UHF Gen 2 RFID Speedway Reader (IPJ-R1000)

# Octane 3.0 User Guide

9501101260000000469

**www.impinj.com**
Copyright © 2008, Impinj, Inc.

# Overview

The EPCglobal™-certified Speedway™ IPJ-R1000 reader is a stationary, UHF Gen 2 RFID tag reader that provides network connectivity between tag data and enterprise system software.

A key element of Impinj's GrandPrix™ RFID system solution, the Speedway reader is the first high-performance reader designed from the ground up to support the EPCglobal Gen 2 standard in its entirety, including the accommodation of 640 kbps tag-to-reader data rates, robust performance in dense-reader environments, operation in near- and far-field applications, and more. Combined with an extensible architecture that supports seamless integration of field-upgradeable, third party application software, the Speedway reader is the most adaptable reader solution available today.

This user guide provides instructions on how to install, connect, configure, operate, upgrade, and troubleshoot Speedway readers. It assumes the user is familiar with appropriate networking facilities, the EPCglobal Gen 2 specification, and general principles of RFID system management.

**Important**    The user guide only covers readers having part numbers in the following format: IPJ-R1000-ABC1MZ, where ABC is the country code, M indicates mass production, and Z is a number indicating the packaging and accessory options.

Countries decode as:
- USA = United States, FCC certification (also includes Canadian certification)
- EU1 - Euopean EU302-208
- AS1 = Taiwan
- CHN = China
- JPN = Japan

Packaging and Accessory Options decode as:
- 1 = 1-up box, No power module
- 2 = 5-up box, No power module
- 3 = 1-up box, power module included
- 4 = 5-up box, power module included

# Federal Communications Commission (FCC) Compliance

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

• Reorient or relocate the receiving antenna
• Increase the separation between the equipment and receiver
• Consult the dealer or a qualified radio/TV technician for assistance

**Caution**   Changes to this product or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate per FCC Part 15.

# Industry Canada (IC) Compliance

Operation is subject to the following two conditions: (1) this device may not cause interference and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with the antenna(s) listed in Section 2.6 that have a maximum gain of 6 dB. Antennas not included in this list or having a gain greater than 6 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that permitted for successful communication.

**Note**

The term "IC:" before the radio certification number only signifies that Industry of Canada technical specifications were met.

# CE Marking and European Economic Area (EEA)

RFID devices designed for use throughout the EEA must have a maximum radiated transmit power of 2W ERP in the frequency range of 865.6–867.6 MHz. For other EEA restrictions on RFID device use, please refer to the Impinj Declaration of Conformity (DoC) located at http://rfid-support.impinj.com

# Before You Begin

**Warning**

Please read this document in its entirety before operating the Speedway reader, as serious personal injury or equipment damage may result from improper use.

Unauthorized opening of the Speedway reader enclosure voids the warranty.

## Table of Contents

Octane 3.0 User Guide

# 1 Regions of Operation

The Speedway reader has been designed to work in various regions with differing frequency requirements. This document covers operation in North America, Europe, China, and Taiwan.

**Important**   In each region, the reader is locked to only operate in the specific frequencies listed in the respective frequency plan tables (Table 1-1 through Table 1-6).

## 1.1 Operation in North America

The FCC specifies frequency hopping across the North American spectrum allocated to UHF RFID (902–928 MHz, with hopping occurring between 902.75–927.25 MHz in 500 KHz steps). See Table 1-1.

**Table 1-1 Frequency Plan for North America**

| Transmit Channel Number | Center Frequency (MHz) |
|:---:|:---:|
| 1 | 902.75 |
| 2 | 903.25 |
| 3 | 903.75 |
| 4 | 904.25 |
| . . . | . . . |
| 49 | 926.75 |
| 50 | 927.25 |

## 1.2 Operation in Europe

For European operation, the Speedway reader supports the frequency plan listed in Table 1-2 and operates under EN 302-208 using listen-before-talk (LBT). An optional setting allows use of a third-party controller for deployment where readers share channels. Consult the manufacturer of compatible controllers for details on how to setup and deploy.

**Table 1-2 Frequency Plan for Europe**

| Transmit Channel Number | Center Frequency (MHz) |
|---|---|
| 4 | 865.7 |
| 7 | 866.3 |
| 10 | 866.9 |
| 13 | 867.5 |

## 1.3 Operation in China

The Speedway reader supports the frequency plans listed in Table 1-3 for operation in China. The Speedway reader complies with Chinese regulations and provides sixteen high power channels in the 920.625–924.375 MHz frequency band, numbered 3 to 18. The default operation is 1 MHz channel spacing, with the four channels specified in Table 1-4. Or as an alternative, the user may provide a list up to 16 in length from the available channels specified in Table 1-3. The reader can also channel hop in a pseudo-random manner over a channel list, which can be either the default set shown in Table 1-4, or user specified.

**Table 1-3 Frequency Plan for China**

| Transmit Channel Number | Center Frequency (MHz) |
|---|---|
| 3 | 920.625 |
| 4 | 920.875 |
| 5 | 921.125 |
| 6 | 921.375 |
| 7 | 921.625 |
| 8 | 921.875 |
| 9 | 922.125 |

**Table 1-3 Frequency Plan for China**

| Transmit Channel Number | Center Frequency (MHz) |
|---|---|
| 10 | 922.375 |
| 11 | 922.625 |
| 12 | 922.875 |
| 13 | 923.125 |
| 14 | 923.375 |
| 15 | 923.675 |
| 16 | 923.875 |
| 17 | 924.125 |
| 18 | 924.375 |

**Table 1-4 Default Frequency Plan for China**

| Transmit Channel Number | Center Frequency (MHz) |
|---|---|
| 3 | 920.625 |
| 7 | 921.625 |
| 11 | 922.625 |
| 15 | 923.625 |

## 1.4 Operation in Taiwan

The Speedway reader supports the frequency plan listed in Table 1-6 for operation in Taiwan. The NCC stipulates frequency hopping across the Taiwanese spectrum allocated to UHF RFID (922-928 MHz, with hopping occurring between 922.25–927.75 MHz in 500 KHz steps).

**Table 1-5 Frequency Plan for Taiwan**

| Transmit Channel Number | Center Frequency (MHz) |
|---|---|
| 1 | 922.25 |
| 2 | 922.75 |
| . . . | . . . |
| 11 | 927.25 |
| 12 | 927.75 |

## 1.5 Operation in Japan

The Speedway reader supports the frequency plans listed in Table 1-6 for operation in Japan. The MIC allocates a six MHz range of the Japanese spectrum to UHF RFID (950-956 MHz). The standard transmit power is 30 dBm at the connector.

**Table 1-6 Frequency Plan for Japan**

| Transmit Channel Number | Center Frequency (MHz) |
|---|---|
| 1 | 952.2 |
| 2 | 952.4 |
| . . . | . . . |
| 8 | 953.6 |
| 9 | 953.8 |

# 2 Setting Up the Speedway Reader

The Speedway reader unit requires a power supply module with 24 VDC output. Ensure that power supply module has one of the following part numbers:

For regions other than Japan, CUI, Inc., **ETS240250U-P11P-DB-IM** (power brick) with one of the following power cords:
AC1 for North America
AC2 for European Union
AC4-1 for China

For any region, including Japan, CUI, Inc., **ETS240250U-P11P-C1-DP-IM** (power brick) with one of the following power cords:
AC1 for North America or Japan
AC2 for European Union
AC4-1 for China

**Warning**    The use of any other power supply module may cause damage to the reader.

## 2.1 Hardware Version

Every reader has a label on the side listing the part number, the serial number, the MAC address, and the hardware revision number.



**Figure 2-1 Reader Labeling**

## 2.2 System and Equipment Requirements

Table 2-1 summarizes the supported operating environments.

**Table 2-1 Operating Environments**

| Interface | Protocol | Recommended Tools | | |
|---|---|---|---|---|
| | | Microsoft® Windows | Linux | Mac/Other |
| Web Interface | HTTP | Compatible with common browsers Microsoft® Internet Explorer® (6+) and Mozilla® Firefox® (1.5+)[a] | | |
| Remote Login | SSH/Telnet | Putty | SSH or Telnet | Terminal |
| Serial | RS-232 | Hyperterminal | Minicom | N/A |

a. Microsoft and Internet Explorer are registered trademarks or trademarks of the Microsoft Corporation in the United States and/or other countries.
Mozilla and Firefox are registered trademarks or trademarks of the Mozilla Foundation.

The components and accessories detailed below are required in order to ensure compliance with the Speedway reader. It is the responsibility of the user or professional installer to provide and properly use all these components and accessories:

- A computer running Microsoft® Windows® 2000 (or higher), XP, or Linux PC, which has:
  - An available RS-232 serial port (required only if host system does not support DHCP)
  - Standard, grounded DB9 serial cable (required only if system does not support IP provisioning)
  - An Ethernet port
  - Standard Ethernet cable(s)
  - HTTP browser that includes the Java™ Runtime Environment (JRE)[1], version 1.4.2 or later. Note that the Microsoft Windows 2000 JRE default is version 1.3.1. The latest version of JRE can be downloaded from: http://www.java.com/en/download/manual.jsp (to determine/verify your version, go to http://www.java.com/en/download/installed.jsp)
- TCP/IP network equipment, as required to connect the reader to a PC, Mac, or other network terminal
- Impinj-approved UHF RFID antenna(s), including associated RF cable with RP-TNC male connector interface

---

1. Java and Java Runtime Environment are either registered trademarks or trademarks of Sun Microsystems, Inc. in the United States and other countries.

## 2.3 Speedway Reader I/O Ports & Status

Refer to Figure 2-1 for the location of the Speedway reader's major ports, connectors, and status indicators, which are clearly indicated on the unit. The Speedway reader is equipped with the following ports:

- RJ-45 Ethernet port (labeled 10/100 BASE-T)

- Female DB-9 connector for serial communication (SERIAL)

- Female DB-25 connector with user I/O capability (GPIO) The GPIO contains: RS-232 serial interface, four 3.3/5V logic inputs, and eight 3.3V logic outputs. See Table 2-2 for the pin-out, Table 2-3 for the GPIO electrical specifications, and Figure 2-2 for the physical pin view.

- Four female RP-TNC RF antenna connectors (ANT1 – ANT4)
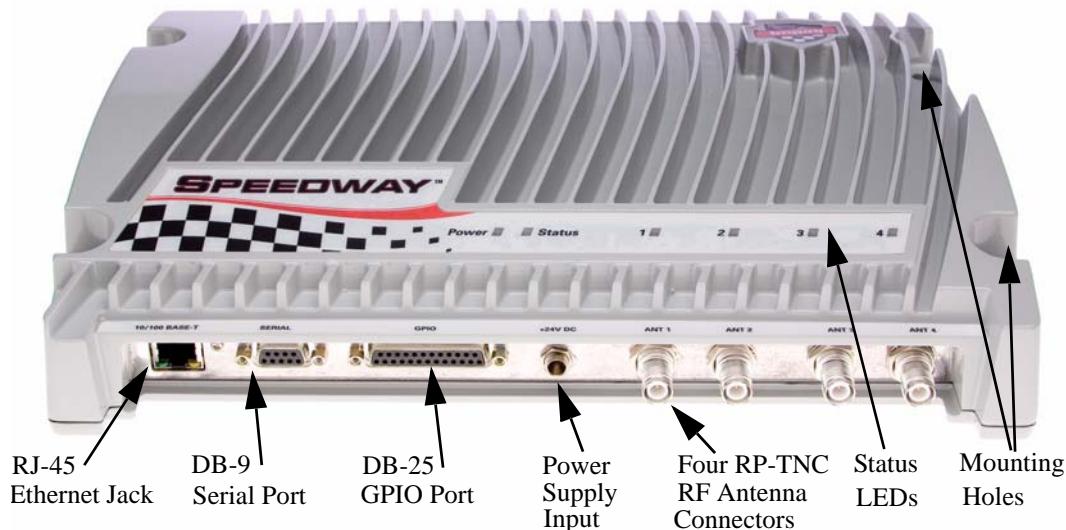


**Figure 2-1    Impinj Speedway Reader Port Connections**

**Table 2-2 DB-25 Connector Pin-Out**

| Pin | I/O | Pin | I/O | Pin | I/O |
|-----|-----|-----|-----|-----|-----|
| 1 | No connect | 10 | GPIN3 | 19 | GPOUT5 |
| 2 | RS-232 RXD | 11 | GPIN2 | 20 | No connect |
| 3 | RS-232 TXD | 12 | GPIN1 | 21 | GPOUT6 |
| 4 | RS-232 CTS | 13 | GPIN0 | 22 | No connect |

**Table 2-2 DB-25 Connector Pin-Out (continued)**

| Pin | I/O | Pin | I/O | Pin | I/O |
|-----|-----|-----|-----|-----|-----|
| 5 | RS-232 RTS | 14 | GPOUT0 | 23 | GPOUT7 |
| 6 | No connect | 15 | GPOUT1 | 24 | No connect |
| 7 | Signal Ground | 16 | GPOUT2 | 25 | No connect |
| 8 | No connect | 17 | GPOUT3 | | |
| 9 | No connect | 18 | GPOUT4 | | |

**Caution**      Pins listed in Table 2-2 as "No connect" must be left unconnected.

**Table 2-3 GPIO Interface Electrical Specifications**

| Pin | Parameter | Description | Min | Max | Unit | Conditions |
|-----|-----------|-------------|-----|-----|------|------------|
| GPIN[3:0] | $V_{IH}$ | HIGH-level input voltage | 2 | 5 | V | |
| GPIN[3:0] | $V_{IL}$ | LOW-level input voltage | 0 | 0.8 | V | |
| GPIN[3:0] | $I_{LI}$ | Input Leakage Current | -5 | 5 | µA | $V_{in}$=0–5V |
| GPIN[3:0] | $V_I$ | Input Voltage Range | -5 | 5 | V | No damage |
| GPOUT[7:0] | $V_{OH}$ | HIGH-level output voltage | 3 | 3.3 | V | $I_{out}$ = 100 µA |
| GPOUT[7:0] | $V_{OL}$ | LOW-level output voltage | 0 | 0.25 | V | $I_{out}$ = -100 µA |
| GPOUT[7:0] | $V_I$ | Input voltage range | -5 | 5 | V | No damage |
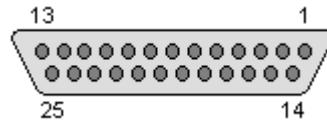
**Figure 2-2 DB-25 Female Connector**

The labeled LEDs indicate Power, Status, and antenna activity. The LEDs that correspond to the connected antenna(s) (labeled 1, 2, 3, and 4)**,** only light green when active (transmitting). A description of the status LED states appears in Table 2-4.

**Table 2-4 LED Status Indicators**

| Reader Operation | LED Action |
|---|---|
| Startup | Continuous Red |
| Power-on Start Test (POST) Failure | Flashing Red (~2 Hz) |
| Bootloader Running | Off |
| File System Mounting Operation[1] | Alternately Flashing Red/Green (1 Hz) |
| Speedway Reader able to Accept Mach1™[2] or LLRP Connection | Continuous Green |
| Speedway Reader in Active Mach1™ Connection | Flashing Green (1 Hz, 50% duty cycle) |
| Speedway Reader in Active LLRP Connection | Double Flashing Green (1 Hz, 40% duty cycle) |
| Speedway Reader in Disconnected LLRP Operation | Single Flashing Green (1 Hz, 20% duty cycle) |
| Inventory in Progress with Tags in Field | Flashing Orange (Frequency increases with the number of tags) |
| Inventory in Progress with no Tags in Field | Flashing Orange (1/3 Hz) |

1. May also occur in certain upgrade scenarios to indicate the unit is functional but in a file system operation that will take some time to complete.
2. Mach1™ denotes the Speedway RFID Command Interface, used by the reader to communicate with EPCglobal™ Generation 2 (Gen 2) RFID tags. LLRP denotes the Low Level Reader Protocol, the EPCglobal standard for the client-reader interface.

## 2.4 Mounting the Speedway Reader

When securing the unit with #10 screws via the four mounting holes, the Speedway reader may be mounted horizontally or vertically on a stable surface where it will be safe from disturbance. Keep the unit away from direct sunlight, high humidity, extreme temperatures, vibration, and sources of electromagnetic interference, as any combination of these conditions may degrade performance or shorten the life of the unit.

## 2.5 Connecting Power

Connect the AC power plug into a suitable 100-240 VAC, 50-60 Hz power outlet. The reader's green Power LED will light when power is on.  The reader will then begin its boot sequence (the normal boot time for the reader's operating system is ~50 seconds). The reader will not accept commands until the boot sequence is complete.

## 2.6 Connecting the Antenna(s)

The Speedway reader is equipped with four (4) independent, bidirectional, full duplex TX/RX ports (monostatic).

**Caution**   Unused antenna ports must be left unconnected; they should not be terminated.

### 2.6.1 FCC, Industry Canada, and Taiwan

**Warning**   Position reader antennas such that any personnel in the area for prolonged periods of time may safely remain at least 25 cm from the antenna's surface. See FCC OET Bulletin 65, "Evaluating Compliance with FCC Guidelines for Human Exposure to Radiofrequency Electromagnetic Fields," and FCC OET Bulletin 56, "Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields," for more details.

**Warning**   Readers of hardware revision 2.0 (see Section 2.1) and higher and running firmware versions 2.6.0 and higher are capable of up to 32.5 dBm conducted power on the Speedway housing RF connector and require professional installation.

For readers of hardware revision 1.X.X, power has been factory preset to 30 dBm to accommodate an antenna with 6 dBi composite gain (inclusive of cabling).The Speedway reader may only be operated with Impinj-approved antennas and can radiate no more than 36 dBm EIRP (Equivalent Isotropically Radiated Power) per FCC Part 15.247 regulations. The Speedway output power may be increased to provide the maximum allowable EIRP subject to a maximum conducted power allowance as well. The maximum conducted power at the antenna connector can be no more than 30 dBm. The maximum allowable output power of the reader can be set to satisfy both the conducted and radiated maximum criteria. The expression for the maximum reader power setting is:

Maximum power setting (in dBm)
= The **Smaller** Of
(36 – Composite Antenna Gain (in dB))
OR
(30 + Cable loss (in dB)),

where the composite antenna gain comprises the maximum linear antenna gain in dBi minus any cable loss between the reader and antenna in dB. Approved antenna vendors, model numbers, and associated gain are listed below:

- Cushcraft model number S9028PCL/R (left- or right-hand CP), with integrated 8 foot pigtail to RP-TNC male connector; 6 dBi composite gain

- Impinj model number IPJ-A0301-USA (Mini-Guardrail) with SMA female connector; -15 dBi gain

- Impinj model number IPJ-A0310-USA (Threshold-T Antenna) with 12 inch integrated pigtail to BNC male connector, 6 dBi composite gain.

- Impinj model number IPJ-A0400-USA, CSL CS-777-2  (Brickyard) with 7 foot integrated pig-tail to RP-TNC male connector; 2 dBi composite gain

- Impinj model number IPJ-A0401-USA (Guardwall) with 6 foot integrated pigtail to RP-TNC male connector; 6 dBi composite gain

- MA/COM MAAN-000246-FL1 integrated RFID floor-mounted stand (multiple configurations available, 2 or 4 antennas left-hand and right-hand CP) with 8 foot integrated pigtail to RP-TNC male connector; 6 dBi composite gain

- MA/COM MAAN-000246-WL1 integrated RFID wall-mounted stand (multiple configurations available, 2 antennas left-hand and right-hand CP) with 8 foot integrated pigtail to RP-TNC male connector; 6 dBi composite gain

- MTI MT-262006/TLH (left-hand CP) or MT-262006/TRH (right-hand CP) with RP-TNC female connector (antennas available in IP54 or IP67 ratings); 6 dBi gain

- MTI MT-262013/NLH (left-hand CP) or MT-262013/NRH (right-hand CP) with N-type female connector (antennas available in IP54 or IP67 ratings); 4.5 dBi gain

- MTI MT-262013/TLH (left-hand CP) or MT-262013/TRH (right-hand CP) with RP-TNC female connector (antennas available in IP54 or IP67 ratings); 4.5 dBi gain

- Sensormatic Electronics Corp. model number IDANT20TNA25 with 25 foot Belden 7806A RG-58 coaxial cable (0.1 dB per foot loss) to RP-TNC male connector; 5.5 dBi composite gain

- Sensormatic Electronics Corp. model  number IDANT10CNA25 with 25 foot Belden 7806A coaxial cable (0.1 dB per foot loss) to RP-TNC male connector; 3.5 dBi composite gain

- Sensormatic Electronics Corp. model  number IDANT10CNA25 with 6 foot Belden 7806A coaxial cable (0.1 dB per foot loss) to RP-TNC male connector; 5.4 dBi composite gain

**⚠ Warning**    The use of any antenna not listed above may damage the reader or adversely affect performance.

## 2.6.2 China and European Economic Area

Chinese and European regulations allow a maximum radiated power of 33 dBm ERP (Effective Radiated Power) for high power RFID systems.  The maximum Speedway output power is determined by the following equation:

**Maximum power setting (in dBm) = 33 − Antenna Gain (in dBd) + Cable loss (in dB)**

For example, for an application with an antenna gain of 6 dBd and cable loss of 2 dB, the reader output power can be set no higher than 33-6+2 = 29 dBm. Note that it is important to apply the antenna gain expressed in dBd (dB with respect to a dipole), which is equivalent to the isotropic antenna gain (in dBi) minus 2.15 dB. Additionally, the antenna gain used to set the output power must be the maximum linear gain of the applicable antenna. Approved antenna vendors, model numbers, and associated gain are listed below:

- Cushcraft Model Number S8658PCL/R (left- or right-hand CP) with integrated pigtail to RP-TNC male connector; 3.85 dBd gain

- Impinj Model Number IPJ-A0400-EU1, CSL CS-777-1 (Brickyard) with 7 foot integrated pigtail to RP-TNC male connector; 0 dBd composite gain

- MTI MT-242032/NLH (left-hand CP) or MT-242032/NRH (right-hand CP) with N-type female connector (antennas available in IP54 or IP67 ratings); 1.85 dBd gain

- Sensormatic Electronics Corp. Model number IDANT10CEU25 (left-hand CP only) with 6 foot Belden 7806A coaxial cable (0.1 dB per foot loss) to RP-TNC male connector; 3.25 dBd composite gain

**Warning**    The use of any antenna not listed above may damage the reader or adversely affect performance.

## 2.6.3 Japan

Japanese regulations limit reader transmit power to 1 W (or 30 dBm) and the absolute gain of the connected transmission antenna to 6 dBi. The  Speedway reader, limited to 30 dBm, complies.

