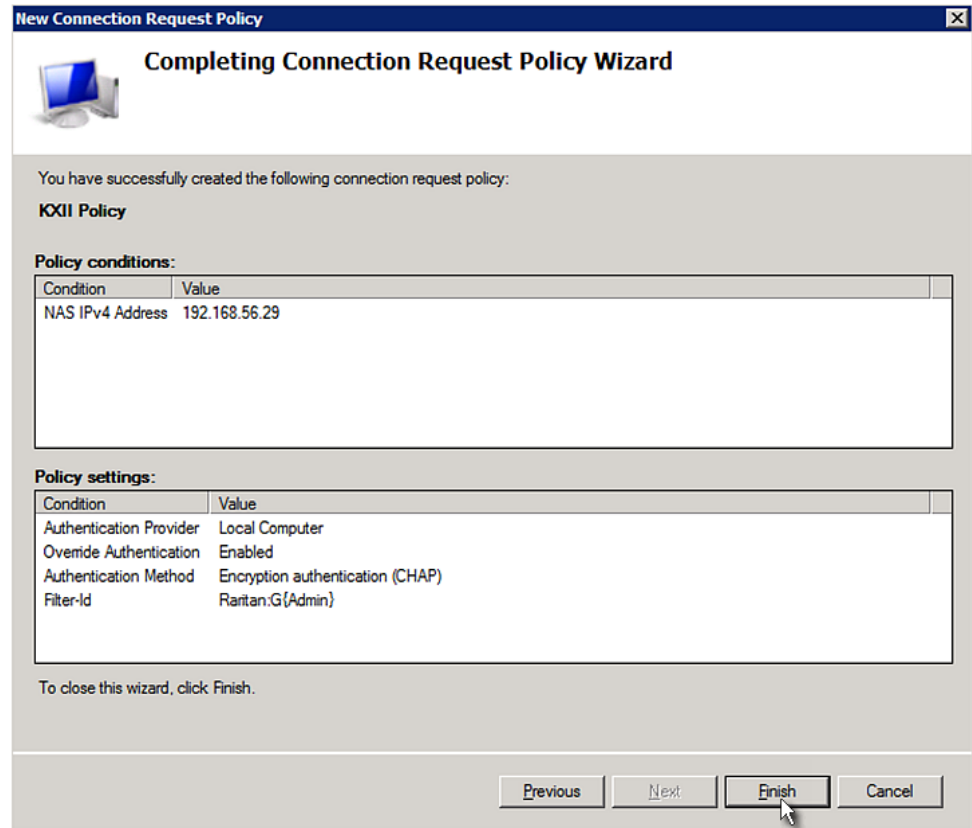
AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

- Register the NPS server in AD
- Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