Approved antenna vendors, model numbers, and associated gain are listed below:

- Impinj Model Number IPJ-A0303-000, with 2 meter RG-58 cable, (RP-TNC to  SMA connectors);  -20.6 dBi composite gain

- MTI MT-262017/NLH (left-hand CP) or MT-262017/NRH (right-hand CP) with 2-meter RG-58 cable (N-type connector); 5.0 dBi composite gain

**Note**    All antenna connectors are female, as are the Speedway reader connectors. The cable connectors are male.

**Warning**    The use of any antenna not listed above may damage the reader or adversely affect performance.

# 3 Connecting to the Speedway Reader

There are four ways of communicating with the Speedway reader: the Web-based interface, the command line interface (or "rshell"), the Mach1 interface, and the LLRP interface. The Web-based interface is a means of configuring the reader, obtaining status, and demonstrating RFID operation. The command line interface is an alternate way to configure the reader and obtain status if not using the Web interface. Both the Web-based interface (see Section 4, Section 5, and Section 6) and the CLI (see Section 8) are covered in this user guide. The CLI interface is available remotely through SSH and telnet, and available locally on the serial port (see Section 3.2).

The Mach1 interface, a comprehensive RFID command interface, is used both by clients to communicate with the reader (to configure it) and by the reader itself to communicate with EPCglobal™ Generation 2 (Gen 2) RFID tags. The description of this interface is covered in other documents. Many application providers offer software that is compatible with Mach1. Consult your solutions provider or applications software vendor for additional information.

The LLRP interface is an EPCglobal™ standard interface that supports client control of RFID readers. It is used both to configure the reader and to communicate with EPCglobal Generation 2 (Gen 2) RFID tags. The description of this interface is covered in other documents.

## 3.1 Basic Network Setup

This section provides instructions for the most straightforward network setup. For additional options, see Section 3.2 and Section 3.3.

### 3.1.1 Default network configuration

A factory-configured, Speedway reader running firmware version 2.6.0 has the following default network configuration:

- **hostname**:  The reader comes with a default hostname of  "Speedway-XX-XX-XX," where the XX-XX-XX are the last three bytes of the unit's MAC address (printed on the Speedway reader enclosure and expressed in hexadecimal, e.g., MAC 00:16:25:**00:02:2E** becomes "Speedway-**00-02-2E**"). See Section 2.1 for the location of the MAC address on the enclosure.

- **DHCP**: the reader has DHCP enabled and will report its configured hostname to the DHCP server.

- **LLA**: Link Local Addressing is enabled, permitting the reader to select a 169.254.XXX.XXX address when DHCP is not available.

- **mDNS/DND-SD**: Multi-cast DNS service discovery is enabled by default, allowing access via zero-configuration networking  (e.g., Apple® Bonjour®)[1] without an existing DHCP or DNS server.

**Note** Upgrading  just the Speedway OS partition (SOP, see Section 7 introduction) to 2.6 from previous firmware versions will not alter an existing reader's network configuration. Upgrading both the Speedway OS partition and the Speedway Configuration Partition (SOP and SCP, see Section 7 introduction and Section 7.9, specifically)  will result in the reader being restored to the factory default configuration once the new image is activated.

---

1. Apple, Bonjour, and the Bonjour icon are registered trademarks or trademarks of Apple, Inc.

### 3.1.2 Hardware Connections

Connect the reader to your network via the Ethernet port (see Figure 3-1).



**Ethernet**

**Ethernet**

PC
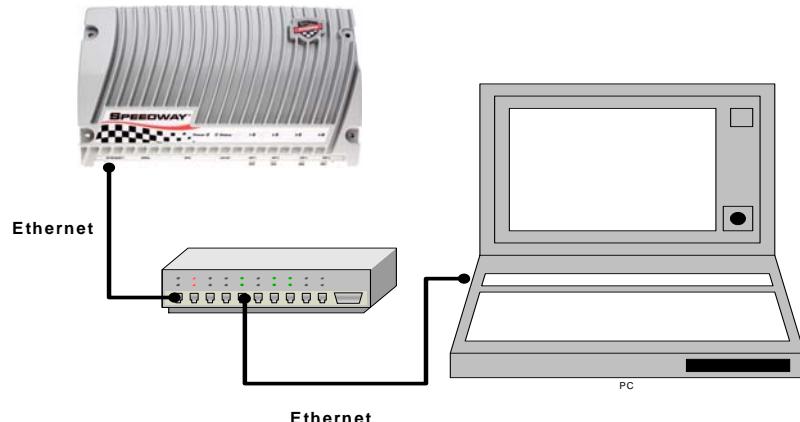
**Figure 3-1 Ethernet Connectivity**

### 3.1.3 Zero-configuration Networking Option

The Speedway reader supports zero-configuration networking. Zero-configuration networking is a term used to indicate devices that have included software in their design to enable automatic discovery of other devices on IP networks. This software uses industry standard protocols to permit automatic discovery without entering IP addresses or configuring DNS servers.

One of the ways the Speedway reader supports straightforward zero-configuration network connectivity is through the Microsoft® Internet Explorer® browser[1] using the Apple® Bonjour® plug-in, which implements an auto service discovery feature.

To obtain the plug-in, navigate to:
**http://www.apple.com/support/downloads/bonjourforwindows.html**
and follow the download and installation instructions.

Once the plug-in is installed, open an Internet Explorer window. The Bonjour icon will appear in the toolbar along the top of the screen. See Figure 3-2.

**Figure 3-2 Bonjour Icon**

---

1. Microsoft and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Copyright © 2008, Impinj, Inc.

Selecting this icon will bring up a menu along the left side of the browser with all discovered devices. See Figure 3-3.

Speedway readers will be identified by a hostname of the word "Speedway" concatenated with the last three bytes of the unit's MAC address (printed on the Speedway reader enclosure and expressed in hexadecimal, e.g., MAC 00:16:25:**00:02:2E,** see Section 2.1), separated by "**-**" (e.g., Speedway-**00-02-2E**).

Double click on the appropriate Speedway reader listed to bring up the Web interface and log onto the reader by entering the established user name and password. The default login (case-sensitive) is:

```
User Name: root
Password: impinj
```

At this point, proceed to Section 4, Section 5, and Section 6 for instructions on how to use the Web interface.
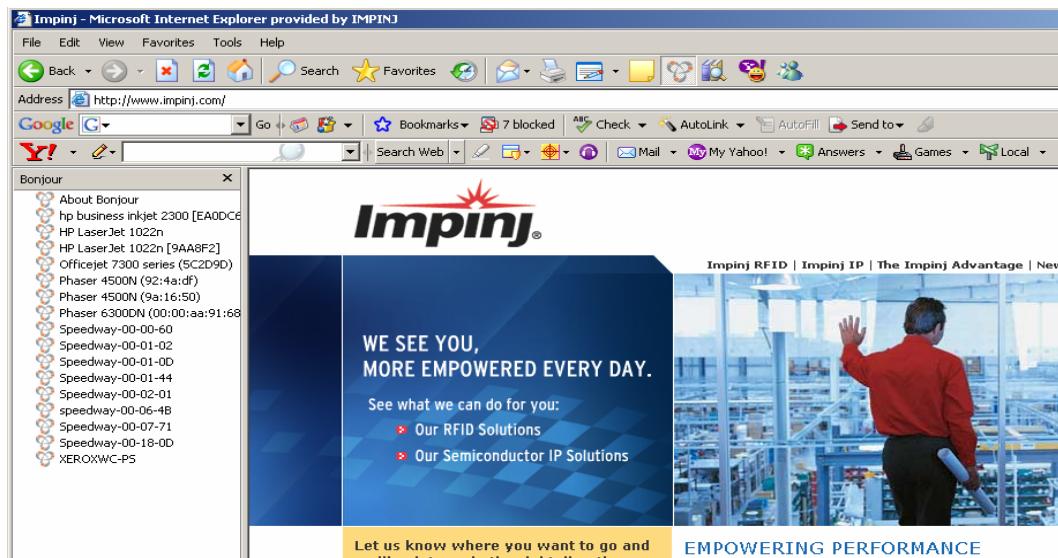


**Figure 3-3 Bonjour-enabled Browser**

**Important**    If using the Mozilla® Firefox® browser[1], the auto-discovery feature works in a different manner than it does for the Internet Explorer browser. For access using the Firefox browser, the URL must be entered into the browser window as:

**http://speedway-XX-XX-XX.local**

where the XX-XX-XX is the last three bytes of the desired unit's MAC address as described above. See the example in Figure 3-4.

If Bonjour does not work or may not be used on your network, see Section 3.2 and Section 3.3 for instructions on how to set an IP address on the device via the serial port.

---

1. Mozilla and Firefox are registered trademarks or trademarks of the Mozilla Foundation.

:
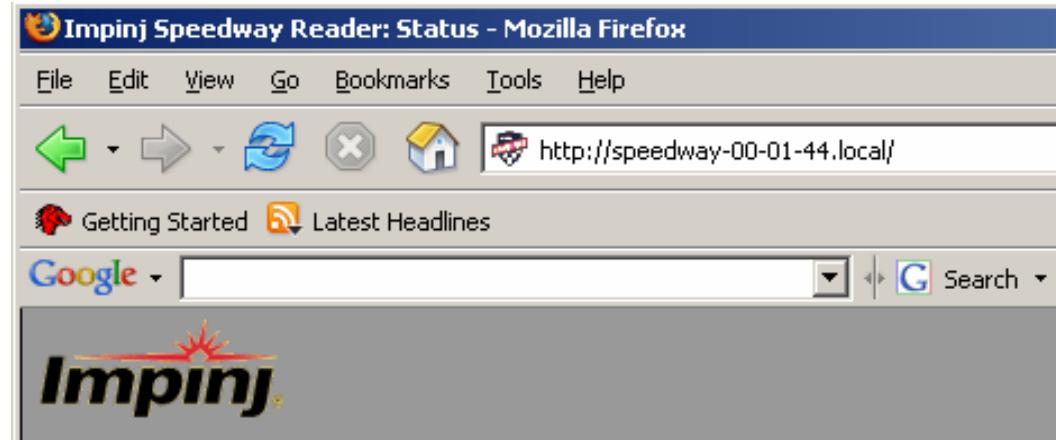


**Figure 3-4  Firefox Browser URL**

## 3.2 Preparing Serial Connectivity

Serial communication with the reader can be used  to configure the reader. The serial interface may be necessary to establish initial communications with the Speedway reader (via the command line interface) if your network equipment is not compatible with the default network configuration of the reader (DHCP). In this case, the reader's network connection can be configured using the serial port; Ethernet connectivity can then be used for control thereafter.

Launch HyperTerminal  (supplied with Microsoft Windows) or a similar communication program (such as Tera Term for Windows or Minicom for Linux) to establish serial reader communication.

After connecting the Speedway reader's serial port to the host PC's valid/active COM port, plug the reader's AC power unit into a suitable 100–240 VAC, 50–60 Hz power outlet. The Power LED will illuminate when power is applied. The reader will then begin its boot sequence. (Normal boot time for the reader's operating system is ~50 seconds. The reader will not accept commands until the boot sequence is complete, indicated by the Status indicator turning to a solid green, see Table 2-4).

Set the communication parameters of the terminal software per Figure 3-5 (Tera Term screenshot shown).

Once the terminal window opens, log onto the reader by entering the established user name and password. The default login (case-sensitive) is:

```
User Name: root
Password: impinj
```

The network may now be configured for the Speedway reader (see Section 3.3).
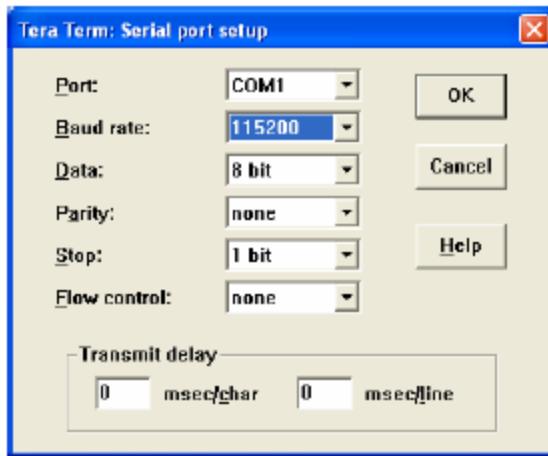
**Figure 3-5 Serial Port Configuration**

# 3.3 Manual Network Setup

After establishing serial connectivity and logging in (see Section 3.2), the network may be configured for the Speedway reader using the Rshell command line interface (see Section 8 for detailed information).

## 3.3.1 Essential Configuration Commands

Shown here are the essential configuration commands; for complete information on how to configure this interface, see Section 8.5.4 and Section 8.6.5.

To view the reader's current network configuration settings, enter the following command at the prompt:

> show network summary

The following is an example response from the reader (sample only; actual data may differ):

```
> show network summary
Status=0,'success'
ipAddressMode=dynamic
ipAddress=192.168.20.121
ipMask=255.255.255.0
gatewayAddress=192.168.20.1
broadcastAddress=192.168.20.255
hostname=speedway-00-41-0C
llaStatus=enabled
>
```

At this point, the TCP/IP configuration parameters, such as IP address (static or dynamic) and hostname, may be changed via the following command examples:

To set **hostname**, at the prompt, enter the command:

```
config network hostname <HOSTNAME>
```

To set **static IP address**, at the prompt, enter the command:

```
config network ip static <IP ADDRESS> <NETMASK> <GATEWAY>
<BROADCAST>
```

Alternatively, either of the following two versions of the **config network ip static** command may be used, in which case the reader will use default values for the unspecified parameters:

```
config network ip static <IP ADDRESS>
config network ip static <IP ADDRESS> <GATEWAY>
```

To set **DHCP**, at the prompt, enter the command:

```
config network ip dynamic
```

After achieving successful network configuration, you may connect to the network via the Speedway reader's Ethernet port.

### 3.3.2 Enabling Auto-Discovery

If auto-discovery does not work on your system, it's possible that the commands for enabling discovery on the reader have not been set. For complete auto-discovery command details, see Section 8.5.4.2 and Section 8.5.4.3.

## 3.4 SNMP Network Monitoring

Octane 3.0 supports SNMP, the standard interface for monitoring network-connected devices for status and error conditions. SNMP data is organized into Management Information Bases (MIBs). Each MIB, addressed by unique namespace, contains objects that can be monitored by a host. Each object has a universally unique Object Identifier or OID. Octane 3.0 supports the standard TCP/IP networking MIB (MIB-II) and the standard EPCglobal Reader Management MIB (RM).

Any standard network management system supporting SNMP v2c can query statistics and status data from a Speedway reader with Octane 3.0. Many enterprise systems also use SNMP for auto-discovery of SNMP capable devices on their networks.

MIB-II, defined by RFC 1213, is the standard set of objects defined to manage devices connected to TCP/IP networks. It includes information on TCP/IP interfaces and general system information.

EPCglobal Reader Management MIB defines a standard set of objects specific to RFID readers. These objects include items such as antenna state and RFID statistics. Octane 3.0 supports a subset of the RM MIB. It contains all the relevant RFID statistics, and system information, but does not contain statistics specific to the EPCglobal Reader Protocol (RP) as these statistics have been obsoleted by the EPCglobal LLRP (low level reader protocol) that Octane 3.0 supports.

For more information about SNMP, see the document defining Octane 3.0 SNMP, which is located at http://developer.impinj.com. (Access to this site is granted to all Speedway solution developers that have registered with the Impinj Support Portal http://rfid-support.impinj.com .) This document provides a summary for system architects to validate and understand the standard SNMP features supported by Octane 3.0 SNMP and any unique Octane SNMP behaviours that provide added capabilities. It provides detailed information to developers who are planning to support Impinj readers via SNMP.

For more information about configuring SNMP through the Web interface, see Section 5.3. For more information about configuring SNMP through the CLI, see Section 8.5.6.

# 4 Speedway Reader Web Interface—Status

Navigate to the Speedway reader's Status landing Web page (see Figure 4-1) by selecting the Status link from the navigation bar at the top left of the Web interface screen. This page of the Web interface provides network statistics and logging information through menu selections on the left side of the page.
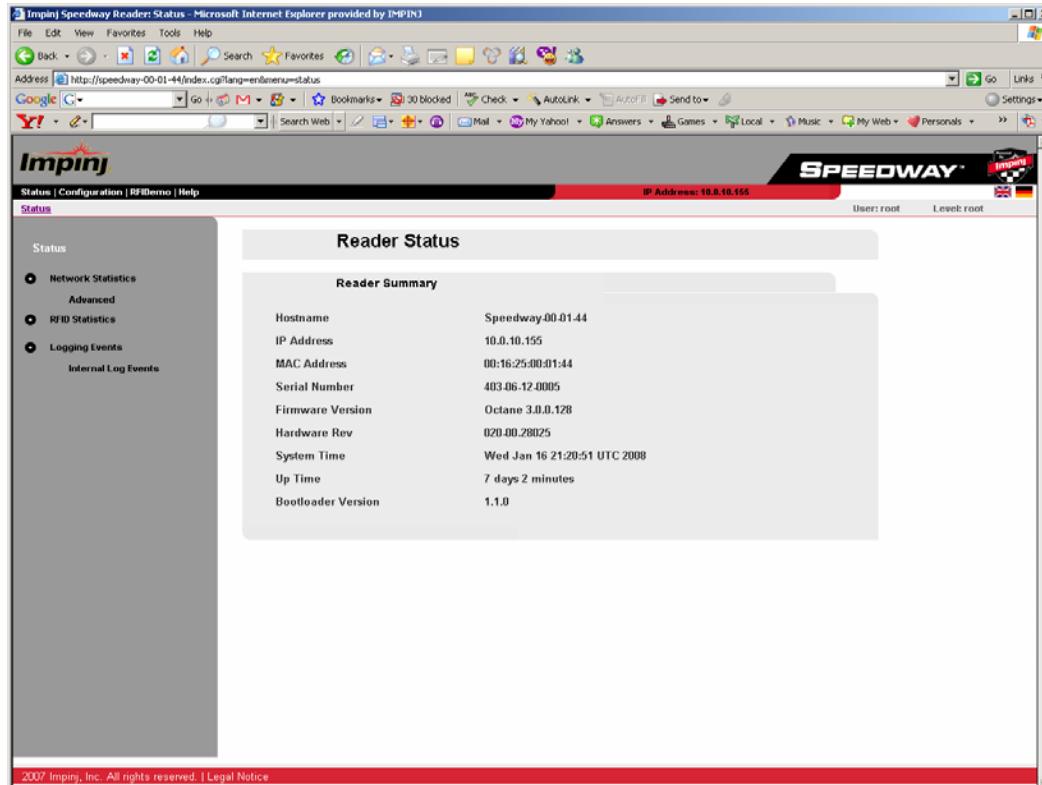


**Figure 4-1  Reader Status Landing Page**

## 4.1 Status Landing Page

The Status landing page contains summary information about the reader, both hardware and firmware:

- Hostname—statically set hostname or dynamically configured (set via DHCP) hostname

- IP address—current static IP address if configured statically. For DHCP, this field displays the currently assigned IP address.

- MAC address—hardware-specified MAC address assigned at time of manufacture

- Serial Number—reader serial number assigned at time of manufacture

- Firmware Version—firmware version currently running on the reader

- Hardware Revision—hardware version of the reader

- System time—currently configured system time of the reader

- Up time—amount of time the reader has been running since last reset

- Bootloader (BIOS) version—current version of the boot loader used to start the reader from reset

## 4.2 Network Statistics Status Page

Selecting the Network Statistics link under the Status menu will lead to a page that includes network statistics about the interface (see Figure 4-2):

- Interface—the name of the interface (ixp0)

- MTU—maximum unit transfer size

- Met—interface metric

- RX-OK—number of successfully received frames

- RX-ERR—number of received frames with errors

- RX-DRP—number of dropped received frames

- RX-OVR—number of receiver overruns

- TX-OK—number of successfully transmitted frames

- TX-ERR—number of transmitted frames with errors

- TX-DRP—number of dropped transmitted frames

- TX-OVR—number of transmitter overruns

- Flag—a string set to one of these values: B (broadcast address has been set), L  (this interface is a loopback device), M (all packets are received), O (ARP is turned off for this interface), P (this connection is point to point), R (interface is running), or U (interface is up).



**Figure 4-2 Network Statistics Page**

By selecting the Advanced link under the Network Statistics menu, much more detailed information may be displayed, including IP, TCP, UDP, and ICMP statistics. For complete descriptions of each parameter, see reference MIB-2 RFC 1213 (see Section 10).

# 4.3 RFID Status Page

Selecting "RFID Statistics" under the Status menu will bring up a window (see Figure 4-3) that displays the RFID statistics.
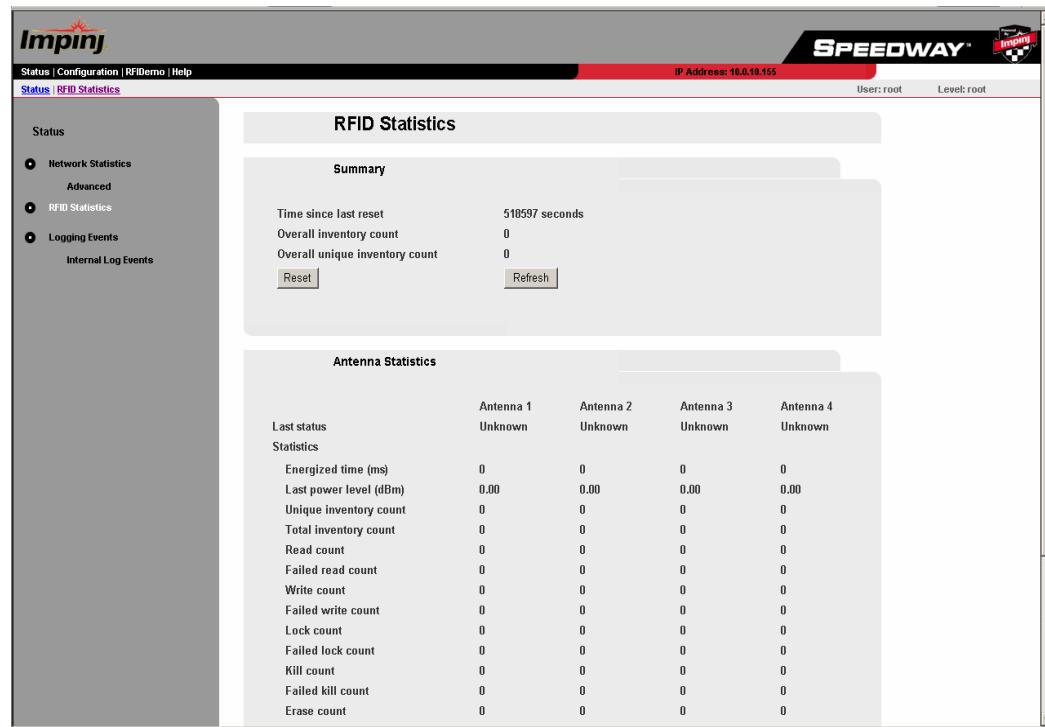


**Figure 4-3 RFID Statistics Page**

## Summary

This section presents a summary of the RFID statistics, including the time since the last reset of the statistics, the overall inventory count accumulated on all antennas, and the overall inventory of unique tags on all antennas.

Use the "Refresh" button to update all statistics or the "Reset" button to clear all statistics.