▶ **To register NPS:**

1. Open the NPS console.

2. Right-click NPS (Local) and select "Register server in Active Directory."
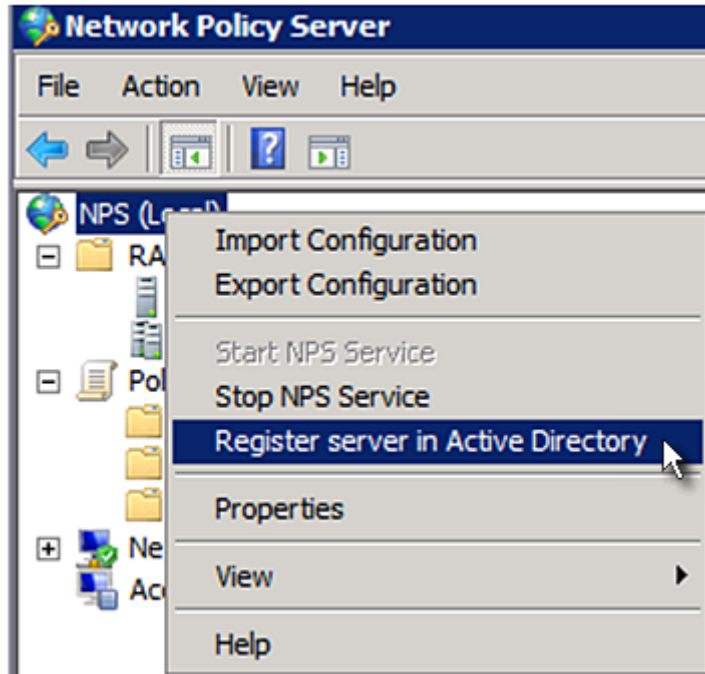
3. Click OK, and then OK again.
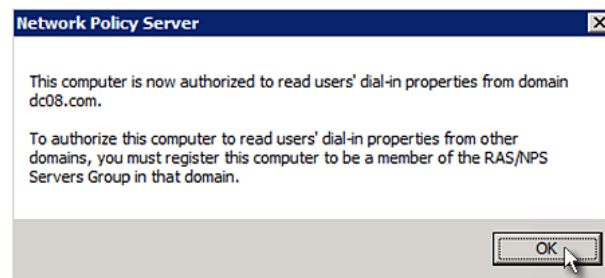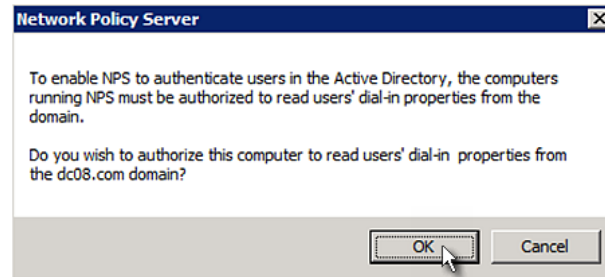
▶ **To grant BCM2 users remote access permission:**

1. Open Active Directory Users and Computers.

2. Open the properties dialog of the user whom you want to grant the access permission.

3. Click the Dial-in tab and select the "Allow access" checkbox.
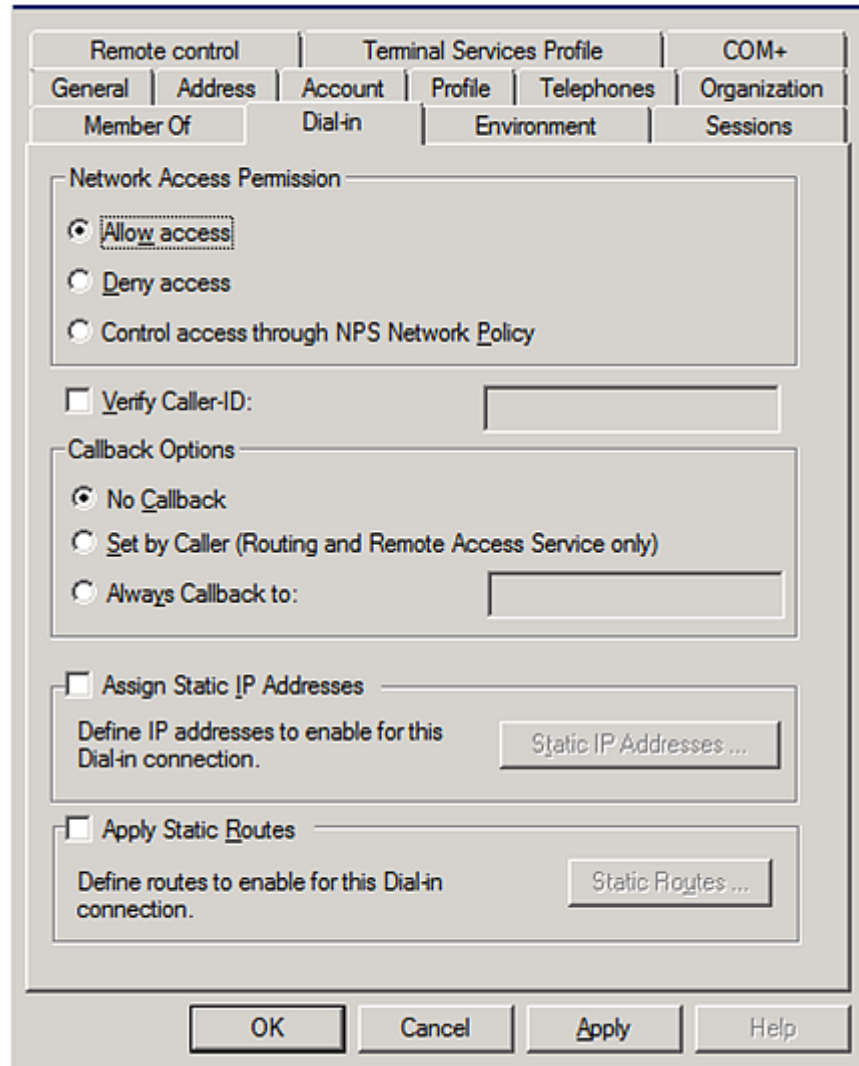
▶ **To enable reversible encryption for CHAP authentication:**

1. Open Active Directory Users and Computers.

2. Open the properties dialog of the user that you want to configure.

Raritan
A brand of 🔲legrand

3. Click the Account tab and select the "Store password using reversible encryption" checkbox.

FreeRADIUS VSA Illustration

A vendor-specific dictionary file is required for the vendor-specific-attribute configuration on FreeRADIUS. Therefore, there are two major configuration steps.

a. Use a dictionary to define the Raritan vendor-specific attribute

b. Add all user data, including user names, passwords, and roles

▶ **Presumptions in the illustration:**

- Raritan attribute = `Raritan-User-Roles`
- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin`, `User` and `SystemTester`

▶ **Step A -- define the vendor-specific attribute in FreeRADIUS:**

1. Go to this location: `/etc/raddb/dictionary`.
2. Type the following in the Raritan dictionary file.

```
VENDOR Raritan 13742
BEGIN-VENDOR Raritan
ATTRIBUTE Raritan-User-Roles 26 string
END-VENDOR Raritan
```

▶ **Step B -- create a user profile for "steve" in FreeRADIUS:**

1. Go to this location: `/etc/raddb/users`.
2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Raritan-PDU-User-Roles = "Raritan:G{Admin User SystemTester}"
```

Raritan.
A brand of ▢ legrand

Appendix D Additional BCM2 Information

In This Chapter

Raritan Training Website

Raritan offers free training materials for various Raritan products on the *Raritan training website http://www.raritantraining.com*. The Raritan products introduced on this website include the intelligent PDU, dcTrack®, Power IQ, KVM, EMX, BCM and CommandCenter Secure Gateway (CC-SG). Raritan would update the training materials irregularly according to the latest development of Raritan products.

To get access to these training materials or courses, you need to apply for a username and password through the Raritan training website. After you are verified, you can access the Raritan training website anytime.

Having access to the training website could be helpful for learning or getting some ideas regarding Raritan products and making correct decisions on purchasing them. For example, you can take the dcTrack video training before implementing or using it.

Altitude Correction Factors

If a Raritan differential air pressure sensor is attached to your device, the altitude you enter for the device can serve as an altitude correction factor. That is, the reading of the differential air pressure sensor will be multiplied by the correction factor to get a correct reading.

This table shows the relationship between different altitudes and correction factors.

Altitude (meters)	Altitude (feet)	Correction factor
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01

Altitude (meters)	Altitude (feet)	Correction factor
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Ways to Probe Existing User Profiles

This section indicates available ways to query existing user accounts on the BCM2.

- With SNMP v3 activated, you get the "user unknown" error when the user name used to authenticate does not exist.
- Any user with the permission to view event rules can query all local existing users via JSON RPC.
- Any user with the permission to view the event log may get information about existing users from the log entries.
- Any authenticated users can query currently-existing connection sessions, including Webcam-Live-Preview sessions, which show a list of associated user names.

Reserving IP Addresses in DHCP Servers

The BCM2 uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the BCM2 in a DHCP server, use the BCM2 device's serial number as the unique ID instead of the MAC address.

Since all network interfaces of the BCM2 can be simultaneously enabled and configured with diverse static IP addresses, the client identifier of each network interface is different. The main difference is the absence/presence of a suffix, which is the interface name added to the end of the serial number. The table below lists the client identifiers of all network interfaces.

Interface	Client Identifier
ETHERNET	serial number
WIRELESS	serial number plus the uppercase suffix "-WIRELESS"