Note that the statistics counters are only cleared with the "Reset" button, so they will accumulate across multiple RFID connections. However, the unique tag history stored inside the reader is reset between connections. One unique tag may cause multiple increments to the counter if multiple connections have been established while the tag is visible.

## Antenna Statistics

This section provides a tabulation of RFID statistics, using one column for each antenna. The first two rows show the administrative and operational status of each antenna. Administrative status indicates whether the antenna is administratively set to be in use and the operational status indicates whether the reader is currently using it in its operation. The rest of the table lists the individual counters broken down by antenna.

### GPI Statistics

This section provides a tabulation of RFID statistics, using one column for each general purpose input (GPI) interface.

## 4.4 Logging Events Status Page

The Logging Events Status page (see Figure 4-4) provides a listing of all events logged into the local syslog file. This page also displays the current level setting of the syslog logging severity. The syslog  is stored in the local Flash memory file system, is the standard Unix logging system, and may be forwarded to a remote syslog server. If a remote syslog server is configured, the syslog events will be forwarded without storing a local copy so the events displayed in the Web interface screen no longer represent the most recently logged activities.

Under the Logging Events Status page, an Internal Log Events page lists all internal events. The internal log is only stored in the RAM file system, is capable of high-speed, real-time logging of internal events, and is routed to the syslog based on the severity level. See Section 8.5.3 for more details on how to configure the logging system.

The three buttons along the bottom of the screen allow the user to "Refresh" the screen to obtain the latest information, "Clear" the information (reset the logs), or "Download" the information to a file on a local machine. The "Clear" button is only available to users logged in at the levels of root or operator.
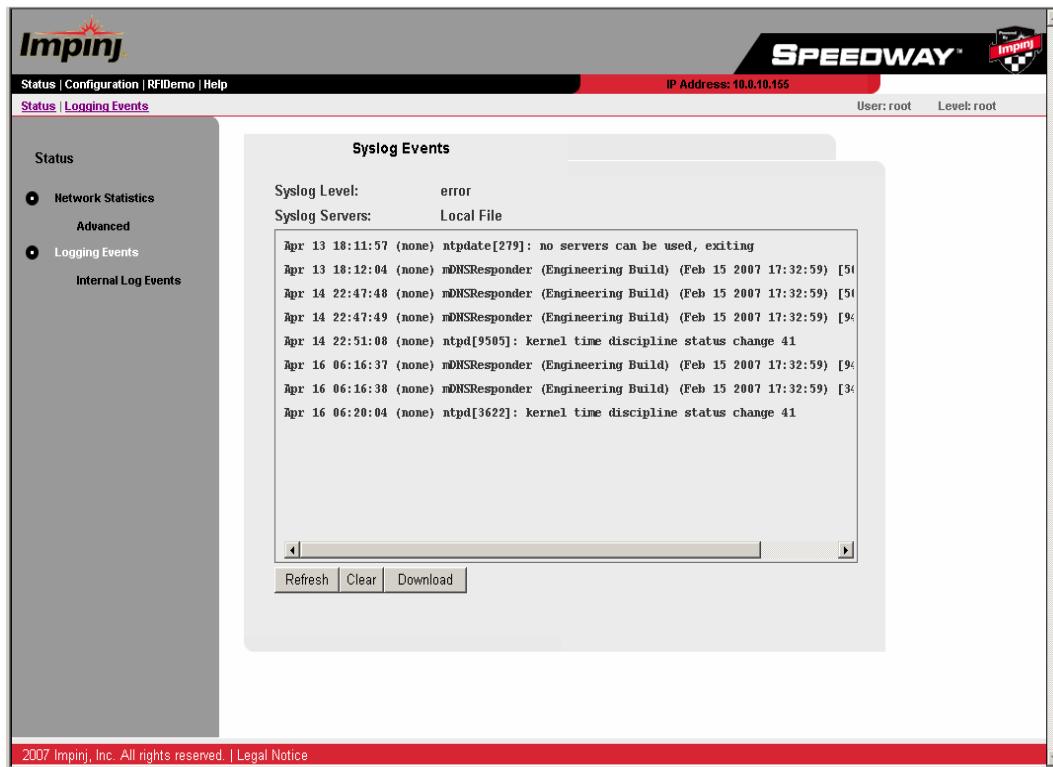


**Figure 4-4 Logging Events Page**

# 5 Speedway Reader Web Interface—Configuration

Navigate to the Speedway reader's hosted Web page (see Section 3.1 for instructions on how to access the reader from your network). From the navigation bar at the top left of the screen, select Configuration. A page similar to that shown in Figure 5-1 should appear. This initial landing page provides network summary and system information.

**Important**    Only a user logged in with either root or operator privilege may change settings via this Web interface. Those users logged in at the monitor level may not make any setting modifications. Also, when configuring the Speedway reader via the Web interface, the user should be aware that the status of radio buttons (checked or unchecked) and information in dialog boxes (if filled) reflect the current settings of those parameters.
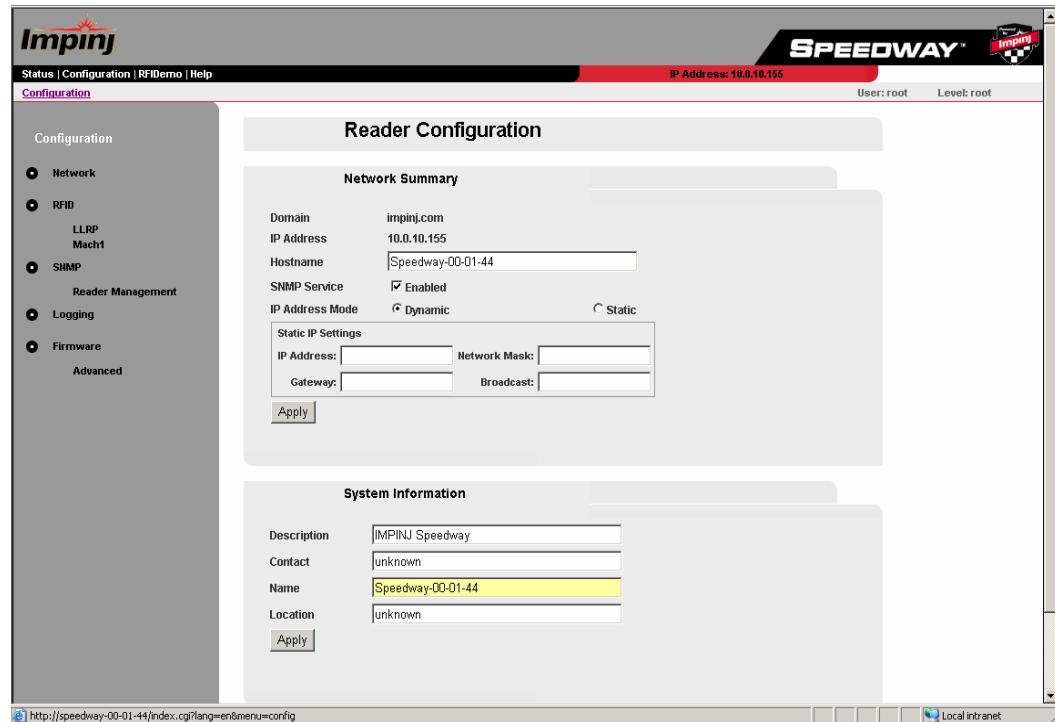


**Figure 5-1  Speedway Configuration Landing Page**

## Network Summary

The upper part of this page will display the defaults with which the system is configured during the auto-discovery process (and the button labeled Dynamic will be darkened). If the current IP address is static, the button labeled Static will be darkened and the static IP settings boxes will display the current settings.

If the user decides to configure the network for static address resolution (by selecting the button labeled Static), the four dialog boxes allow for entry of the IP Address, Gateway Address, Network Mask, and Broadcast Address.

Invalid parameters entered into the static address dialog boxes will not be accepted and a pop-up box will alert the user about the error.

### System Information

The Description, Contact, Name, and Location dialog boxes allow for entry of strings to further identify the reader.

**Note**    Quotes are not accepted as part of strings for System Information. Strings entered with quotes will be displayed with all quote marks stripped.

# 5.1 Network Configuration

Selecting Network from the menu along the left side of the screen (see Figure 5-1) will bring up a screen as illustrated in Figure 5-2. Note that this picture does not show the full selections possible (by scrolling down).
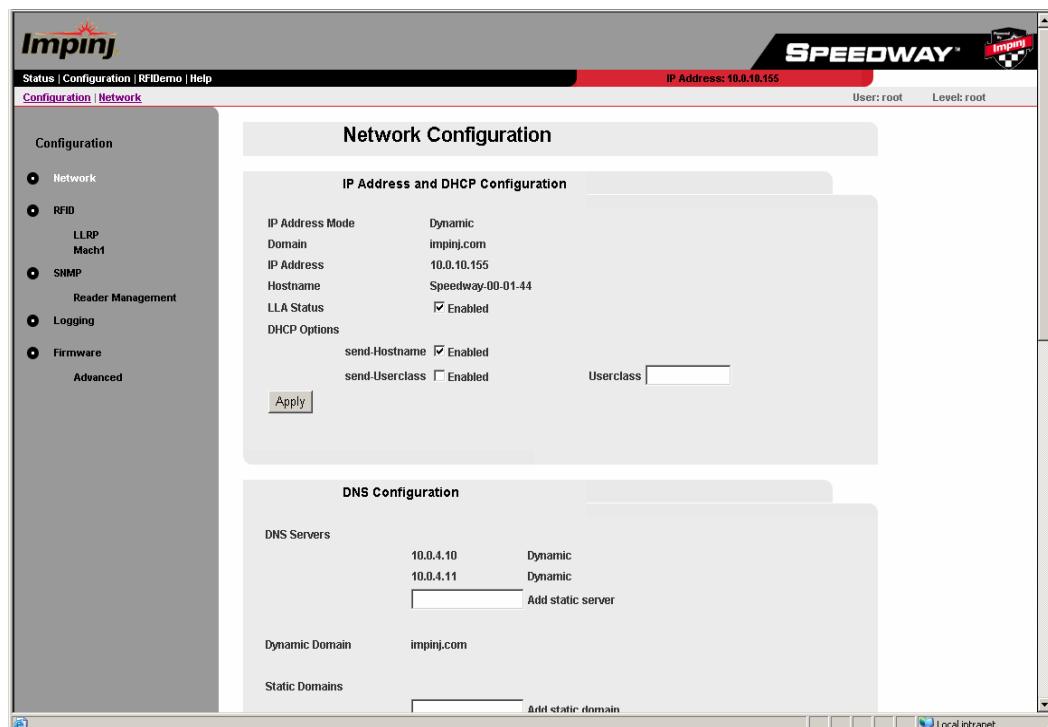


**Figure 5-2 Network Configuration Page**

### IP Address and DCHP Configuration

• Checking the box labeled "LLA Status" will enable the link-local address (LLA) feature. With LLA enabled, the reader will automatically choose an IP address in the link-local IP address range (169.254.XXX.XXX) when no dynamic IP address is available from a DHCP server. Link-local addressing is part of a feature set sometimes referred to as "zero-configuration networking" or simply "zeroconf."

• Checking the box labeled "send-Hostname" will enable the "send hostname" feature in the DHCP client configuration. This option causes the reader to send its hostname via option number 12 in the DHCP request and discover packets.

• Checking the "send-Userclass" box will set the value for the "send user-class" option of the DHCP client configuration to the string entered in the "Userclass" box. This action causes the reader to send the user-entered string as option 77 of the DHCP request and discover packets.

### DNS Configuration
- To add a static DNS server, enter an IP address into the box labeled "Add static server" and select "Apply."
- To add a static domain, enter a domain name into the box labeled "Static Domain" and select "Apply."

### NTP Configuration
- To add a static NTP server, enter an IP address or a hostname into the box labeled "Add static server" and select "Apply."
- Multiple NTP servers may be configured for time synchronization that is more reliable.

### Multicast DNS and DNS Service-Discovery Configuration
- Enable Multicast DNS (mDNS) by checking the box. Working in conjunction with the two service-discovery (SD) features listed below, this function allows the reader's HTTP (Web) service and RFID service (Impinj proprietary or LLRP) to be auto-discovered by other network devices that are mDNS and DNS-SD capable and reside on the same local network.
- Enable the HTTP service announcement by checking the box.
- Enable the RFID service announcement by checking the box. The RFID service type is _rfid._tcp. Impinj Multireader™ can be used to discover this service.

### Network Trace
Network trace allows a user to capture the network-level communications traffic and redirect the captured data to a different computer for monitoring. The source of the data to be captured can be either internal (the traffic between various processes inside the reader) or external (traffic into and out of the reader). The destination of the data can be a local file (on the computer where the Web browser is running) or a server where a listener process has been set up to accept the captured data. (The TCP port on the remote system must be configured with a TCP/IP listener waiting to accept and store the data, otherwise the connection will automatically terminate and the network trace will stop.) The format of the capture file is the "libcap" format, used by Ethereal®, Wireshark®, tcp-dump and numerous other network packet analyzers.[1] Also see section Section 8.5.4.6.

Referring to Figure 5-3, enable a network trace by:
- selecting the source (internal or external)
- selecting the destination (local file or server)
- entering a destination server address and a destination TCP port (if using a server as destination)
- selecting "Start."
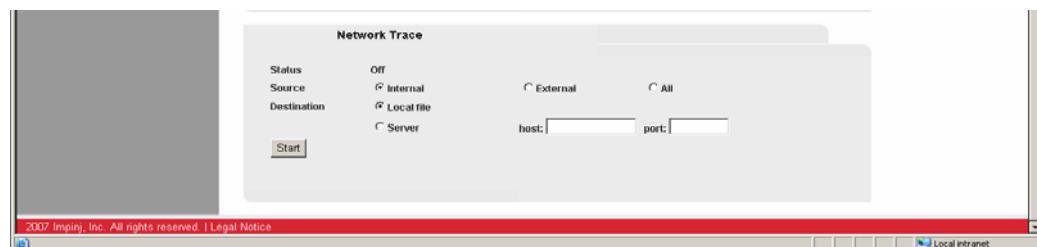


**Figure 5-3   Network Trace Configuration**

1. Ethereal is a registered trademark of Ethereal Inc. Wireshark is a registered trademark of Gerald Combs.

## 5.2 RFID Configuration

Selecting the RFID link under Configuration will bring up a window (see Figure 5-4) that displays a summary of the RFID application settings.
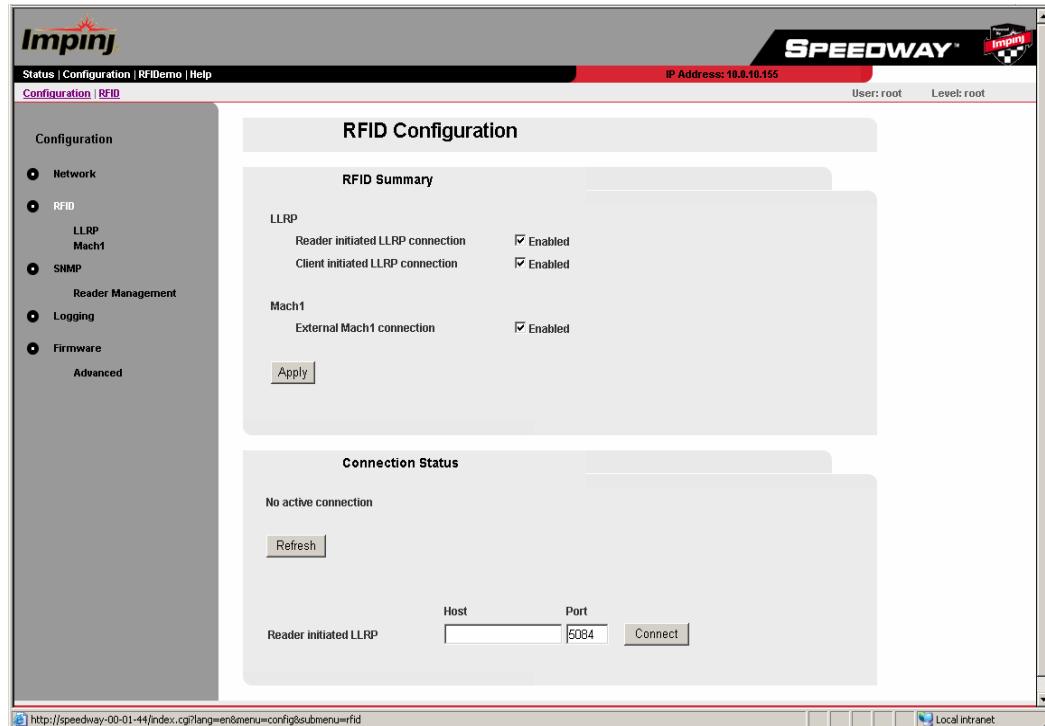


**Figure 5-4 RFID Configuration Page**

### RFID Summary

The administrative status of three types of RFID connections can be set through their respective checkboxes.

### Connection Status

This section consists of two parts:

The upper part of the screen displays the information of any active connection. This information includes:
• the peer information (i.e., host, port, and transport protocol)
• the connection type, either: Reader-initiated LLRP, Client-initiated LLRP, Internal Mach1, or External Mach1
• the time when the connection was established
Use the "Close" button to close the current connection. This button is only present when the connection type is not Internal Mach1. Use the "Refersh button to refresh the connection status.

The lower part of the screen provides an interface to make a reader-initiated LLRP connection. To make a connection, enter the hostname (or IP address), and the port number of the server with which to connect, and select the "Connect" button. Subsequently, display the connection status by selecting the "Refresh" button. Note that this action only creates a one-time connection, not permanently configured outgoing connections. For permanently configured connections, see the LLRP Configuration page.

## 5.2.1 Low Level Reader Protocol (LLRP) Configuration

Selecting "LLRP" under Configuration/RFID will bring up a page that provides an interface to display and set the LLRP configurations, as shown in Figure 5-5.
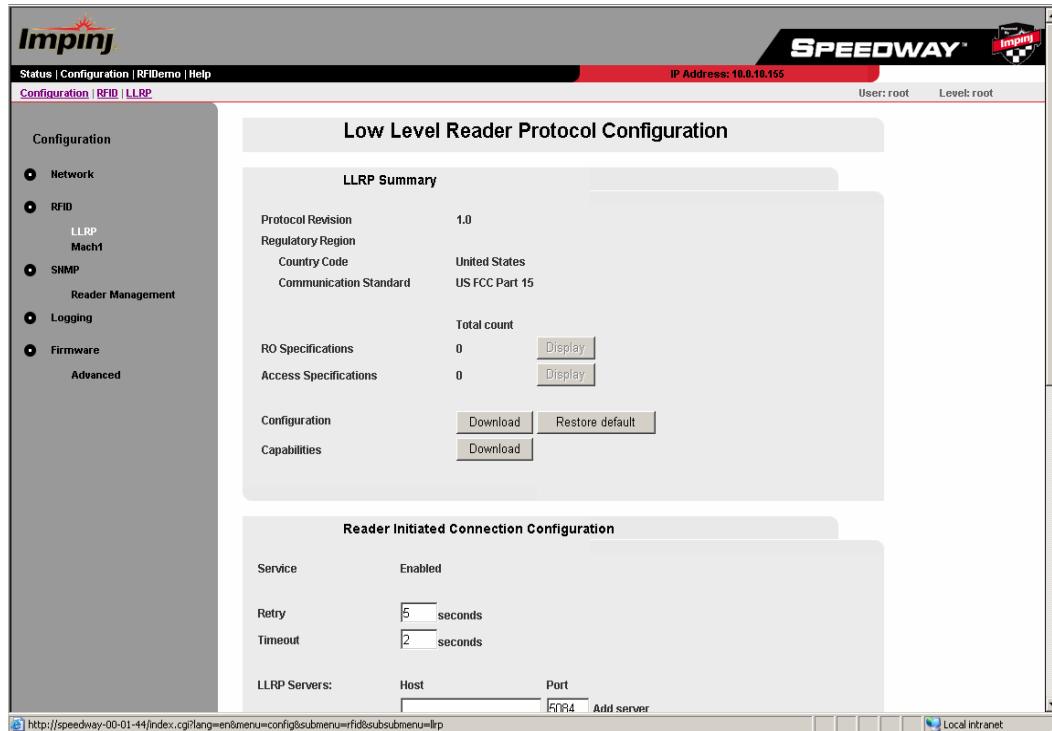


**Figure 5-5 Low Level Reader Protocol Configuration Page**

## LLRP Summary

This section displays the LLRP protocol revision implemented by the reader, and the regulatory region within which the reader operates. Also presented are the numbers of currently configured Reader Operation and Access Specifications in the LLRP connection.

View the details of the Reader Operation or Access Specifications in a pop-up window by selecting the "Display" button. (Ensure that the browser is configured to allow pop-up windows.)

Download the current configuration of the LLRP session as an XML file by selecting the "Download" button on the Configuration row; restore the default configuration for LLRP connections by selecting the button labeled "Restore default" when there is no active connection. See Appendix E for reader's default LLRP configuration.

To download LLRP capabilities as an XML file, select the "Download" button on the Capabilities row. When the capabilities are unavailable, the "Download" button text will be gray. The capabilities become available after an LLRP connection is established. See Appendix D for the reader's LLRP capabilities.

## Display Window for LLRP Reader Operation and Access Specification

This pop-up window displays the currently available Reader Operation or Access specifications and their states, indexed by their respective identifiers. For Reader Operation specifications, the state is "Disabled" or "Enabled." For Access specifications, the state is "Disabled," "Inactive," or

"Active." Select the specification(s) to be downloaded via the column of checkboxes, labeled "Select."
Download the selected specifications as one XML file via the "Download" button.

Use the "Refresh" button to obtain the latest information about the Reader Operation or Access specifications.

## Reader-initiated Connection Configuration

This section displays a reader-initiated LLRP connection configuration.

The administrative state of the connection is displayed on the "Service" row as either "Enabled" or "Disabled." The information of the currently active LLRP server, if any, is displayed under the heading "LLRP Servers." Only one server can be configured. The server is characterized by "Host" (hostname or IP address) and "Port" (the port number). Mark an LLRP server for deletion by selecting the "Delete" checkbox next to it.

## Client-initiated Connection Configuration

This section displays a client-initiated LLRP connection. Client-initiated connections are those initiated by applications wishing to connect to the reader.

The administrative state of the connection is displayed on the "Service" row as either "Enabled" or "Disabled." The dialog box labeled "TCP Listen Port" displays and permits changes to the port number on which the reader listens for incoming connections initiated by a client. The reader accepts incoming client-initiated connections only when the administrative state is "Enabled" and a current connection will be broken if the administrative state is changed to "Disabled." Changing the "TCP Listen Port" will not affect a current connection.