BRIDGE	serial number

You can reserve the IP addresses of more than one interfaces in the DHCP server if preferred. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Reserving IP in Windows

To reserve the IP address of any network interface in the Windows DHCP server, you must convert that interface's client identifier into *hexadecimal* ASCII codes.

For each interface's client identifier, see *Reserving IP Addresses in DHCP Servers* (on page 480).

In the following illustration, it is assumed that the BCM2 serial number is PEG1A00003.

▶ **Windows IP address reservation illustration:**

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETHERNET	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
WIRELESS	PEG1A00003-**WIRELESS** = 50 45 47 31 41 30 30 30 30 33 **2D 57 49 52 45 4C 45 53 53** ▪ The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. In your DHCP server, bring up the New Reservation dialog, and separate the converted ASCII codes with spaces.

   For example, to reserve the IP address of the ETHERNET interface, enter the following data in the dialog.

Field	Data entered
IP address	The IP address you want to reserve.
MAC address	The following ASCII codes. 50 45 47 31 41 30 30 30 30 33
Other fields	Configure as needed.
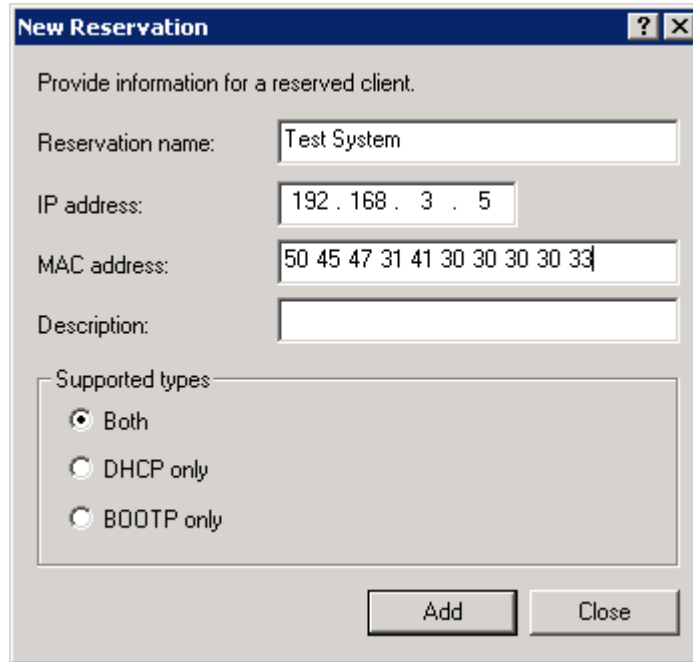
Reserving IP in Linux

There are two methods to reserve the IP address of any network interface in the standard Linux DHCP server (ISC DHCP server):

* Convert an interface's client identifier into *hexadecimal* ASCII codes.
* Use an interface's original client identifier without converting it into ASCII codes.

For each interface's client identifier, see *Reserving IP Addresses in DHCP Servers* (on page 480).

In the following illustrations, it is assumed that the BCM2 serial number is PEG1A00003, and the IP address you want to reserve is 192.168.20.1.

▶ **Illustration with ASCII code conversion:**

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETHERNET	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
WIRELESS	PEG1A00003-**WIRELESS** = 50 45 47 31 41 30 30 30 30 33 **2D 57 49 52 45 4C 45 53 53** ▪ The suffix comprising the dash symbol and the word "WIRELESS" is also converted.

Interface	Client identifier conversion
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. Separate the converted ASCII codes with a colon, and a prefix "00:" must be added to the beginning of the converted codes.

   For example, the *converted* client identifier of the ETHERNET interface looks like the following:

   `00:50:45:47:31:41:30:30:30:30:33`

3. Now enter the converted client identifier with the following syntax.

   host mypx {

   option dhcp-client-identifier = 00:50:45:47:31:41:30:30:30:30:33;

   fixed-address 192.168.20.1;

   }

▶ **Illustration without ASCII code conversion:**

1. Use the original client identifier of the desired network interface. DO NOT convert them into ASCII codes.

2. A prefix "\000" must be added to the beginning of the client identifier.

   For example, the client identifier of the ETHERNET interface looks like the following:

   `\000PEG1A00003`

3. Now enter the original client identifier with the following syntax. The client identifier is enclosed in quotation marks.

   host mypx {

   option dhcp-client-identifier = "\000PEG1A00003";

   fixed-address 192.168.20.1;

   }

Cascading Troubleshooting

Any accessibility problem occurred on one of the devices in the cascading chain may result in failure to access all downstream slave devices that are connected to it.

Possible Root Causes

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

You can always troubleshoot the software settings by connecting the BCM2 to a computer if network access to that BCM2 fails. See Connecting the BCM2 to a Computer.

Symptom	Probable cause

Failure to access the master device	• Network connection to the master device is lost.
	• No power is supplied to the master device.
	• The Ethernet or wireless interface on the master device is disabled.
	• IPv4 (or IPv6) settings are disabled on the master device.
	• In the port forwarding mode, the master device's role is incorrectly set to 'Slave'.
	• In the port forwarding mode, the interface where the network is connected is incorrectly selected as the downstream interface.
	• For the wireless networking, one of the following may lead to the accessibility failure:
	  ▪ The USB wireless LAN adapter attached to the master device is not the Raritan USB WIFI LAN adapter. See *USB Wireless LAN Adapters* (on page 58).
	  ▪ The wireless LAN configuration is not supported. See *Supported Wireless LAN Configuration* (on page 59).
	  ▪ The installed CA certificate chain contains any certificate that has expired or is not valid yet.

Symptom	Probable cause
Failure to access a slave device	- Network connection to the master device is lost. - The cascading cable connected to the slave device in question or any upstream device (if available) is loose or lost. - No power is supplied to the slave device in question or any upstream devices. - The Ethernet or wireless interface on the master device is disabled. - IPv4 (or IPv6) settings are disabled on the slave device in question. - The cascading mode of the slave device in question or any upstream device is set incorrectly. For example, the master device is set to Bridging, but one of the slave devices is set to Port Forwarding. - In the port forwarding mode, the master device's role is incorrectly set to 'Slave'. - In the port forwarding mode, the master device's downstream interface is incorrectly set. For example, you use a USB cable to connect the 1st slave device, but select the Ethernet port as the downstream interface. - In the port forwarding mode, the role of the slave device in question or any upstream device is set to 'Master' instead of 'Slave'. - In the port forwarding mode, the port number you added to the IP address is incorrect. See *Port Number Syntax* (on page 152). - The firmware version of the slave device in question or any upstream device is older than 3.3.10.

Tip: To determine which BCM2 may be the failure point of network, you may ping each BCM2 in the cascading chain, or check the slave-related events in the event log of each BCM2. See **Slave Connection and Disconnection Events** *(on page 486).*

Slave Connection and Disconnection Events

In the bridging mode, events regarding connection/disconnection of a downstream slave device via USB is NOT logged.

However, in the port forwarding mode, whenever the connection or disconnection of a downstream slave device via USB is detected, the BCM2 at the USB-A end of the USB cable logs it in the internal log. Note that the BCM2 at the USB-B end of the cable does NOT log these events.

There are two slave-related events:

Event	Description
Slave connected	This log entry is generated when a BCM2 detects the presence of a slave device on its USB-A port.
Slave disconnected	This log entry is generated when it detects the disconnection of a slave device from its USB-A port.

The Ping Tool

The BCM2 provides a ping tool in the web interface and CLI so you can ping any host or BCM2 in your data center.

Ping via the Web Interface

To log in to the web interface, see HTTP/HTTPS Access.

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.
2. Type values in the following fields.

Field	Description
Network Host	The name or IP address of the host that you want to check.
Number of Requests	A number up to 20. This determines how many packets are sent for pinging the host.

3. Click Run Ping to ping the host. The Ping results are then displayed.

Ping via the CLI

You can access the CLI interface by connecting a computer to the BCM2 or using SSH/Telnet. See *SSH/Telnet Access* (see "*With SSH or Telnet*" on page 281) for details.

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

```
#        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.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds ranging from 1 to 600.

The command looks like the following when it includes all options:

```
diag>      ping <host> count <number1> size <number2> timeout <number3>
```

Index

Raritan.
A brand of legrand

Raritan.
A brand of legrand

Raritan.
A brand of legrand

Raritan.
A brand of legrand

Raritan.
A brand of legrand

W

Y