## 5.2.2 Mach1 Protocol Configuration

Selecting "Mach1" under Configuration/RFID will bring up a window (see Figure 5-6) that displays the Mach1 protocol configuration.
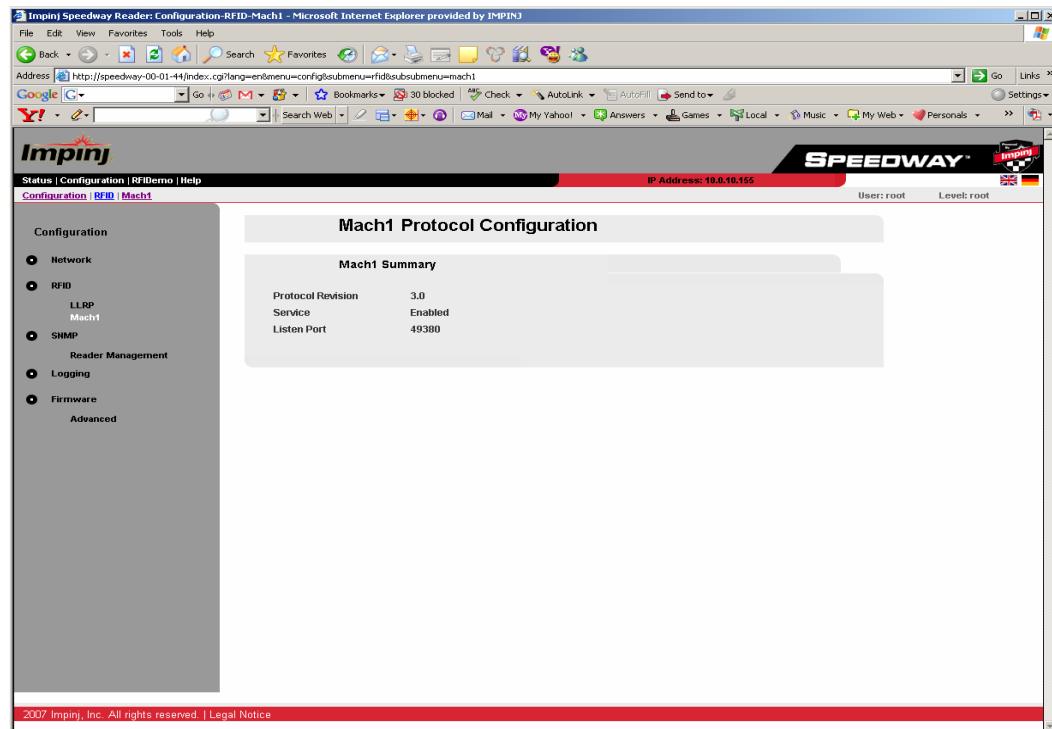


**Figure 5-6 Mach1 Protocol Configuration**

The summary of Mach1 protocol configuration includes:
• "Protocol Revision," which is the Mach1 protocol revision implemented by the reader.
• The administrative state of the connection, which is displayed on the "Service" row as either "Enabled" or "Disabled."

The reader accepts incoming Mach1 connections only when the administrative state is "Enabled" and a current connection will be broken if the administrative state is changed to "Disabled." Changing the "Listen Port" will not affect a current connection.

## 5.3 SNMP Configuration

Selecting the SNMP link under Configuration will bring up a window (see Figure 5-7) that allows each aspect of the SNMP feature to be set.
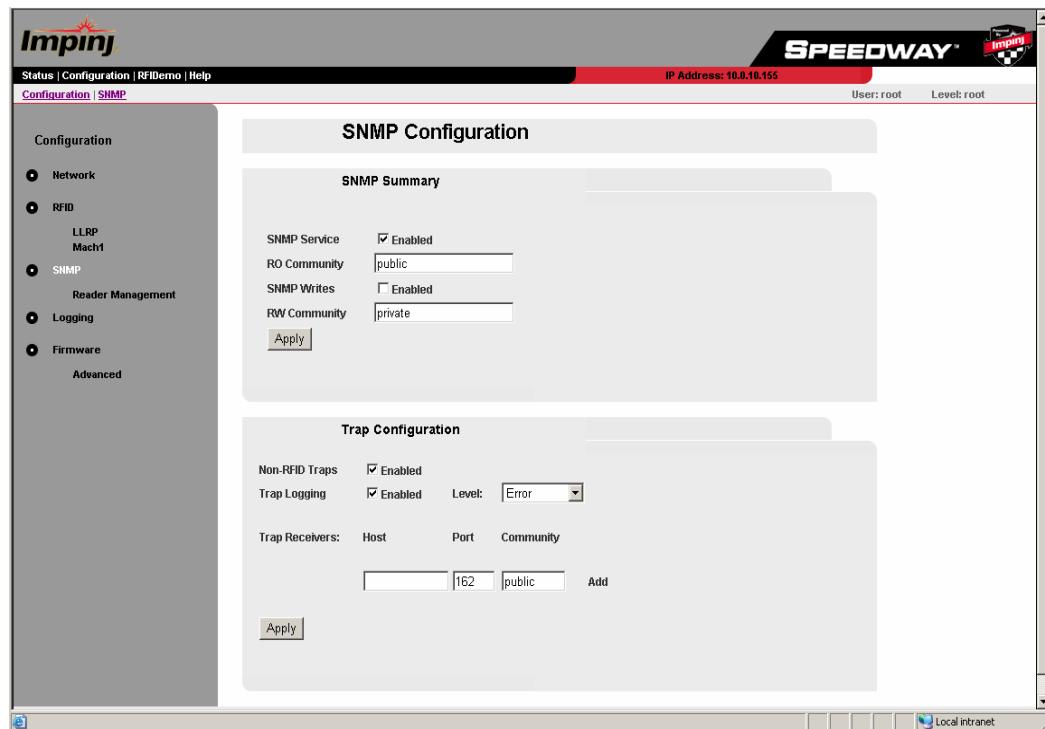


**Figure 5-7 SNMP Configuration Page**

## 5.3.1 General SNMP Configuration

The front page of the SNMP configuration menu provides interfaces for displaying and setting the generic SNMP configuration.

### SNMP Summary

- Use the checkbox labeled "SNMP Service" to globally enable or disable the SNMP feature. When SNMP is disabled, the reader will not respond to any SNMP requests, but all the SNMP configurations can still be set.
- The box labeled "RO Community" displays the current value and can take a new value of the Read-Only community string, which is used for reading SNMP objects on the reader.
- The boxed labeled "RW Community" displays the current value and can and take a new value of the Read-Write community string, which is used for reading and writing SNMP objects on the reader.
- The checkbox labeled "SNMP writes" can be used to globally enable or disable SNMP writes on MIB objects

### Trap Configuration

- Use the checkbox labeled "Non-RFID traps" to globally enable or disable the sending of Non-RFID traps.
- Use the checkbox labeled "Trap Logging" to globally enable or disable the local logging of all traps. Use the pulldown menu to select the severity level at which non-RFID traps are logged. Severity levels for logging of RFID traps are set on the "EPCglobal Reader Management Configuration" page. Only traps that are enabled are logged.

Information about the currently active trap receivers, if any, is displayed under the heading "Trap Receivers." Each trap receiver is characterized with "Host" (hostname or the IP address), the port number, and the community string for receiving traps.

• Mark a trap receiver for deletion by selecting the "Delete" checkbox next to it.
• To add a trap receiver, enter the host, port, and community information for the receiver into the respective dialog boxes on the row labeled "Add."

Select the "Apply" button to apply changes made in this section.

## 5.3.2 EPCglobal Reader Management (RM) Configuration

Selecting "Reader Management" under Configuration/SNMP will bring up a window (see Figure 5-8) that allows each aspect of the EPCglobal Reader Management MIB to be set.
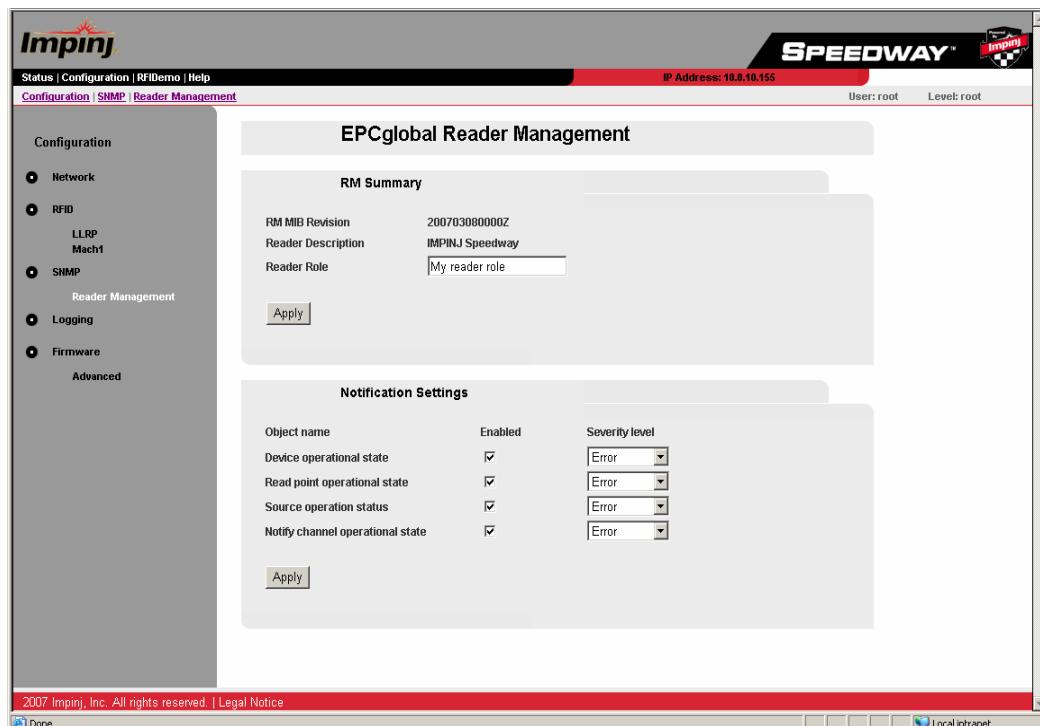


**Figure 5-8 EPCglobal Reader Management Page**

### RM Summary

A summary of the RM MIB is displayed in this section.

• "RM MIB Revision" is the revision of the Reader Management MIB implemented by the reader.
• "Reader Description" is the value of the RM epcgRdrDevDescription object and it takes the same value as the "Description" field of the System Information on the Configuration page.
• The box labeled "Reader Role" displays the current value and can take a new value for the epcgRdrDevRole object.

### Notification Settings

The section displays a table of RM MIB notifications supported by the reader.

• Use the checkboxes in the "Enabled" column to enable or disable the notification (trap).
• Use the pulldown option to select its severity level. The severity level is also used in the local logging of the notification.

## 5.4 Network Logging

Selecting the Logging link under Configuration will bring up a window (see Figure 5-9) that allows each aspect of the internal logging to be set (in increasing order of severity) via pulldown menus. (Debug is the least severe level and Emergency is the most severe.) The internal log is only stored in the RAM file system and is capable of high-speed, real-time logging of internal events.

The syslog setting may also be configured via this window. Only those items logged into the internal logs which are of equal or greater severity than the syslog level setting will be transferred to the syslog. See Figure 8-1 for a graphical representation of relative logging data transfers. The syslog is stored in the local Flash memory file system, is the standard Unix logging system, and is forwarded to a remote syslog server when an IP address or hostname is entered into the dialog box labeled "Add static server." Servers added here will persist over reboots.
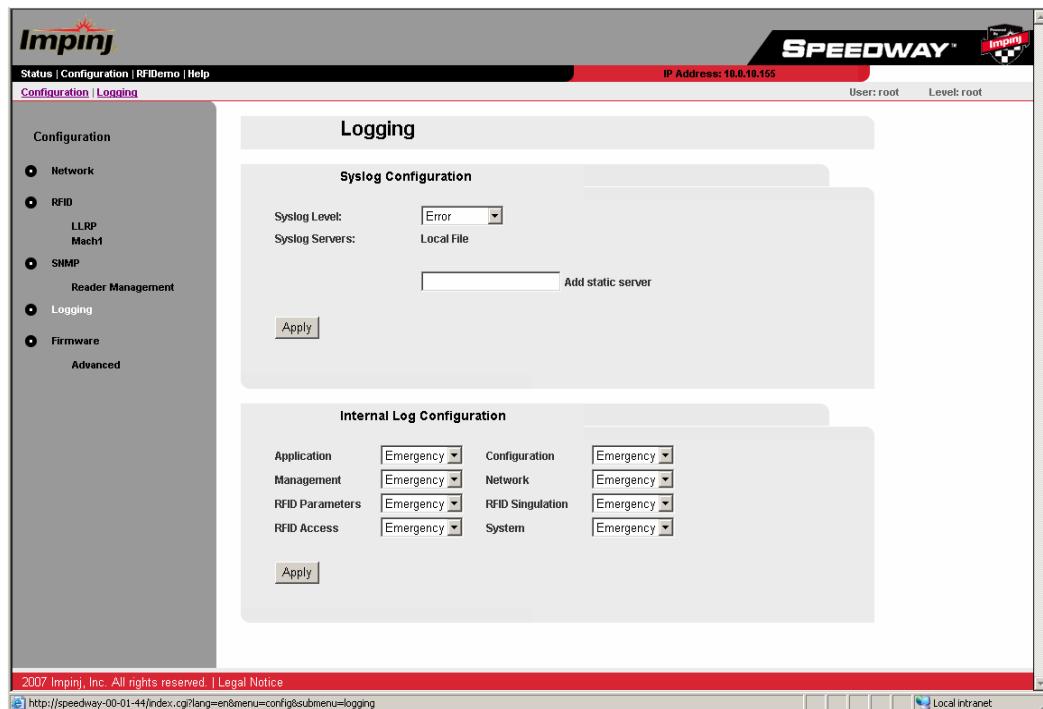


**Figure 5-9 Logging Configuration Page**

## 5.5 Firmware Upgrade

The reader firmware may be upgraded manually on one reader (push mode) or on multiple readers simultaneously (pull mode). See Section 7 for a complete description of the firmware upgrade process. The firmware upgrade page illustrated in Figure 5-10 provides a Web interface for the push mode method (allows the user to upgrade the reader currently being used).
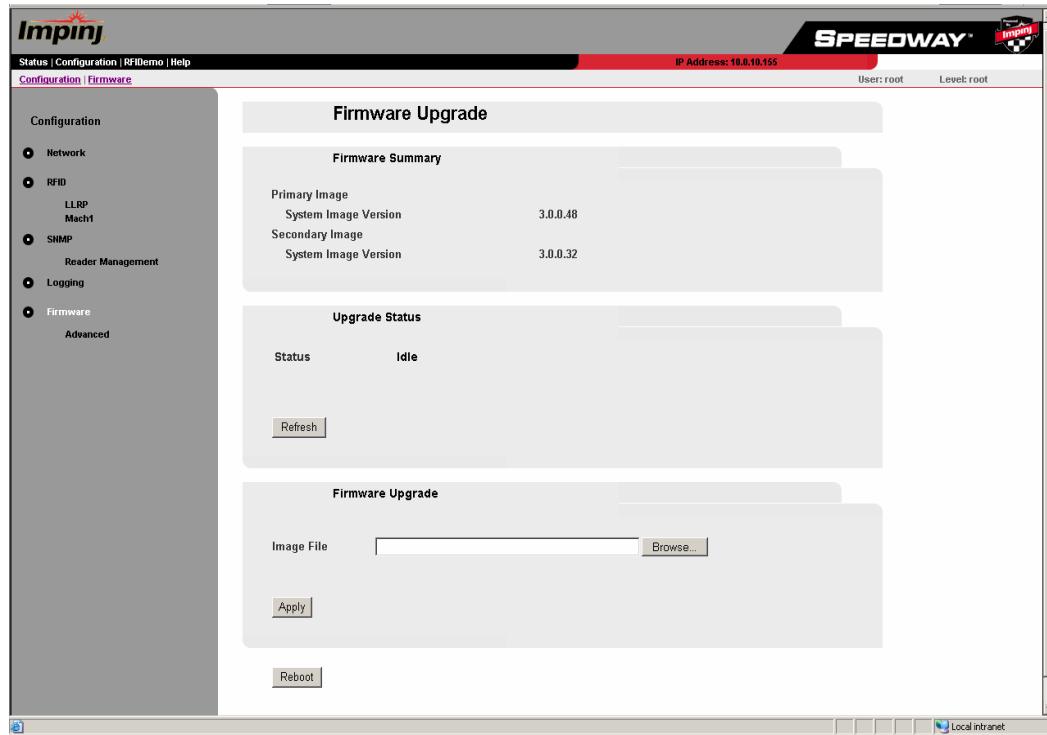
**Figure 5-10 Firmware Configuration Page**

## Firmware Summary

This section of the firmware upgrade Web page is a summary of the primary (currently running) and secondary (backup) system images (firmware versions). For details on the upgrade method, see Section 7).

## Upgrade Status

The Upgrade Status section of the Firmware Upgrade Web page displays the status of an upgrade. If no upgrade is in progress, the status will be "Idle." If an image file is entered into the Firmware Upgrade section and the button labeled "Apply" is selected, the status of the upgrade will be displayed.

The current status of the image upgrade (idle, contacting server, downloading, download failed, bad configuration, bad image, no upgrade, erasing, programming, done, or failed) will be refreshed every 30 seconds or when the "Refresh" button is selected.

In cases where the upgrade fails, the reason for the failure will be displayed below the status. For example, "Unknown Host" means the download failed due to an unknown host given in the metafile or image URI. See Section 8.6.3 for a complete description of all the firmware upgrade status information.

The upgraded firmware will not become the primary image until the reader is rebooted. After the upgrade is complete, a commit mode is displayed under the status to indicate how to activate the new firmware. The commit mode can be either a manual reboot or a reboot at a scheduled time.

**Firmware Upgrade**

Under the window labeled "Firmware Upgrade," the name of a network-accessible local upgrade image file may be entered or located by browsing through the local file system. This file is uploaded to the reader for upgrade by clicking the "Apply" button.

## 5.5.1 Advanced Firmware Upgrade

Selecting "Advanced" under Configuration | Firmware will bring up a window (see Figure 5-11) where upgrades using either the pull or push methods may be initiated. This screen also has the Firmware Summary and Upgrade Status information described in Section 5.5.
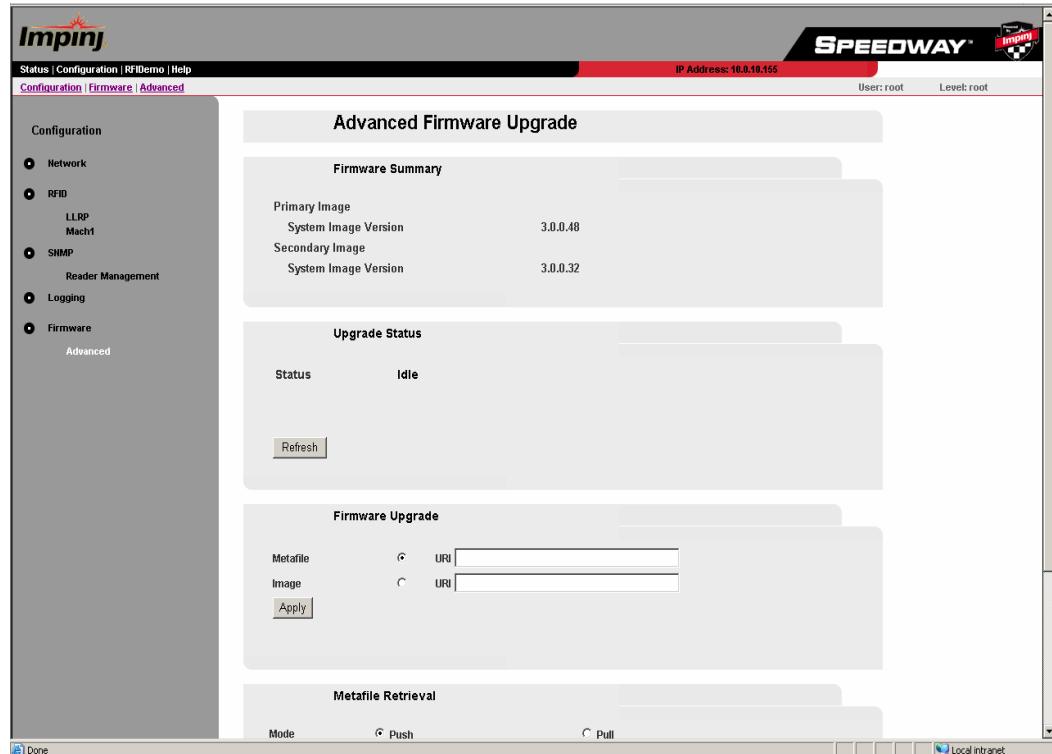


**Figure 5-11 Advanced Firmware Configuration Page**

**Advanced Firmware Upgrade**

For upgrades using the pull method, enter the URI of the metafile (see Section 7) that contains upgrade image information into the dialog box labeled "Metafile" and select the button labeled "Apply."

For upgrades using the push method, enter the URI of the upgrade image file into the dialog box labeled "Image" and select the button labeled "Apply."

**Metafile Retrieval**

The two radio buttons may be used to select between the manual "push" mode and the automated "pull" mode. For the "pull" mode, the retrieve period (time interval, in minutes, between automatic upgrade attempts) may be entered through the dialog box labeled "Period." See Section 7 for more details on the pull method.

## Reboot

The upgraded firmware image will not be activated unless the reboot command is issued by selecting the button labeled "Reboot" at the bottom of the page (see Figure 5-12).
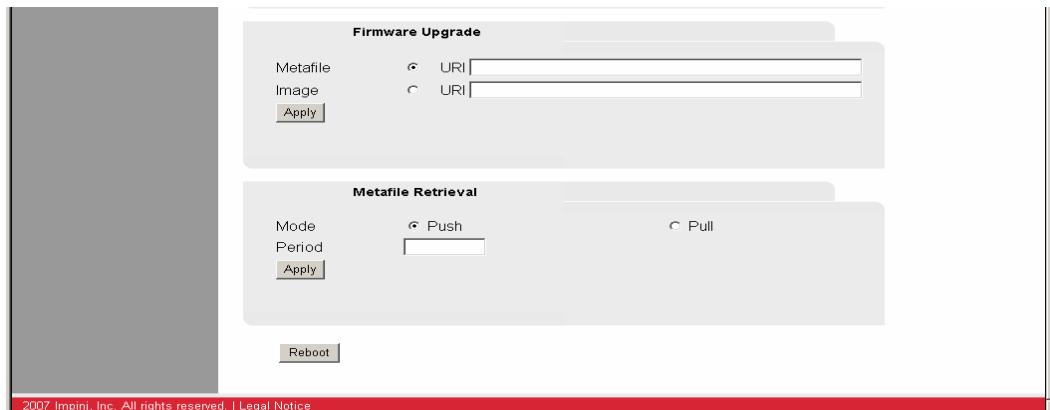
**Figure 5-12 Advanced Firmware Configuration Page (scrolled down)**

# 6 Speedway Reader Web Interface—RFIDemo

## 6.1 Settings

Navigate to the Speedway reader's RFID demonstration (RFIDemo) Web page. (Note that the actual Web interface appearance may vary from that shown in this User's Guide.)

**Important**    If the applet is opened, no other external software may connect to the reader via Mach1™ or LLRP Also, the RFID demonstration Web page does not expose all the control that is available via Impinj's Multireader™ control software, the Impinj Mach1™ interface, or the LLRP interface.

Clicking this tab will bring up a region selection page (see Figure 6-1).

The five user-selected fields on the Settings page include Mode, Antenna, Session, Transmit Power, and Channel, each of which are described below.
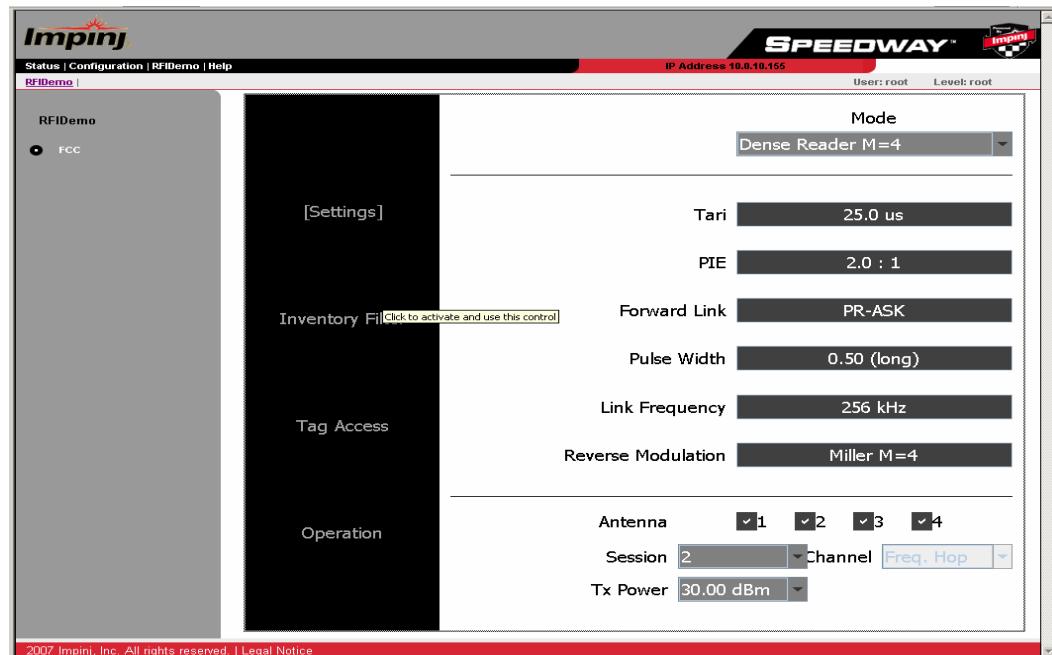


**Figure 6-1   Speedway Reader RFIDemo Landing Page**

### Mode

The reader mode is established via the Mode pull-down menu. Mode is a factory preset that configures the reader according to the respective default settings of that mode profile. For specific usage applications of the various modes, see Table 6-1.

**Table 6-1 Mode Usage**

| Mode | Mode Description | Usage |
|---|---|---|
| 0 | Maximum Throughput | Maximum read rate required<br>Population of readers is very low<br>Likelihood of interferers is very low |
| 1 | Hybrid | Fast read rate required<br>Modest number of likely interferers<br>Low likelihood of co-channel, adjacent-channel, or alternate-channel interferers |
| 2 | Dense reader M=4 | Intermediate read rate required<br>Population of readers is large<br>Likelihood of interference is high |
| 3 | Dense reader M=8 | Half the data rate of Mode 2<br>Extreme interference environments where tags are stationary or moving slowly |
| 4[1] | Max Miller | Maximum tag commissioning required<br>Population of readers is low<br>Likelihood of interference is low |

1. The fourth mode is only available for these regions: FCC, Taiwan, and Hong Kong

## Antenna

The Speedway reader supports four (4) independent, bidirectional, full duplex TX/RX ports. Each antenna port is labeled (ANT1−ANT4) on the Speedway unit and these designations correspond to the Antenna selection buttons that appear on the lower third of the screen. Only those antennas activated by clicking the appropriate button(s) will be operational. (See Figure 6-2.)



**Figure 6-2 Closeup of Variable Selections**

## Session

The reader may be assigned to one of four sessions (0−3), selectable via the Sessions pull-down menu. The Gen 2 standard specifies inventory flags that are stored by each tag to help the reader avoid redundant access to tags that have been recently read. Each tag has a flag that may be set to

"A" or "B." Any time a tag is read, this flag is switched from A to B, or B to A. The Gen 2 protocol further requires that B-flagged tags automatically revert (decay) to A-flagged tags after a period of time that depends on the Gen 2 session being used. The Gen 2 sessions and associated decay times are shown in Table 6-2.

**Table 6-2 Session Definitions**

| Session | A -> B Energized[1] | A -> B Not Energized | Application |
|---------|---------------------|----------------------|-------------|
| S0 | No Decay | Immediate Decay | **Characterization** of the read zone. Not intended for production inventory because of excessive redundant reads |
| S1 | 500 ms < t < 5s | 500 ms < t < 5s | Best for **Dynamic** Applications |
| S2 | No Decay | 2s < t | Best for **Static** Applications |
| S3 | No Decay | 2s < t | Same as Session 2 |

1. Receiving power from the reader

## Transmit Power

The reader power setting may be selected from the Tx Power pull-down menu. Depending on the hardware revision (see Section 2.1) and firmware version, readers may be set to transmit power in a range from 15 dBm up to 32.5 dBm (in .25 dB increments) measured at the RF antenna ports. However, because there are regional limitations on allowable conducted power, use of settings greater than 30 dBm must factor in antenna and cable configuration as further described in Section 2.6.

## Channel

North America: The FCC stipulates frequency hopping across the North American spectrum allocated to UHF RFID (902–928 MHz, with hopping occurring between 902.75–927.25 MHz in 500 KHz steps). As such, the Speedway reader does not allow the setting of a static frequency for North American operation and the Channel is factory-set and fixed to frequency hop. See Section 1.1.

Europe: A pulldown menu supports channel selection. See Section 1.2.

Taiwan: The NCC stipulates frequency hopping across the Taiwanese spectrum allocated to UHF RFID (922–928 MHz, with hopping occurring between 922.25–927.75 MHz in 500 KHz steps). See Section 1.4.

China: The Speedway reader complies with Chinese regulations and provides sixteen high-power channels in the 920.625–924.375 MHz frequency band. See Section 1.3.

# 6.2 Operation Screen—Monitoring Inventory Results

From the Operation page (see Figure 6-3), simply click the Start/Stop toggle button to begin reading tags within range of the reader. The Clear button clears the results of the inventory operation that commenced with Start.

Tags being read are displayed in white fields, which fade to blue after not being seen by the reader within the last ~10 seconds. To see all tags and their status, simply scroll the screen.

As tags are read, their EPC numbers appear in the primary window of the Operation screen. If the Read TID button on the Operation screen has been enabled, the logo of the tag silicon manufacturer corresponding to the TID will also be displayed.

In addition to the EPC and TID, the results displayed include:  Read Rate (expressed as tags/sec), Running Time (in hh:mm:ss from last Start), Total Tags (total number of tags read), and Total Active Tags (number of tags currently in the reader's field of view).

For more sophisticated inventory operations, the **Inventory Filter** and **Tag Access** pages allow the selection of tags according to user-specified criteria and rules. To access the Inventory Filter, Tag Access or protocol setup menus, any currently executing operation must be stopped.
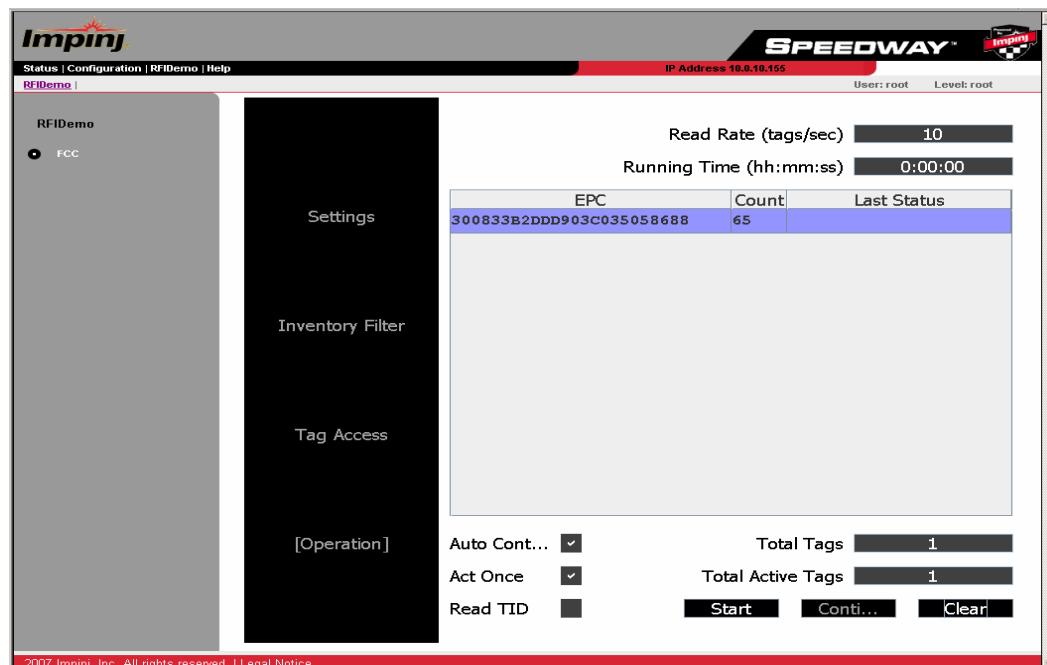


**Figure 6-3 Operation Screen**

# 6.3 Operation Screen—Filters

If the Inventory Filter has been activated (see Section 6.4), this status will be indicated in the Operation screen view (see Figure 6-4) with the text **Inventory Filter** appearing at the top of the screen. Likewise, if the Halt Filter has been activated (see Section 6.5), the text **Halt Filter** will appear.

## Auto Continue

Referring to the set buttons in the lower-left portion of the Operation screen, Auto Continue directs the reader to continue singulation after a halt condition has been met. Otherwise, if the Halt Filter has been set, the reader will stop reading and return control to the user, resuming operation only when the Continue button has been clicked by the user. Note also that Halt does not require any subsequent action.

**Act Once**

The Act Once button, if enabled, directs the reader to execute the action indicated in the Tag Access Action setting (read, write, lock, kill, etc.) only one time (see Section 6.5). If the operation is successful (see 'Last Status' column in the primary read window), the reader will continue the inventory or halt operation, depending on the status of the Auto Continue setting. If the Act Once setting is not enabled, and the action indicated is a write, the reader will write the tag over and over in a continuous loop. If both Act Once and Auto Continue are enabled, the reader will write the tag once and then continue the inventory operation, responding in accordance with the Inventory Filter settings that have been established.

To change settings from Operation mode:

1.  Stop continuous singulation using the Start/Stop button.

2.  Configure the reader to the desired new mode using the Settings, Inventory Filter and Tag Access pages.

3.  Return to the Operation page and re-start continuous singulation.
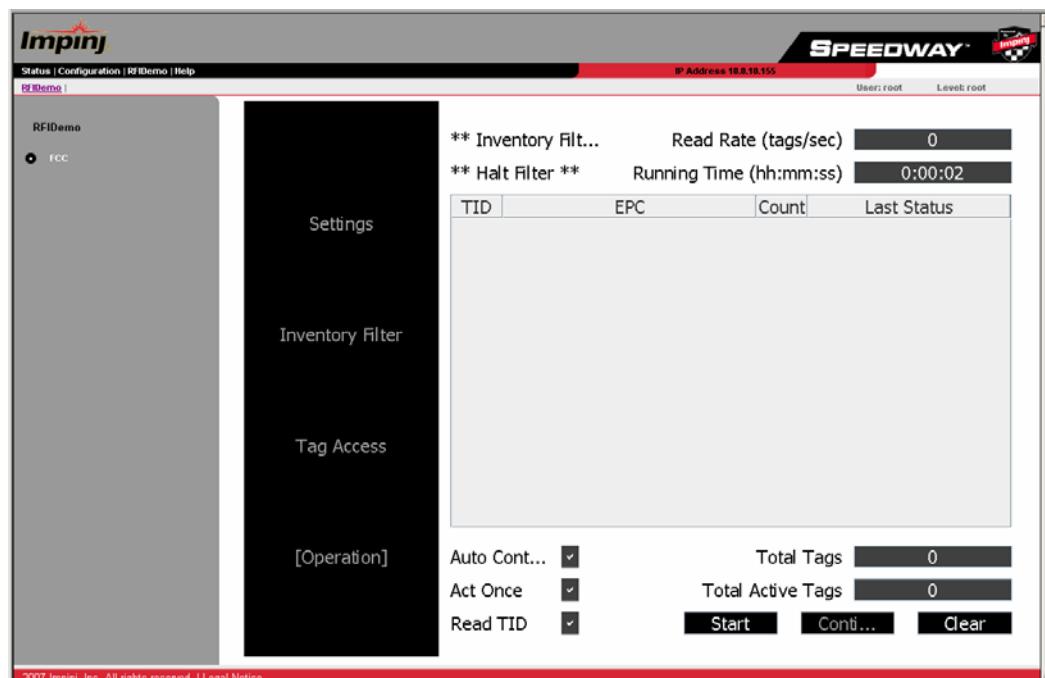


**Figure 6-4 Operation Screen with Filters Enabled**

# 6.4 Inventory Filter Screen

The **Inventory Filter** screen (see Figure 6-5) is the user interface to the Select command, which the reader may apply successively to a particular tag population based on user-defined criteria that may include union, intersection, and negation-based tag partitioning (union and intersection operations are performed by issuing successive Select commands).

Select commands apply to a single memory bank; the Mem Bank field specifies if the criteria applies to the TID, EPC, or User memory of the tag (see Section 6.5), as follows:

Mem Bank 00 (0): Reserved (cannot select filter on this bank)
Mem Bank 01 (1): EPC
Mem Bank 10 (2): TID
Mem Bank 11 (3): User

Successive Selects may apply to different memory banks. The Bit Offset and Bit Length fields are used to target a specific portion of the tag memory on which to perform the filtering, while the Pattern field contains the comparison bits of interest. Note that the Bit Length must be non-zero. As tags are read, the Pattern is evaluated against the Select criteria, which includes Equal and Not Equal options in the Comparison field.

The Inventory Filter allows the use of two sets of criteria (defined by primary filter A and secondary filter B) that may be used separately, jointly, or not at all (the pull-down options include No Filter, A ONLY, A AND B, A OR B). When applied to an inventory round, only those tags that match the Select criteria will be displayed.
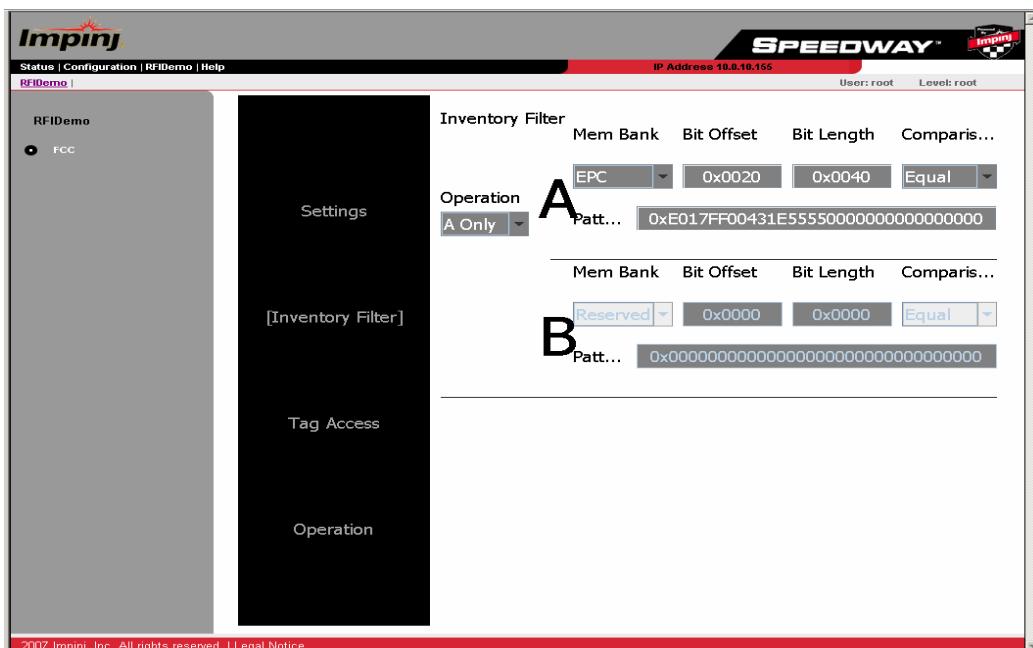


**Figure 6-5  Inventory Filter**

In Figure 6-5, the Pattern written is "0xE017FF00431E55550000000000000000, the bit offset is "0x0020," and the bit length is "0x0040." The bit offset for an EPC code must be nonzero because the first 32 bits in the memory map (see Figure 6-6) are taken up by the CRC and PC codes. Figure 6-7 provides an example of how this pattern would be stored into the tag memory.

| | | MSB | | LSB | |
|---|---|---|---|---|---|
| | | | ⋮ | | |
| 10ₕ | | | TID [15:0] | | 1Fₕ |
| 00ₕ | | | TID [31:16] | | 0Fₕ |

| **Bank 11** | **USER** |
|---|---|
| **Bank 10** | **TID** |
| **Bank 01** | **EPC** |
| **Bank 00** | **RESERVED** |

| | MSB | | LSB | |
|---|---|---|---|---|
| | | EPC [15:0] | | |
| | | ⋮ | | |
| 20ₕ | | EPC [N:N-15] | | 2Fₕ |
| 10ₕ | | PC [15:0] | | 1Fₕ |
| 00ₕ | | CRC-16 [15:0] | | 0Fₕ |

| | MSB | | LSB | |
|---|---|---|---|---|
| | | ⋮ | | |
| 30ₕ | | Access Passwd [15:0] | | 3Fₕ |
| 20ₕ | | Access Passwd [31:16] | | 2Fₕ |
| 10ₕ | | Kill Passwd [15:0] | | 1Fₕ |
| 00ₕ | | Kill Passwd [31:16] | | 0Fₕ |

**Figure 6-6 Tag Memory Map**

| **Bank 11** | **USER** |
|---|---|
| **Bank 10** | **TID** |
| **Bank 01** | **EPC** |
| **Bank 00** | **RESERVED** |

| | MSB | | LSB | |
|---|---|---|---|---|
| 70ₕ | | XXXX | | 7Fₕ |
| 60ₕ | | XXXX | | 6Fₕ |
| 50ₕ | | 5555 | | 5Fₕ |
| 40ₕ | | 431E | | 4Fₕ |
| 30ₕ | | FF00 | | 3Fₕ |
| 20ₕ | | E017 | | 2Fₕ |
| 10ₕ | | PC [15:0] | | 1Fₕ |
| 00ₕ | | CRC-16 [15:0] | | 0Fₕ |

**Figure 6-7 Writing EPC Example**

# 6.5 Tag Access Screen

After acknowledging a tag, the Speedway reader may be commanded to access it. Under the **Tag Access** menu, a pull down menu provides five command Actions: Read, Write, BlockWrite, Lock, and Kill.

The menu item Tag Access (see Figure 6-8) adds a Mask field to the filtering operation, which allows the user to mask individual "don't care" bits or segments of the matching pattern, where "1" identifies a bit of interest and "0" represents a masked bit.

Tag Access differs from the Inventory Filter operations in several respects. First, rather than performing a continuous inventory of a tag population, Tag Access allows the user to automatically halt the inventory process upon finding a tag of interest (e.g., a tag that meets the Halt Filter criteria). At this point, the tag can be automatically read, written, locked, or killed, according to the action selected in the Action pull-down menu. Note that the Halt criteria memory bank is independent of the write memory bank. For example, in Figure 6-8, the halt criteria is based on the EPC but the write action will happen on the TID.

The action is applied only to the selected Mem Bank and within it, the desired memory rows (00–07), the rows being made up of 16-bit words. If Action calls for a write, the specific bit pattern to be written must be entered (in hex format) in the corresponding field(s) below the selected row number(s). Multiple selected rows must be contiguous. For example, if only data in rows 1 and 3 must be changed, the data for row 2 must still be entered. The row number will change color to orange to indicate the valid rows for each memory bank. In the example of Figure 6-8, the TID only encompasses two sixteen bit rows so only rows 0 and 1 change color to orange to indicate valid selections. For the EPC, row 0 may not be overwritten (this is the CRC field, see Figure 6-6).

For Tag Access, the comparison criteria supports Greater Than and Less Than in addition to the Equal and Not Equal options available in the Inventory Filter page.

The Tag Access view is consistent with the Operation view (described in Section 6.2 and Section 6.3) in that settings input into one screen are valid for the other.
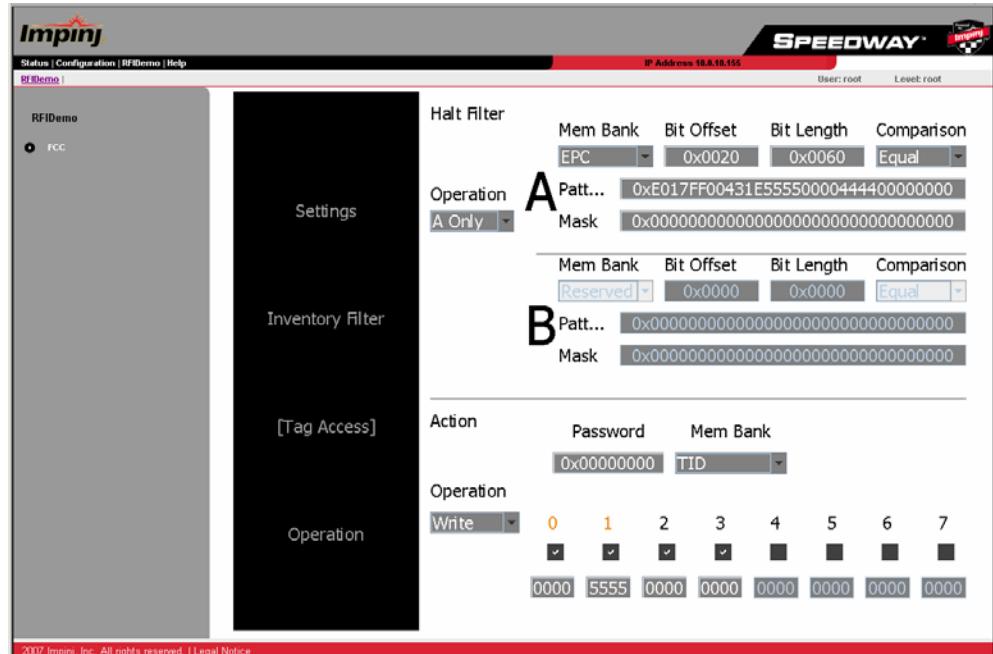


**Figure 6-8 Tag Access**

# 7 Firmware Upgrade

The Speedway reader provides methods for managing the firmware image that include:

- Upgrade to a new image

- Fallback to a previous valid image

- Restore to factory default settings

These operations can be performed without disturbing the current operation of the reader. The user may manage the upgrade process through the steps described in this section. The upgrade may be performed via the command line interface or via the Web interface Configuration Menu tab (see Section 5.5).

Terms and Acronyms
- Client: the user program that uses the upgrade management service

- Primary image: the image that is currently running

- Secondary image: the image that is not running and may be the target of upgrading or fallback

- Upgrade configuration: the information for determining the upgrading procedure

- Upgrade Image File: file that contains the Speedway reader image used for upgrade—stored on a file server and retrieved by the Speedway reader

- Metafile: data file that resides on a file server and contains the Upgrade Configuration information

- Metafile-URI: Universal Resource Identifier of the metafile

- URI: Universal Resource Identifier as defined in RFC3986

## Dual Image Model

The flash layout can be viewed as consisting of primary and secondary images, each of which contains three partitions, as shown in Figure 7-1. The primary image is the image that the reader is currently running and the secondary image is used for upgrade to a new image or fallback to a previous image.

| | Partition 0 | Partition 1 | Partition 2 |
|---|---|---|---|
| **Primary image** | **System OS Partition** | **System Configuration Partition** | **Custom Application Partition** |
| **Secondary image** | **System OS Partition** | **System Configuration Partition** | **Custom Application Partition** |
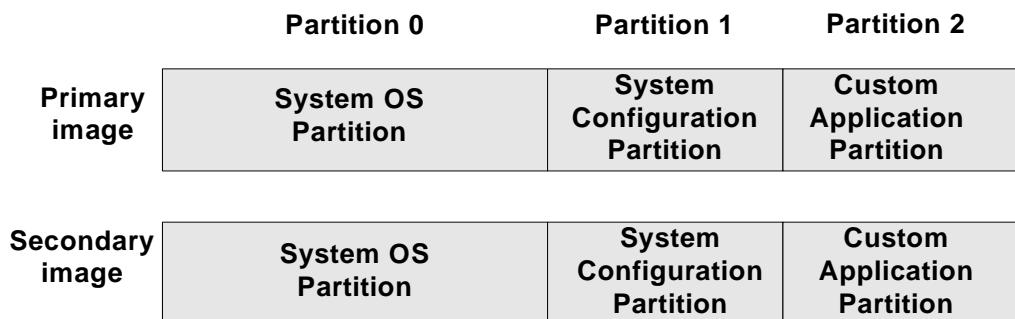
**Figure 7-1  Dual Image Model**

The three partitions in each image are:

- Partition 0, the System OS Partition (SOP). This partition contains the Linux OS image, file system, and Impinj reader application.

- Partition 1, the System Configuration Partition (SCP). This partition contains the Impinj reader application configuration and other general configuration data.

- Partition 2, the Custom Application Partition (CAP). This partition may contain a custom application.

Partitions 0 and 2 can be individually upgraded, while Partition 1 can be upgraded only when Partition 0 is upgraded.

Upgrade is performed in the background, so that the current operation of the reader is not disturbed until the activation of the new image. The time of activation is also controlled by the user.

## Image Versioning Scheme

Each partition has a four-part version number associated with it. In the upgrade configuration file (see Section 7.3), the version number is represented by a string consisting of four fields separated by '.' (dot):

ddd.ddd.ddd.ddd

where each field is a decimal number ranging from 0 to 255. The left-most field is the most significant part of the version number with sub-versions provided to the right. For the purpose of upgrades, when two version numbers are compared, the one with the largest leftmost number is considered a higher version and therefore a newer image. For example, if two versions being compared are 2.3.4.9 and 2.4.4.1, then 2.4.4.1 is considered newer because the second number from the left is larger (in this case 4 versus 3). Other than this comparison, the upgrade mechanism assumes no additional meaning for the version string.

# 7.1 Upgrade Methods

Speedway provides two methods to support firmware upgrade: push and pull. Push mode is a manual technique to perform an upgrade on an individual reader. Pull mode is an upgrade method that allows simultaneous upgrade of multiple readers through a single Upgrade Configuration file called a metafile. The default configuration of the reader is "push" mode.

In push mode, the user can trigger a one-time upgrade of the Speedway image. When triggering the upgrade, the user must specify the location of the Upgrade Image File as a URI. The upgrade will be performed if any of the partitions within the new image are different than those contained in the primary image. Once the download and programming have completed, the reader will remain in push mode and will perform no further upgrades until a new client request is issued. In push mode, the reader will not reboot automatically to activate the new image. The user must issue a reboot command (see Section 8.4) to complete the activation.

In pull mode, the user creates a custom Upgrade Configuration Metafile (or metafile for short). This metafile is stored on a remote server. The user configures the location of the metafile as a URI. The reader downloads the data contained in the metafile at periodic intervals (called the retrieve period) and uses that data to make automatic upgrade decisions. The reader remembers the retrieve mode, retrieve period, and URI across power-cycles so that it can resume the pull method after a system reboot. Typically, when the reader retrieves the metafile at a scheduled time (or when it

reboots), it will find that no upgrade is needed because in the absence of any change in the metafile on the server, the image version the reader is running is the same as that specified in the metafile.

## 7.2 Preparing the Upgrade Image

The path and permission of the image file on the server should be set properly to allow file retrieval via the method as specified by the **upgrade-file-uri** field of the metafile or by the image URI.

## 7.3 The Upgrade Configuration Metafile

The Upgrade Configuration metafile is at the core of the pull upgrade mechanism. The user prepares this file based on upgrade requirements and saves it on a file server accessible from the reader. The file contains instructions to the Speedway reader as to how to perform the upgrade as a list of text-based entries. Each data entry consists of a single line data field and may be qualified with one or more parameters separated with a semi-colon. Table 7-1 lists the data entries in the metafile. All data fields and parameters are mandatory unless marked as optional. The format of a data entry is as follows:

```
field-name:field-value{;parameter-name=parameter-value} <EOL>
```

**Important**    The metafile must not contain any Unicode characters.

### Table 7-1 Upgrade Configuration Definition

| Field Name | Field Value | Argument | Parameter Value | Description |
|---|---|---|---|---|
| retrieve-mode | This field indicates how the metafile is to be retrieved. | | | |
| | push | This field tells the reader to wait to be given upgrade information directly | | |
| | pull | retrieve-period | <int> | This field tells the reader to periodically retrieve the metafile. The mandatory parameter specifies how often (in minutes) the reader downloads the metafile |
| upgrade-mode | This field indicates how the reader determines the need for upgrade. | | | |
| | auto | The reader determines if an upgrade is necessary based on its knowledge of the local image version compared to the upgrade file. Upgrade is needed if the local image has at least one partition that has a lower version than the corresponding partition in the upgrade image file. | | |
| | forced | The reader should upgrade as long as the current image has at least one partition that has a different version from the corresponding partition in the upgrade image file. | | |

**Table 7-1 Upgrade Configuration Definition (continued)**

| Field Name | Field Value | Argument | Parameter Value | Description |
|---|---|---|---|---|
| commit-mode | | | | This field indicates how the image should be activated. |
| | immediate | | | The image should be activated immediately after the upgrade is complete, causing an immediate reboot after programming is complete. |
| | wait-4-cmd | | | The image should be activated by a reboot command from the user. |
| | | | | The following parameters are used where either time or wctime has to be present and early-act-ok is optional. All parameters when present must be given in the order presented here. |
| | scheduled | time | <string> | Reboot is scheduled at the time indicated by the mandatory parameter **time**. The value of time is a string that takes either the fully specified format "<time-zone>.yyyy:mm:dd:hh:mm:ss," or the wildcard format: "<time-zone>.*.hh:mm:ss+r<max-delay>"<br><br>where <time-zone> is utc, and <max-delay> is the maximum value of a random delay. When wildcard time is used, the reboot time is the upcoming hh:mm:ss AFTER the upgrade is completed, plus a delay of random length, up to max-delay, after the hh:mm:ss.  The format of max-delay is "<number>m" or "<number>s," to indicate the max delay number in minutes or seconds.<br>See Section 7.9.6 for a detailed explanation of reboot time. |
| | | wctime | <string> | Reboot is scheduled at the "wildcard" time indicated by the mandatory parameter wctime. The value of wctime is a string that takes the wildcard format "<time-zone>.*.hh:mm:ss+<r<max-delay>" as explained above. |
| | | early-act-ok (optional) | {no, yes} | It's OK to activate the upgraded image before its scheduled activation time because of an early reboot. Default value is no when this parameter is absent. |
| dl-retries | <int> | | | Number of times to retry if download fails because of timeout |

**Table 7-1 Upgrade Configuration Definition (continued)**

| Field Name | Field Value | Argument | Parameter Value | Description |
|---|---|---|---|---|
| dl-retry-period | <int> | | | Time to wait (seconds) before retrying a download. |
| upgrade-file | <int> | | | This field is used as a delimiter. It means all data fields after this one, up to the next delimiter or end of metafile apply to the upgrade file indexed by the number in the field value <int>. |
| img-type | <int> | | | This field indicates the image type of the upgrade file specified by the file field. The type is the enumeration number **<int>**.  Refer to release notes for specific image type. |
| upgrade-file-uri | <string> | | | This field is the URI of the upgrade image file from which the upgrade image is downloaded. |
| partition | | | | This field is the partition descriptor in an upgrade file. Refer to release notes for specific values. |
| | <int> | version | <string> | Version of the partition, consisting of 4 fields of decimal numbers separated by a dot ".". The number in each field must be in the range of 0 to 255. |

# 7.4 Preparing the Upgrade Configuration Metafile

The upgrade configuration metafile is prepared on the server as pointed to by the reader's metafile URI. The data entries in the metafile should follow the format and definition given in Section 7.3. Missing mandatory data entries and bad syntax will cause the reader to reject the metafile.

The upgrade image file pointed to by the **upgrade-file-uri** field must contain the same partitions, image types, and versions as described by the **partition** fields in the metafile. Disagreement between the metafile and the upgrade image file will cause the reader to reject the downloaded image file.

The path and permission of the metafile on the server should be set properly to allow file retrieval via the method specified by the URI parameter in the **config image metafile** command as explained in Section 8.5.2.3.

# 7.5 Image Management Command

## 7.5.1 Command Line Interface Upgrade

An upgrade can be triggered via the Command Line Interface in any one of the following scenarios:

•	The user can invoke the Rshell command **config image upgrade** to instruct the reader to enter push mode, directly download the upgrade image file from the specified URI, and perform an upgrade with the image downloaded.  See Section 8.5.2.5 for details.

- The user can invoke the Rshell command **config image metafile** to instruct the reader to enter pull mode, download a metafile from the specified URI, and perform an upgrade based on the metafile. Regardless of the upgrade status, the reader remembers the URI for future use. See Section 8.5.2.3 for details.

- The user can invoke the Rshell command **config image retrievemode** to manually set the retrieve mode of the reader. If the retrieve mode is set to pull via this command and the reader has a valid metafile URI, the reader will immediately attempt to retrieve the metafile via the URI. If metafile retrieval fails, the reader will retry periodically based on the retrieve period specified in the command. See Section 8.5.2.4 for details.

## 7.5.2 Factory Default Restoration

The user can use the Rshell command **config image factory** to return the reader to a factory default configuration. The command retains the current primary SOP, but defaults the reader's configuration and erases any custom application. See Section 8.5.2.1 for details.

## 7.5.3 Fallback to Previous Image

The user can invoke the Rshell command **config image fallback** to restore the reader to its previous image. See Section 8.5.2.2 for details.

## 7.5.4 Query the Upgrade Status

The user can invoke the Rshell command **show image summary** to view the details of the current primary and secondary images. This command also shows the status of pending and completed upgrades as well as error codes indicating the reasons for upgrade failures. See Section 8.6.3 for details.

The user can invoke the Rshell command **show image metafile** to view the details of the current retrieve mode and metafile data. See Section 8.6.3 for details.

## 7.5.5 Background Execution of Image Management Commands

Some image management commands are executed in the background and are not finished right away. If a previous image management command is still being processed, a subsequent image management command will be rejected with a command response code of "`Previous-Command-In-Progress.`" The following image management commands have this behavior:

```
config image metafile
config image upgrade
config image factory
```

During the execution of these image management commands, the **reboot** command will also be rejected with the "Previous-Command-In-Progress" error unless the force option is applied. All other **config image** and **show image** commands are completed immediately and can be immediately followed by any other image management command.

# 7.6 Upgrade Examples

Shown below is an example of command line activity demonstrating a successful upgrade, using the **push** method. The text entries after the # sign are comments.

```
# Issue a command to upgrade using FTP. The file path is only an
example.
```

```
>
> config image upgrade ftp://
username:password@server1.mydomain.com/binaries/sop-2_4_0.upg
Status=0,'Success'    # command accepted
>
> show image summary   # Query status
Status=0,'Success'
UpgradeStatus=Downloading  # Reader determines upgrade is needed
and starts download
# Current image info
primaryImageType=2
primaryImageSystemVersion='2.4.0.144'
primaryImageConfigVersion='255.255.255.255'
secondaryImageType=2
secondaryImageSystemVersion='2.4.0.128'
secondaryImageConfigVersion='255.255.255.255'>
> show image summary
Status=0,'Success'
UpgradeStatus=Erasing  # Download OK. Erasing secondary flash
primaryImageType=2
primaryImageSystemVersion='2.4.0.144'
primaryImageConfigVersion='255.255.255.255'
secondaryImageType=2
secondaryImageSystemVersion='2.4.0.128'

secondaryImageConfigVersion='255.255.255.255'
>
> show image summary
Status=0,'Success'
UpgradeStatus=Programming  # Now programming new image
primaryImageType=2
primaryImageSystemVersion='2.4.0.144'
primaryImageConfigVersion='255.255.255.255'
secondaryImageType=2
secondaryImageSystemVersion='2.4.0.128'
secondaryImageConfigVersion='255.255.255.255'
>
> show image summary
Status=0,'Success'
UpgradeStatus=Done # programming done successfully
primaryImageType=2
primaryImageSystemVersion='2.4.0.144'
primaryImageConfigVersion='255.255.255.255'
secondaryImageType=2
secondaryImageSystemVersion='2.4.0.128'
secondaryImageConfigVersion='255.255.255.255'
>
# Reader is waiting for reboot to activate the new image. All other
activities are #not affected.
>
> reboot
Status=0,'Success'
>
```

```
# when status LED comes back on as solid green, the reader will be
running from
# the new image
```

# 7.7 Metafile Example

Below is an example of a complete metafile (note that the metafile may contain comment lines that start with a pound sign #):

```
##  This is an example upgrade config metafile.
##  Lines commented out with single # are alternative values or
additional fields
##  Lines commented out with double ## are explanations
##
##  retrieve-period is in minutes
retrieve-mode:pull;retrieve-period=60
#retrieve-mode:push
upgrade-mode:auto
#upgrade-mode:forced
##  reboot at a scheduled time yyyy:mm:dd:hh:mm:ss
commit-mode:scheduled;time="utc.2006:05:08:04:12:32";early-act-
ok=yes
#commit-mode:wait-4-cmd
#commit-mode:immediate
##  dl-retries defaults to no-retry if not present.  retry only if
failed due to timeout
#dl-retries:3
##  dl-retry-period is in seconds
#dl-retry-period:60
upgrade-file:0
img-type:2
## The download-mode field indicates when to start download
## absence of this field means immediate download
## when download-mode is random-delay,'delay' is the max of random
delay
## delay time is in seconds
#download-mode:immediate
#download-mode:fixed-delay;delay=120
download-mode:random-delay;delay=120
upgrade-file-uri:"tftp://fileserver.store.com/impinj-reader-
image.upg"
##  partitions and their versions must agree with what's in the
image
partition:0;version="2.0.1.240"
#partition:1;version="255.255.255.255"
#partition:2;version="1.0.0.3"
```

# 7.8 Other URI Examples

The Speedway reader supports three URI schemes for upgrade: TFTP, FTP, and HTTP. Other examples of URIs:

http://httpserver.mydomain.com/impinj/reader-images/upgrade_metafile
tftp://tftpserver.mydomain.com/image-sop-scp-cap-2.1.1.upg

ftp://user:password@ftpserver.mydomain.com/speedway/images/image-sop-scp-cap-2.1.1.upg

As with any remote file retrieval, the servers should be properly configured such that the files are accessible either anonymously or by the specified user from the client (the reader).

# 7.9 Detailed Upgrade Behavior

## 7.9.1 Upgrade file validity check

The reader always checks the following for the validity of the upgrade file:
- Upgrade file format

- Upgrade file CRC

- Hardware compatibility with the reader

- Agreement between the upgrade metafile and the upgrade image in terms of version number, image type and partitions present.

If the check fails, the upgrade is aborted and the status is reported via the **show image summary** command as explained in Section 8.6.3.

## 7.9.2 Rapid Polling Intervals

If the reader is configured to update automatically (pull mode) and the user attempts to send the reader into push mode by sending a **config image update** command, it is possible that the user will receive the message, "Command-in-Progress" because the automatic update just happened to occur at the same time as the manual command. This situation will most likely occur if the user's network is slow or heavily loaded and the retrieve period (polling interval) is short.

## 7.9.3 Upgrade decision

Not all upgrade attempts will result in an actual upgrade, even if the upgrade file is valid. The reader's upgrade decision is based on the following factors:

- The image versions of the SOP and CAP partitions of the primary image.

- The image version(s) of the partition(s) in the upgrade metafile and the upgrade image files downloaded, as well as the number of partitions present.

- The image type of the primary image, as well as the type indicated by the image metafile and upgrade file.

- The upgrade mode, **forced** or **auto**, as indicated in the upgrade metafile.

In **auto** upgrade mode, the upgrade will happen only when either one of the following is true:

- The upgrade image has the same type as the primary image and at least one partition in the upgrade image has a version higher than the corresponding version in primary image. In this case the partition in the upgrade file that has a lower version number than the one in the primary image will not be used, instead the current primary partition will be kept.

- The upgrade image has different image type from the primary and SOP is present in the upgrade file.

In the **forced** upgrade mode, an upgrade will happen as long as at least one partition in the upgrade file has a different version from the primary image. If the **config image upgrade** command is used, the upgrade is always performed regardless of version numbers or image type.

## 7.9.4 Partition copy-over

The upgrade image file does not necessarily contain all the partitions. The missing partition(s) will be copied over to the secondary image from the primary image upon reboot after upgrade whenever applicable. The behavior is as follows:

If the upgrade file has the same image type as the primary image, then

- If the upgrade file contains the SOP only, the primary SCP and the CAP (if present) are copied over.

- If the upgrade file contains the SOP and the CAP, the primary SCP is copied over.

- If the upgrade file contains the CAP, the primary SOP and the SCP are copied over.

- If the upgrade file contains the SOP and the SCP, the primary CAP, if present, is copied over.

Otherwise, if the upgrade file has a different image type from the primary image, no partition is copied over.  The new image will use the factory default configuration if there is no SCP in the upgrade file. Such behavior allows the current configuration and custom application to be carried over to the new image after an upgrade.

## 7.9.5 Image partitions already programmed

There are cases when the partitions in the upgrade file are already on the secondary image. For example, when a reboot is scheduled in ten hours following a successful upgrade and the reader is pulling the metafile every ten minutes, it will find that the same partitions in the metafile already programmed on the secondary image. The partitions are stored in flash memory, which by its nature has a limited number of programming cycles. To avoid unnecessary programming of this flash memory, the reader checks if any or all of the intended partitions are already programmed and the behavior in these cases is as follows:

- If the upgrade file contains the SOP only and it is already on the secondary image, there is no reprogramming of the flash memory except for marking the primary SCP and the CAP, if present, to be copied over upon reboot after upgrade. (See Section 7.9.4.)

- If the upgrade file contains the SOP and the CAP and both are already on the secondary image, there is no reprogramming of the flash memory except for marking the primary SCP to be copied over upon reboot after upgrade.

- If the upgrade file contains the CAP only and it is already on the secondary image, the primary SOP is copied to the secondary image and the primary SCP is marked as to-be-copied over upon reboot after upgrade.

These behaviors only apply to automatic upgrades performed via the periodic pull method with auto or forced upgrade mode. When the upgrade is manually commanded (pushed) with the **config image upgrade** command, the flash memory is always programmed with the upgrade image regardless of the versions on the primary and secondary images.

## 7.9.6 Scheduled reboot time

As shown in Table 7-1, when commit-mode is set to scheduled , a reboot time must be specified using either the **time** or **wctime** parameters.  There are two formats in specifying time, the fully-specified format:

     &lt;time-zone&gt;.yyyy:mm:dd:hh:mm:ss

and  the wildcard format:

     &lt;time-zone&gt;.*.hh:mm:ss

For readers with system image version (SOP partition) lower than 2.6.0, wildcard time is not supported; reboot time has to be specified with time parameter using the fully-specified time format. For version 2.6.0 and above, both formats are supported in the time parameter.

For backward compatibility, the wctime parameter is used and supported by versions 2.6.0 and above. This allows the same upgrade metafile to be used for upgrading readers with any image version.

For example, to upgrade readers with a mixture of image versions, either one of the following two parameter lists can be used:

```
time="utc.2007:04:15:23:00:00"
time="utc.2007:04:15:23:00:00";wctime="utc.*.23:00:00+r30m"
```

The first one instructs all reader to reboot at the specified time while the second instructs all readers with versions lower than 2.6.0 to reboot at the specified time and all the readers with 2.6.0 and higher to reboot some random number of minutes (up to 30) after the upcoming 11PM after the upgrade is performed.

The use of wctime allows the newer readers to reboot at a wildcard time without causing the older readers to reject the metafile because of an un-recognized time format.

If it's known for sure that all readers have version 2.6.0 or above, either one of the following parameters can be used to reboot at wildcard time:

```
time="utc.*.23:00:00+r30m"
wctime="utc.*.23:00:00+r30m"
```

**wctime** is necessary only when there is a mixture of readers to upgrade *and* wildcard time is desired in rebooting the newer readers. Once all older readers are phased out, only the parameter **time** will be needed for indicating reboot time of either format.

There is a caveat in the use of wildcard time. Since hh:mm:ss of the reboot in the wildcard time is relative to the time of the completion of the upgrade, the actual reboot time may depend on when the upgrade is completed during the day. For example, if the wildcard reboot time is 23:00:00 and the upgrade is completed by 4PM, the reboot is 7 hours away. But if the upgrade is completed by 11:30PM, the reboot will be 23.5 hours away (i.e., at 11PM the next day).

When specifying the desired wildcard reboot time in the metafile, two delay factors should be considered, one is the time it takes for the reader to check the metafile (i.e., the the retrieve-period) and the other is the time it takes to perform the upgrade. Always modify the metafile well ahead of the intended wildcard reboot time if a same-day reboot is desired.

# 8 Rshell Command Line Interface

The Speedway reader's Rshell Command Line Interface (CLI) is accessed via serial, Telnet, or SSH connectivity.

**Important**    The CLI is meant to be a machine interface. As such, Impinj supports backward compatibility for this interface—no existing inputs will change, no existing outputs will change but new commands may be added or new optional arguments may be added to existing commands, always at the end.

## 8.1 Rshell Overview

Users may navigate to any of the menus simply by entering the menu name at the Rshell prompt, as shown below:

```
> show network
show network >
```

For machine execution, all commands can be called from the root menu. For example:

```
> show network
show network> dns

is equivalent to:

> show network dns
```

All commands return data in machine/human readable format. See Section 8.2.

At all menus, the **exit** command or simply '**.**' will return the user to the previous menu context. To exit Rshell and terminate the user session (serial, telnet, or SSH), the **exit** command must be executed from the root menu (the period only will not suffice):

```
show network> exit
> show
show > .
> .
>
```

## 8.1.1 Reader Help

At all menus, the **help** command (or simply **?**) will list all the commands available from the active menu, as well as the submenus that can be accessed from the active menu.

```
> help

Commands:
reboot   - Reboots the system.
exit     - Exit this submenu and return to the parent menu.
help     - Displays this help message.
?        - Displays this help message.

Sub-menus:
config   - Submenu of configuration commands.
```

```
show      - Submenu of elements that may have their configuration
             or  status shown.
transfer  - Submenu of transfer commands.
```

Menu navigation and the help keyword (or ?) can be combined on the same line to list all the commands available for that menu. For example:

```
> show ?

Commands:
access  - Show users and their access level.
exit    - Exit this submenu and return to the parent menu.
help    - Displays this help message.
.       - Exit this submenu and return to the parent menu.
?       - Displays this help message.

Sub-menus:
all     - Submenu of multi-category info display commands.
image   - Submenu of image status commands.
logging - Submenu of logging status commands.
network - Submenu of network status commands.
rfid    - Submenu of RFID status commands.
snmp    - Submenu of SNMP status commands.
system  - Submenu of system status commands.
```

At all menus, entering the help command or ? prior to a command or menu, will return the syntax for its usage. For example:

```
 > ? show

show     - Submenu of elements that may have their configuration or
            status shown.
Usage:  show  [<subcommand> ...]
 >
```

or

```
 > ? show access

access  - Show users and their access level.
Usage:  show access
 >
```

Entering the **?** between a menu and sub-menu/command will return the usage for the items following the **?** at the lowest level. In the example below, **image** is a menu that contains commands of its own, so entering **show ? image** brings up a usage help menu indicating that subcommands are necessary. If one of those subcommands is entered (**show ? image metafile**), the detailed usage is given.

```
 > show ? image

image   - Submenu of image status commands.
Usage:  image  [<subcommand> ...]
```

```
 > show ? image metafile
```

```
metafile - Command to display upgrade metafile info.
Usage:  image metafile
```

## 8.2 Response Format

The first line of every response has the following format:

```
Status=errorCode,'error string'
```

where errorCode is a numeric value and 'error string' is a single-quoted, human-readable error code. The error codes are defined in Table 8-1.

**Table 8-1 Error Codes**

| Error Code | Error String | Description |
|---|---|---|
| 0 | Success | |
| 1 | Invalid-Command | Command could not be parsed and identified as one of the commands supported by the interface |
| 2 | Invalid-Command-Parameter | Parameter types was unrecognized for this command (one or more) |
| 3 | Invalid-Parameter-Value | One or more parameter values was illegal or out-of-range for this command |
| 4 | Parameter-Dependency-Error | Parameter value or combination was invalid in combination with other parameters or values |
| 5 | Incomplete-Parameter-List | The parameter list was incompletely specified and the command cannot be executed |
| 6 | System-Resource-Limit | Command could not be executed because of a resource limit on the box (e.g., could not add a fourth trap receiver because the device only supports three) |
| 7 | Unsupported-Command | Reserved for Future commands |
| 8 | Permission-Denied | User does not have permission to access this command |

**Table 8-1 Error Codes (Continued)**

| Error Code | Error String | Description |
|---|---|---|
| 9 | Previous-Command-In-Progress | The command was rejected because a previous command is still in progress such that this one could not be processed |
| 10 | Command-Being-Processed | The command cannot be finished right away; it is being processed. |

A sample error parameter string is shown below:

```
> conffigg (this is a misspelled, invalid command)
Status=1,'Invalid-Command'
```

When a command's action requires return parameters, they follow the error status, one parameter per line, and in the following format:

```
parameterName=value0
parameterName=value1
…
parameterName=value9
```

The specific response parameters for each command are detailed in the sections that follow.

## 8.3 Interpreting Results

Every command response follows the format given in Section 8.2, with the first line being a status code and any succeeding lines providing key parameters and their values. For backward compatibility, any parameters added to commands as part of a firmware improvement will always be added at the end. Applications designed to machine interpret the CLI responses should ignore responses given after those of interest.

For example, in firmware version 2.4.0, the **show network summary** command provided the following response:

```
 > show network summary
Status=0,'Success'
ipAddressMode=dynamic
ipAddress=10.0.10.155
ipMask=255.255.0.0
gatewayAddress=10.0.0.10
broadcastAddress=10.0.255.255
hostname=Speedway-00-01-44
 >
```

For firmware version 2.6.0, the same command provides this response:

```
 > show network summary
Status=0,'Success'
ipAddressMode=dynamic
ipAddress=10.0.10.155
ipMask=255.255.0.0
gatewayAddress=10.0.0.10
broadcastAddress=10.0.255.255
hostname=Speedway-00-01-44
llaStatus=enabled
 >
```

So any software using the response parameters would need to parse through:

```
hostname=Speedway-00-01-44
```

while ignoring the last line of:

```
llaStatus=enabled
```

**Important**   Because Impinj reserves the right to add new commands and new optional arguments to existing commands, usage and help menus are subject to change.

## 8.4 Reboot Command

The **reboot** command instructs the reader to reboot. This command may be used after a manual upgrade of the reader's firmware or application software. The reboot command may also contain an optional argument **force** that will cause the reader to reboot even if a current operation is pending (such as a firmware download). If the force argument is absent, the reader will reject the command if a current download is in progress.

## 8.5 Config Command

The **config** command has seven submenus, as shown in Table 8-2, and described in the succeeding sections.

### Table 8-2 "config" Command Parameters

| Command | Description |
|---------|-------------|
| access | leads to submenu of access configuration commands |
| image | leads to submenu of image and upgrade configuration commands |
| logging | leads to submenu of logging configuration commands |
| network | leads to submenu of network configuration commands |
| rfid | leads to submenu of RFID configuration commands |
| snmp | leads to submenu of SNMP configuration commands |
| system | leads to submenu of system info configuration commands |

## 8.5.1 config access Command

The **config access** command changes the password for a given access level.  There are three levels of access: root, operator, and monitor.

The root access level consists of only the root user. The root user is allowed all adminsitrative access and cannot be deleted. Only the root user may create other user accounts.

The operator access level allows all administrative functions except for creating or altering user accounts (i.e., a read and write user).

The monitor access level may only query reader status and statistics (i.e., a read-only user).

The factory default setting for the Speedway reader has only the root user established. New user accounts are created by the root user. Each account is given:

• a name of one to eight alphanumeric characters

• an access level of either operator or monitor

• a password of one to eight printable characters

The user account name and password may be used via either the command line interface (telnet or ssh) or the browser-based interface (http). The config access submenu commands are described in Table 8-3 and config access command arguments are described in Table 8-4.

### Table 8-3 "config access" Command Options

| Command | Parameters | Description |
|---------|-----------|-------------|
| adduser | level \| username \| [password] | Add a user, where "level" may be set to either operator or monitor. |
| chpasswd | username \| [newpassword] | Change password of a user |
| deluser | username | Delete a user |
| mypasswd | [oldpassword] \| [newpassword] | A logged-in users may change their own password. |
| root | [newpassword] | This  function may be also be completed using the config access chpasswd command with "root" provided as the username. This subcommand exists to provide backward compatibility with previous firmware versions. |

**Table 8-4 "config access" Command Parameters**

| Argument | Options | Format | Description |
|---|---|---|---|
| Username | Root | N/A | Factory established and may not be deleted. |
| | Selectable | String | one to eight alphanumeric characters |
| Level | Root | N/A | Root level is factory established and may not be deleted. Root has all administrative authority and is the only level that may create other user accounts. |
| | Operator | String | Operator access level has all adminstrative authority (may change the configuration and status of the reader) except for creating or altering user accounts (read/write user). |
| | Monitor | | Monitor access level may only query reader status and statistics (read-only user). |
| (old)Password (new)Password | | String | Password to set as account's active password (one to eight printable characters). Passwords longer than eight characters are allowed but the extra characters are ignored. Passwords entered on the command line are clear text and visible to anyone. If no password is entered in the command line, the reader will prompt for the password. In this case, the password will be kept secret because the "*" character will be repeated on the screen instead of the actual printable character. |

```
Usage:   config access adduser <level> <username> [<password>]
         <level> is one of operator or monitor.

Usage:   config access chpasswd <username> [<newpassword>]

Usage:   config access deluser <username>

Usage:   config access mypasswd [<oldpassword> [<newpassword>]]

Usage:   config access root [<newpassword>]
```

## 8.5.2 config image Command

The **config image** commands provide configuration options for image and upgrade configurations. It contains direct subcommands only, no sub-menus. These commands will not take effect until the reader is rebooted. Detailed explanation of how to upgrade images is given in Section 7.

### 8.5.2.1 config image factory Command

The **config image factory** command, followed by a reboot, returns the reader to the factory default configuration associated with the current running image and at the same time, removes the custom application partition. Once complete, the factory defaults do not take effect until the system is rebooted. This command takes no parameter.

During return to factory defaults, the **show image summary** (Section 8.6.3) command reports the **UpgradeStatus** as "Erasing," "Programming," or "Done." After this command is processed, the reader will continue its operation with the current configuration until a reboot command is issued. In the mean time, the metafile retrieve-mode is set to push (i.e., the factory default restore command cancels a previously scheduled periodic upgrade). When the reader comes up from the reboot, it will run the same SOP image version as the one from which it performed the factory default restore, with factory default configuration and no custom application.

If the reader is in pull mode during the execution of this command, it is possible that the reader is currently retrieving the metafile or performing an upgrade. In these instances, this command may return "Previous-Command-In-Progress."

### 8.5.2.2 config image fallback Command

The successful processing of the **config image fallback** command, followed by a reboot, returns the reader to the previous valid image. This command takes no parameter.

If there is no valid previous image available for fall back, the command response will be "failure" with a reason "No Fallback Image Available," as listed in Table 8-30. After this command is successfully processed, the reader waits for a reboot command to fall back to the previous image. In the mean time, the reader operates normally except that all the **config image** commands will be rejected with the reason "Current Image Invalidated." Also the metafile retrieve-mode is set to push, i.e., the fallback command cancels a previously scheduled periodic upgrade. When the reader is rebooted, the previous image will be activated.

If the reader is in pull mode during the execution of this command, it is possible that the reader is currently retrieving the metafile or performing an upgrade. In these instances, this command may return "`Previous-Command-In-Progress.`"

**Important**    A fallback will utilize all the old configuration settings, including the upgrade metafile settings as if the upgrade to the newer image was never performed—which may trigger an immediate upgrade. If the URI of the old metafile is known and an immediate upgrade is not desired, the user should remove or rename the old metafile before performing a fallback.

### 8.5.2.3 config image metafile Command

This command takes the Universal Resource Identifier (URI) of the upgrade configuration metafile as the parameter. It commands the reader to perform an upgrade using the metafile identified by the URI.

```
Usage:   config image metafile <URI>
```

Upon receiving this command, the reader updates its local upgrade configuration URI, retrieves the upgrade configuration metafile, and performs the upgrade in accordance with the metafile. If the

upgrade is successful, how the new image is activated depends on the commit-mode specified in the metafile (see Table 7-1).

If the reader is in pull mode during the execution of this command, it is possible that the reader is currently retrieving the metafile or performing an upgrade.  In these instances, this command may return "`Previous-Command-In-Progress.`"

### 8.5.2.4 config image retrievemode Command

This command sets the reader's metafile retrieve mode and (if applicable) the retrieve period (see Table 8-5). When the retrieve-mode is set to push, the reader will take no upgrade action. To perform an upgrade in the push mode the user must issue a **config image upgrade** command to directly download an upgrade image (see Section 8.5.2.5).

```
Usage:   config image retrievemode push
         config image retrievemode pull <retrieve-period>
         <retrieve-period> is how often the reader pulls the
          metafile from the most recently specified <URI>.
```

#### Table 8-5 "config image retrievemode" Command Parameters

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| retrieve-mode | pull \| push | String | When the mode is pull, the reader periodically retrieves the metafile from the most recent metafile URI at the rate specified by the retrieve-period.<br>In push mode the user must manually specify a new metafile URI or manually upgrade the file to perform the upgrade. |
| | retrieve-period | Integer | Interval of pull in minutes—only applicable when mode is pull. This retrieve period is used only until the reader retrieves a valid metafile, at which point the retrieve period from the metafile is adopted. |

If this command results in a change from push to pull, or a change of **retrieve-period** while the current mode is pull, the reader immediately attempts to download a new upgrade configuration metafile using its current metafile URI.

### 8.5.2.5 config image upgrade Command

This command is used to instruct the Speedway reader to directly download an upgrade image file and perform an immediate upgrade. Upgrade image files are stored on a file server and retrieved by the Speedway reader from the location identified by the URI.

```
Usage:   config image upgrade <URI>
```

Upon receiving this command, the Speedway reader downloads the image file and, if the file is valid and eligible, performs the upgrade. When this command is used, the upgrade will always be performed even if the version matches the current one.

If the upgrade is successful, the new image is not activated until the user reboots the system.

If the reader is in pull mode during the execution of this command, it is possible that the reader is currently retrieving the metafile or performing an upgrade. In these instances, this command may return "`Previous-Command-In-Progress.`"

Note that this command does not change the reader's upgrade configuration URI, but it sets the retrieve-mode to push, meaning that the reader will not periodically retrieve the upgrade configuration metafile until the retrieve-mode is set to pull again. See Section 8.5.2.4.

## 8.5.3 config logging Command

The **config logging** commands provide configuration options for remote syslog capture as well as internal Impinj log capture via submenus. The internal log is only stored in the RAM file system, is capable of high-speed, real-time logging of internal events, and is routed to the syslog based on the severity level (described below). The syslog is stored in the local Flash memory file system, is the standard Unix logging system, and is forwarded to a remote syslog server.

Logging levels may be set to one of eight options (in decreasing order from most severe to least): emergency, alert, critical, error, warning, notice, info, and debug. Which data are forwarded from the internal Impinj (**internallog**) log capture to the remote system logging (**syslog**) depends on the relative level settings. For example, if the **internallog** is set to the level of "critical," and the **syslog** level is set to "debug," then all internal log data will be sent to the remote system capture because the severity level of the internal Impinj log data will always be greater than the remote system log. Conversely, if the **internallog** is set to "info" and the **syslog** is set to "alert," then only internal log data with severity level of "alert" and higher will be forwarded. The internallog data is still accessible via Rshell but it will not be stored in the syslog. See Figure 8-1.
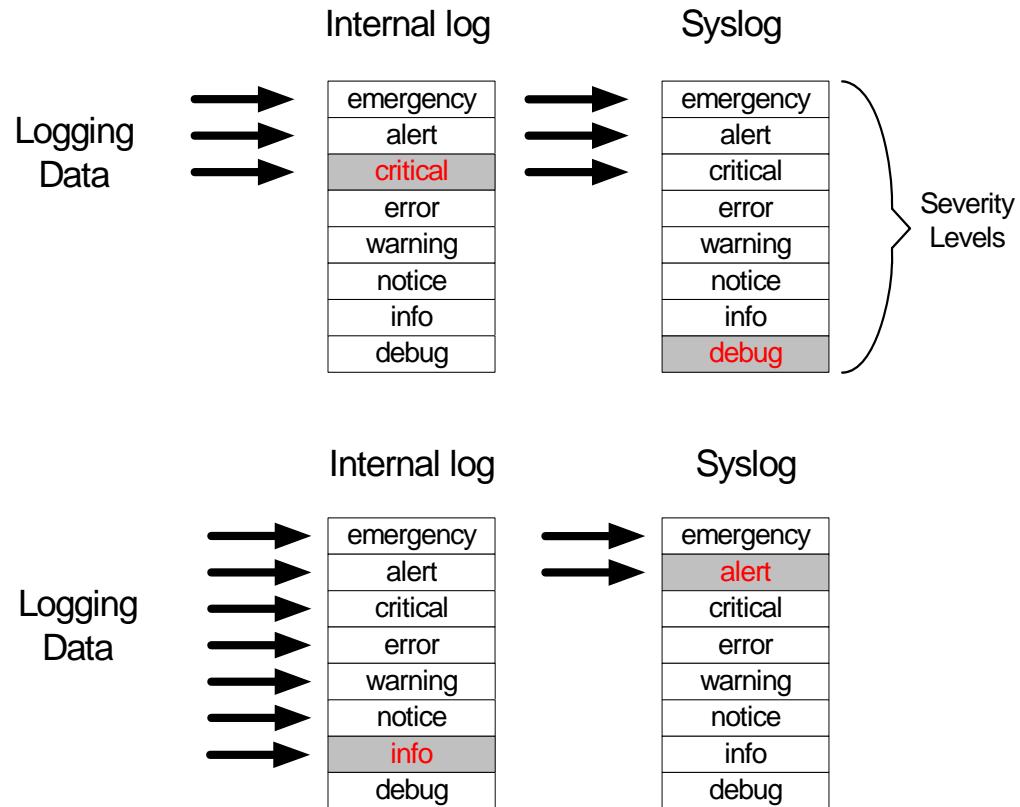
**Figure 8-1 Relative Severity Level Logging Transfer**

### 8.5.3.1 config logging internallog Command

The **config logging internallog** command has only one subcommand, **set**, that sets the internal logging level for reader log events.  These events can be viewed via the **show logging** command or transferred off the reader via the **transfer** command. The command parameters are shown in Table 8-6. The command sets the logging level for a log class to one of a set of pre-defined values.

**Table 8-6 "config logging internallog set" Command Parameters**

| Argument | Option | Format | Description |
|----------|--------|--------|-------------|
| classname | ApplicationLevel \| Configuration-Level \| MgmtLevel \| NetworkLevel \| RFIDParameters \| RFIDSingulation \|RFIDAccess \| System | String | Selects log class level to set |

**Table 8-6 "config logging internallog set" Command Parameters**

| Argument | Option | Format | Description |
|---|---|---|---|
| level | Emergency \| Alert \| Critical \| Error \| Warning \| Notice \| Info \| Debug | String | Configures the level at and above which logs are sent to the log database. Listed in decreasing order of severity. |

Usage for the **config logging internallog set** command is shown below:

```
Usage:  config logging internallog set <className> <level>

<className> is (ApplicationLevel | ConfigurationLevel | MgmtLevel
| NetworkLevel | RFIDParmeters | RFIDSingulation | RFIDAccess |
System)

<level> is
(emergency|alert|critical|error|warning|notice|info|debug)
```

A sample command that sets the RFID Access logging is shown below:

```
> config logging internallog set RFIDAccess emergency
Status=0,'Success'
```

### 8.5.3.2 config logging syslog Commands

The **config logging syslog** menu provides the configuration interface for the syslog module on the reader. If all remote syslog servers are removed, the reader will begin to log in its internal memory. The command parameters are shown in Table 8-7.

**Table 8-7 "config logging syslog" Command Parameters**

| Command | Argument | Format | Description |
|---|---|---|---|
| add | IpAddress\| hostname | String | Add a new syslog server with given address or hostname |
| del | IpAddress\| hostname | String | Delete a syslog server with given address or hostname |
| delall | | | Delete all syslog servers |

**Table 8-7 "config logging syslog" Command Parameters (Continued)**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| level | Emergency \| Alert \| Critical \| Error \| Warning \| Notice \| Info \| Debug | String | Set the syslog security level. Only logs at or greater in severity than this level will be forwarded to syslog. Levels listed in order of decreasing severity. |
| reset | | | Removes all archived syslog messages. |

Sample commands are shown below:

```
> config logging syslog add 10.0.10.37
Status=0,'Success'

> config logging syslog del 10.0.10.37
Status=0,'Success'

> config logging syslog level warning
Status=0,'Success'

> config logging syslog reset
Status=0,'Success'
```

## 8.5.4 config network Command

The **config network** menu allows the user to administer and manually provision the network settings for the reader. The config network command has the following subcommands:
.

**Table 8-8 "config network domain" Command Parameters**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| domain | domain-name | String | Configures one or more static search domains for the reader. If DHCP is used, this static domain(s) will not be used. If the IP address mode is turned to static, the domains will be put to use. The STRING is a list of domains, separated by a space. If the STRING is absent, this command deletes the static search domain. |

**Table 8-8 "config network domain" Command Parameters (Continued)**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| hostname | host-name | String | Configures the current hostname for the reader. Parameters returned from DHCP will override this value. |
| lla | enable \| disable | String | Enable/disable the link local address protocol. With LLA enabled, the reader will automatically choose an IP address in the link-local image range (169.254.*.*) when no dynamic IP address is available from the DHCP server. A link-local address allows a reader to communicate with other LLA-capable network devices on an isolated network that lacks a service infrastructure such as DHCP. |
| mdns | enable \| disable | String | Enable/disable multicast DNS protocol, including local hostname resolution and service discovery. The local hostname resolution feature gives the reader a local hostname in addition to an IP address as its network identity. On an isolated network that lacks DNS service but has the hostname enabled, a reader with hostname **speedway-00-01-02**, for example, may be reached using **speedway-00-01-02.local**. This command works in conjunction with the service discovery feature (see Section 8.5.4.3), which allows the RFID (Impinj proprietary) service, LLRP (Low Level Reader Protocol) service, and HTTP (Web) service to be auto-discovered by other network devices. |

Samples of the direct commands and responses are shown below:

```
> config network domain bar.com
Status=0,'success'

> config network hostname speedwayc11
Status=0,'success'

> config network lla enable
> Status=0,'success'
>
 > config network mdns enable
Status=0,'Success'
```

### 8.5.4.3 config network dnssd Command

The **config network dnssd** enables or disables service discovery of the HTTP (Web), RFID (Impinj proprietary), and LLRP (low level reader protocol) services. When service discovery is enabled on the reader, another device on the network with DNS-Service-Discovery (DNS-SD) capability can automatically discover the reader. For example, the Internet Explorer™ with Apple®'s Bonjour™ plug-in installed can auto-discover and display a list of readers that advertise HTTP service on the same local network. The RFID service that the reader advertises is "`_rfid._tcp.`" A DNS-SD-capable application can browse, find the reader, and connect to it based on the service port it advertises. Command parameters are shown in Table 8-11:

**Table 8-11 "config network dnssd" Command Parameters**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| http | enable \| disable | String | Enable/disable http service announcement |
| rfid | enable \| disable | String | Enable/disable rfid service announcement |
| llrp | enable \| disable | String | Enable/disable llrp service announcement |

A sample command and response is shown below:

```
>config network dnssd http enable
Status=0,'success'
```

## 8.5.4.4 config network ip Command

The **config network ip** command allows the user to statically configure IP settings, or configure the reader to use DHCP. Command parameters are shown in Table 8-12:

**Table 8-12 "config network ip" Command Parameters**

| Command | Argument | Format | Description |
|---|---|---|---|
| dynamic | | | Configures the network for dynamic address resolution using the DHCP proto-col. |
| static | IpAddress<br><br>netmask<br><br>gateway-address<br><br>broadcast-address | | Configure the network for static address resolution. The following combinations of parameters are valid:<br><br><IpAddress><br><br><Ip Address> <gateway-address><br><br><Ip_Address> <netmask> <gateway-address> <broadcast-address><br><br>For parameters not specified the reader will use default values. |

Samples of the commands and responses are shown below:

```
> config network ip dynamic
Status=0,'success'

> config network ip static 192.168.20.116
Status=0,'Success'
 > show network summary
Status=0,'Success'
ipAddressMode=static
ipAddress=192.168.20.116
ipMask=255.255.255.0
gatewayAddress=192.168.20.1
broadcastAddress=192.168.20.255
hostname=speedwayc11

> config network ip static 192.168.20.116 255.255.255.0
192.168.20.1 192.168.20.255
Status=0,'success'
 > show network summary
Status=0,'success'
ipAddressMode=static
ipAddress=192.168.20.116
ipMask=255.255.255.0
broadcastAddress=192.168.20.255
gatewayAddress=192.168.20.1
```

```
hostname=speedwayc11
>
```

### 8.5.4.5 config network ntp Command

The **config network ntp** command allows the user to statically configure NTP servers. These servers are in addition to any provisioned through DHCP. The command parameters are shown in Table 8-13:

**Table 8-13 "config network ntp" Command Parameters**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| Add | IpAddress\|hostname | String | Add a static server (identified by either an IP address or hostname) to the list of current NTP servers. |
| Del | IpAddress\|hostname | String | Delete a statically configured server (identified by either an IP address or hostname) from the list of current NTP servers. |
| Delall | | | Delete all the statically configured NTP servers. |

A sample of the command and response is:

```
> config network ntp add yourservername.com
> Status=0,'success'
>
```

### 8.5.4.6 config network trace Command

The **config network trace** command sets up a remote network trace utility to capture all network traffic data and redirect it from the `<source>` to a remote system. For example, it is possible to capture all data transmitted and received on the external network connection and redirect the captured data to a remote computer for analysis. When the trace is active, the data is transmitted in "libpcap" format to the remote system via a TCP/IP connection. Since TCP/IP requires acknowledgement of packet data, an application (such as "netcat" in Linux/Unix) must be running on the remote computer (on the desired port) to save all the data transmitted, otherwise the data will be dropped, and the trace will end. The commands are shown in Figure 8-14.

**Table 8-14 "config network trace" Command Parameters**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| start | source | String | source address for network trace |
| | destination address | String | destination address for network trace |
| | destination TCP port | String | port at destination address configured with a TCP/IP listener waiting to accept and store the data |
| stop | | | stops any on-going remote network trace utility |

A sample of the command and response is shown below:

```
> config network trace start external my_pc 2002
> Status=0,'success'
>
```

This example usage of the **config network trace** command would start capturing the external net-work traffic and redirecting it to <my_pc> port 2002 for analysis. Note that <my_pc> must have a TCP/IP listener waiting on port 2002 to accept and store the data. For example, if my_pc is run-ning Linux/Unix, it is possible to use the "netcat" utility to listen on port 2002 and redirect the data to a file. Since this file is in "libpcap" format, it may be directly opened with standard networking monitoring tools such as "tcpdump," "ethereal," or "wireshark."

To stop an active redirection, enter:

```
> config network trace stop
> Status=0,'success'
>
```

## 8.5.5 config rfid Command

The **config rfid** menu allows the user to set parameters of the speedway control interface.

### 8.5.5.1 config rfid resetstats Command

The **config rfid resetstats** command resets the RFID statistics maintained by the reader.
A sample of the command and response is shown below:

```
> config rfid resetstats
Status=0,'success'
```

### 8.5.5.2 config rfid llrp Command

The **config rfid llrp** command enables the user to configure the LLRP implementation. This menu provides the following subcommands:

**Table 8-15 "config rfid llrp" Command Parameters**

| Command | Description |
|---------|-------------|
| connclose | Supports manual closing of the current LLRP connection |
| factory | Resets the LLRP configuration to its factory defaults. This action resets only in-band configuration, not configuration items controlled by rshell or the Web interface. In addition to configuration reset, all ROSpecs and AccessSpecs are also deleted |
| resetstats | Resets the LLRP-specific statistics maintained by the reader. |

### 8.5.5.2.1 config rfid llrp inbound Command

The **config rfid llrp inbound** command provides a submenu of client-initiated connection configuration commands. At the moment, only the **tcp** subcommand is supported, which has its own series of subcommands, as described in Table 8-16.

**Table 8-16 "config rfid llrp inbound tcp" Command Parameters**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| port | port number | Integer | Configure the port where TCP connections are accepted. Default is IANA-assigned port of 5084 |
| service | enable / disable | String | enable/disable LLRP client-initiated TCP connections to the reader. Disabling this service will cause an active client-initiated connection to be terminated and all future connection attempts to be refused. Enabling this service will cause the reader to accept new connections at the port configured using the port subcommand. |

```
Usage:  config rfid llrp inbound tcp port <port number>

Usage:  config rfid llrp inbound tcp service <enable|disable>
```

## 8.5.5.2.2 config rfid llrp outbound Command

The **config rfid llrp outbound** command leads to a submenu of reader-initated connection configuration commands, as shown in Table 8-17.

**Table 8-17 "config rfid llrp outbound" Command Parameters**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| add | hostname \| <:port> | String \| Integer | Add a new host to which the reader will attempt reader-initiated LLRP connections. This host is mandatory, but the port number is optional. If the port number is omitted, the reader will attempt to connect to the remote host at the default IANA LLRP port of 5084. The reader currently only supports one configured remote host. |
| delall | | | Delete all remote hosts to which the reader attempts reader-initiated LLRP connections |
| del | hostname \| <:port> | String \| Integer | Delete a specific remote host to which the reader attempts reader-initiated LLRP connections. The host and port combination must already have been configured for the command to succeed. |
| open | hostname \| <:port> | String \| Integer | Attempt to open an LLRP connection to the specified remote host. This connection is attempted just once. No retries are attempted and the host/port combination is not preserved. This command should only be used as a debugging aid. Deployment scenarios using reader-initiated connections should use the "add" command parameter for this purpose. |

**Table 8-17 "config rfid llrp outbound" Command Parameters (Continued)**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| retry | seconds | Integer | Configure the frequency in seconds at which reader-initiated connections are attempted. This number represents the minimum time between a failed connection attempt and the next connection attempt by the reader. The reader implements a geometric progression back-off timer using this input number as the multiplier (seconds X $2^{(n-1)}$, where n is the number of attempts). For example, if the seconds argument is set to 5, the reader will attempt to connect to the remote host after 5 seconds, 10 seconds, 20 seconds, then 40 seconds, etc. After a successful connection, the retry timer is reset to the minimum value and will repeat if the connection fails. |
| service | enable \| disable | String | Enable or disable reader-initiated LLRP connections from the reader. Disabling this service will cause an active reader-initiated connection to be terminated and all future connection attempts to be cancelled. Enabling this service will cause the reader to begin connection attempts to any configured remote hosts. |
| timeout | seconds | Integer | Configure the number of seconds a reader will wait for a connection to be established (the three-way handshake of the TCP layer) before declaring failure. The LAN/WAN type should be considered when tuning this value. For example, for a high-latency WAN, one could tune this variable higher so that the reader waits longer for the handshake to complete before giving up on the connection attempt. A failed connection will invoke the retry timer (see retry command entry). |

### 8.5.5.3 config rfid mach1 Command

The **config rfid mach1** command leads to a submenu of client-initated connection configuration commands, as shown in Table 8-18

**Table 8-18 "config rfid mach1" Command Parameters**

| Command | Argument | Format | Description |
|---|---|---|---|
| service | enable \| disable | String | Enable or disable client-initiated Mach1 connections to the reader. Disabling this service will cause an active client-initiated connection to be terminated and all future connection attempts to be refused. Enabling this service will cause the reader to accept new conections at the default Mach1 port of 49380. Note that this command only disables external Mach1 connections. Internal Mach1 connections by reader-hosted applications (for example, SDK) will still be allowed. |
| resetstats | | | Reset the Mach1-specific statistics maintained by the reader |

## 8.5.6 config snmp Command

The **config snmp** menu allows the user to set the SNMP configuration. The command parameters are shown in Table 8-19.

**Table 8-19 "config snmp" Command Parameters**

| Command | Argument | Format | Description |
|---|---|---|---|
| service | enable/ disable | String | globally enable or disable the SNMP service |

The command usage is shown below:

```
Usage:  config snmp service <enable/disable>
```

### 8.5.6.1 config snmp access Command

The **config snmp access** command supports setting of SNMP access configuration. The command parameters are shown in Table 8-20.

**Table 8-20 "config snmp access" Command Parameters**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| rocommunity | RO-Community | String | Set the Read-Only community string |
| rwcommunity | RW-Community | String | Set the Read-Write community string |

A sample of the command and response is shown below:

```
> config snmp access rocommunity public
Status=0,'success'
```

### 8.5.6.2 config snmp write Command

The **config snmp write** command supports setting of SNMP write capability. The command parameters are shown in Table 8-21.

**Table 8-21 "config snmp write" Command Parameters**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| enable | all | String | Enable SNMP write on all objects that support write |
| disable | all | String | Disable SNMP write on all objects |

A sample of the command and response is shown below:

```
> config snmp write enable all
Status=0,'success'
```

### 8.5.6.3 config snmp trap Command

The **config snmp trap** command supports setting of SNMP write capability. The command parameters are shown in Table 8-22.

**Table 8-22 "config snmp trap" Command Parameters**

| Command | Argument | Format | Description |
|---|---|---|---|
| enable | all \| non-rfid \| devopstate \| srcopstate \| rdpntopstate \| notifchanop-state | String | Enable a particular group or an individual trap represented by the argument, where arguments are:<br>*all*: all traps<br>*non-rfid*: all the traps except for those defined in EPCglobal Reader Management MIB<br>*devopstate*: device operational state trap<br>*srcopstate*: source operational state trap<br>*rdpntopstate*: readpoint operation state trap<br>*notifchanopstate*: notification channel operation state trap |
| disable | all | String | Disable SNMP write on all objects |

A sample of the command and response is shown below:

```
> config snmp trap enable all
Status=0,'success'
```

### 8.5.6.3.1 config snmp trap receiver Command

The **receiver** submenu under **config snmp trap** supports the setting of trap receiver configurations. The command parameters are shown in Table 8-23.

**Table 8-23 "config snmp trap receiver" Command Parameters**

| Command | Argument | Format | Description |
|---|---|---|---|
| add | host \| [port \| community] | host: IP address or hostname<br><br>port: Integer<br><br>community: String | Add a trap receiver.<br>*host*: IP address or hostname of the receiver.<br>*port*: port number of the receiver. This parameter is optional and defaults to 162.<br>*community*: the trap community string of the receiver. This parameter is optional and defaults to "public." |

**Table 8-23 "config snmp trap receiver" Command Parameters (Continued)**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| del | host \| [port \| community] | host: IP address or hostname<br><br>port: Integer<br><br>community: String | Delete a trap receiver. *port* and *community* are optional parameters. When they are present, the trap receiver(s) with the specified port and/or community are deleted. When they are absent, the trap receiver matching *host* is deleted regardless of port and community. |
| delall | None | | Delete all trap parameters |

A sample of the command and response is shown below:

```
> config snmp trap receiver add 100.100.100.100
Status=0,'success'
```

### 8.5.6.3.2 config snmp trap log Command

This command configures the logging of traps. The command parameters are shown in Table 8-24.

**Table 8-24 "config snmp trap log" Command Parameters**

| Command | Argument | Format | Description |
|---------|----------|--------|-------------|
| enable | all | String | Enable logging of all traps. |
| disable | all | String | Disable logging of all traps. |
| level | trap name; level name | String | Sets the log level of a group of traps or a particular trap.<br><br>*trap name* is one of the following:<br>*all*: All traps<br>*non-rfid*: all the traps except for those defined in EPCglobal Reader Management MIB<br>*devopstate*: Device operational state trap<br>*srcopstate*: Source operational state trap<br>*rdpntopstate*: Readpoint operation state trap.<br>*notifchanopstate*: notification channel operation state trap.<br><br>*level name* is one of the following:<br>debug, info, notice, warning, error, critical, alert, emergency |

A sample of the command and response is shown below:

```
> config snmp trap receiver add 100.100.100.100
```

```
Status=0,'success'
```

### 8.5.6.4 config snmp epcg Command

The **config snmp epcg** command supports the setting of objects in the EPCglobal RM MIB. There are no direct subcommands and only one submenu, **device**, for this command.

### 8.5.6.4.1 config snmp epcg device Command

This submenu permits configuration of the snmp egcg device role. The command parameters are shown in Section 8-25.

**Table 8-25 "config snmp epcg device" Command Parameters**

| Argument | Format | Description |
|---|---|---|
| <device-role> | String | A device role description string as defined by EPCG RM Device Role object. |

## 8.5.7 config system Command

This menu allows configuration of the system identification parameters. See Table 8-26 for a description of the command parameters.

**Table 8-26 "config system" Command Parameters**

| Command | Format | Description |
|---|---|---|
| contact | String | Configure the system contact. Any ASCII characters are allowed, except for single and double quotes; double and single quotes may only be used as leading and tailing characters if the string has white space |
| description | String | Configure the system description. Any ASCII characters are allowed, except for single and double quotes; double and single quotes may only be used as leading and tailing characters if the string has white space |
| location | String | Configure the system location. Any ASCII characters are allowed, except for single and double quotes; double and single quotes may only be used as leading and tailing characters if the string has white space |

Octane 3.0 User Guide

**Table 8-26 "config system" Command Parameters (Continued)**

| Command | Format | Description |
| --- | --- | --- |
| name | String | Configure the system name. Any ASCII characters are allowed, except for single and double quotes; double and single quotes may only be used as leading and tailing characters if the string has white space |
| time | MMDDhhmmCCYY<br>MM.DD-hh:mm:ss<br>CCYY.MM.DD-hh:mm:ss<br>CCYY.MM.DD-hh:mm<br>hh:mm:ss<br>hh:mm | Configure the system time. Time must be entered in one of the given formats |

**Important** The command to set time will be rejected if the reader is using NTP server(s) to set system time. In this case, the command response will be:

```
Status=4,'Parameter-Dependency-Error'
```

In order to use this command to set system time, the user must remove any statically configured NTP server(s) and set the DHCP server configuration to NOT offer the NTP server option to the reader.

A sample **config system** command is shown below:

```
config system > location 'a specific location identifier'
Status=0,'Success'
sysDesc="Impinj Speedway"
sysContact="http://www.supplier.com/techsupport"
sysName="speedway-00-00-06"
sysLocation="a specific location identifier"
time="Tue Apr 25 03:59:00 UTC 2006"
```

A sample command that sets **time** is shown below: (Time is set to April, 27th 1:11:00 p.m. 2006.)

```
> config system time 042713112006

Status=0,'Success'
sysDesc="Impinj Speedway"
sysContact="http://www.supplier.com/techsupport"
sysName="speedway-00-00-06"
sysLocation="a specific location identifier"
time="Thu Apr 27 13:11:00 UTC 2006"
```

# 8.6 Show Command

The **show** command has seven submenus, as shown in Table 8-27, and described in the succeeding sections.

**Table 8-27 "show" Command Parameters**

| Command | Description |
| --- | --- |
| access | displays a list of the configured user accounts showing the account name and the access level (root, operator, or monitor) for each account. Also displayed are the name and access level of the current user. |
| all | leads to submenu of multi-category info display commands |
| image | leads to submenu of image status commands |
| logging | leads to submenu of logging status commands |
| network | leads to submenu of network status commands |
| rfid | leads to submenu of RFID status commands |
| snmp | leads to sbumenu of SNMP status commands |
| system | leads to submenu of system status commands |

## 8.6.1 show access Command

An example **show access** command is given below where two users have been added, one at operator level and one at monitor level.

```
 > show access
Status=0,'Success'
CurrentUser=root
CurrentLevel=root
UserName_1=root
AccessLevel_1=root
UserName_2=Opuser1
AccessLevel_2=operator
UserName_3=Monuser1
AccessLevel_3=monitor
```

## 8.6.2 show all Command

The **show all** menu has one subcommand, **config**, that elicits a summary of the static configuration entries of all categories. The static configuration entries are those that are manually set via CLI commands. The entries that are obtained via such protocols as DHCP are considered dynamic and

are not displayed. The response of the command is the concatenation of all the static entries from the following four categories: network, system information, upgrade agent, and logging. Each category is preceded with a delimiter field. The entire collection of possible parameters is listed in Table 8-28. Note that some parameters are present only when set and applicable.

**Table 8-28 "show all config" Response Parameters**

| Argument | Format | Description |
| --- | --- | --- |
| ConfigCategory | Network | Delimits the network category |
| Domain<n>Stat | String | The nth statically set domain; n starts with 1 |
| dnsServerAddress<n>Stat | IP Address | The $n$th static DNS server address. $n$ starts with 1. |
| NtpServerAddress<n>Stat | IP Address | The $n$th static NTP server address, $n$ starts with 1. |
| IpAddressMode | dynamic \| static | The IP address mode. Dynamic means DHCP is used to obtain IP address. |
| IpAddress | IP Address | The IP address of the reader's Ethernet interface. Present only if ipAddressMode is static. |
| IpMask | IP Address | The IP subnet mask of the Ethernet interface. Present only if ipAddressMode is static. |
| GatewayAddress | IP Address | The default gateway IP address of the Ethernet interface. Present only if the ipAddressMode is static. |
| BroadcastAddress | IP Address | The broadcast address of the Ethernet interface. Present only if the ipAddressMode is static. |
| Hostname | String | The hostname of the reader |
| llaStatus | enable \| disable | The link local address (LLA) status |

**Table 8-28 "show all config" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| sendHostname | on \| off | Indicates if the "send hostname" option of DHCP client configuration is turned on |
| userclass | String | Displays the user-class option of the DHCP client configuration. String is empty if this option is not set. |
| mDNSStatus | enabled \| disabled | Indicates whether the zeroconf features supported with mDNS are enabled |
| rfidServiceDiscovery | enabled \| disabled | Indicates whether the RFID service discovery feature is enabled |
| llrpServiceDiscovery | enabled \| disabled | Indicates whether the LLRP service discovery feature is enabled |
| httpServiceDiscovery | enabled \| disabled | Indicates whether the HTTP service discovery is enabled. |
| ConfigCategory | RFID | Delimits the RFID configuration category |
| LLRP1ClientAdminState | enabled \| disabled | Indicates whether the client initiated (inbound) LLRP connection is supported |
| LLRPInboundTCPPort | Integer | The port number to listen on for inbound LLRP connection |
| LLRP1ReaderAdminState | enabled \| disabled | Indicates whether the reader-initiated (outbound) LLRP connection is supported |
| LLRPOutboundRetrySec | Integer | Retry period of outbound LLRP connection in seconds |
| LLRPOutboundTimeout-Sec | Integer | Timeout of outbound LLRP connection in seconds |

**Table 8-28 "show all config" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| LLRPOutboundServer<n> | String | The server and port number for outbound LLRP connection. <n> is the index. The value is a string in the form of <server-host>:<port> |
| Mach1ExtAdminState | enabled \| disabled | Indicates whether the external Mach1 connection (inbound) is supported |
| Mach1InboundTCPPort | Integer | The port number to listen on for inbound Mach1 connection |
| ConfigCategory | SNMP | Delimits the SNMP configuration category |
| SnmpServiceStatus | enabled \| disabled | The status of SNMP service |
| ROCommunity | String | The RO community string |
| RWCommunity | String | The RW community string |
| WriteEnabled=true | enabled \| disabled | Indicates whether the SNMP write is enabled |
| NonRfidTrapEnabled | true \| false | Indicates whether non-RFID traps are enabled |
| TrapReceiver | String | Trap receiver(s) currently configured. <n> is an index starting from 0. The value is a string in the form of '<host>:<port> < community>' where <host> is the receiver's hostname or IP address, <port> is the port number and <community> is the community string |
| TrapLogEnabled | true \| false | Indicates whether logging of traps is enabled |
| TrapLogLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The log level of the non-RFID traps |

**Table 8-28 "show all config" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| epcgRmMibRevision | String | The EPCglobal Reader management MIB revision, e.g., 200703080000Z |
| epcgRdrDevDescription | DisplayString | Reader description |
| epcgRderDevRole | DisplayString | Device role |
| epcgRderDevOperStateEnable | true \| false | Controls whether device operational state trap is enabled |
| epcgNotifChanName<n> | DisplayString | Notification channel name, where <n> is the index starting with 1 |
| epcgRdrDevOperNotifStateLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The severity level of epcgRdrDevOperNotifState trap |
| epcgReadPointOperStateNotifyEnable | true \| false | Indicates whether epcgReadPointOperStateNotify trap is enabled |
| epcgReadPointOperNotifyStateLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The severity level of epcgReadPointOperNotifyState trap |
| epcgSrcOperStatusNotifEnable | true \| false | Indicates whether epcgSrcOperStatusNotif trap is enabled |
| epcgSrcOperStatusNotifyLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The severity level of epcgSrcOperStatusNotify trap |
| epcgNotifChanOperNotifEnable | true \| false | Indicates whether epcgNotifChanOperNotif trap is enabled |
| epcgNotifChanOperNotifLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The severity level of epcgNotifChanOperNotif trap |
| ConfigCategory | SystemInfo | Delimits the system info category |
| SysDesc | String | The system description |

**Table 8-28 "show all config" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| SysContact | String | The system contact |
| SysName | String | The system name |
| SysLocation | String | The system location |
| SysTime | String | A time in UTC |
| ConfigCategory | UpgradeAgent | Delimits the upgrade agent category |
| MetafileUri | String | The URI of the upgrade metafile |
| RetrieveMode | pull \| push | The upgrade agent's metafile retrieve mode |
| RetrievePeriod | Integer | The retrieve-period in minutes. Present only if the RetrieveMode is pull. |
| ConfigCategory | Logging | Delimits the logging category |
| ApplicationLevel | Emergency\| Alert \| Critical \| Warning \| Notice \| Info \| Debug | The individual component's internal logging level, as returned by the "show logging summary" command. |
| ConfigurationLevel | | |
| MgmtLevel | | |
| NetworkLevel | | |
| RFIDParameters | | |
| RFIDSingulation | | |
| RFIDAccess | | |
| System | | |

**Table 8-28 "show all config" Response Parameters (Continued)**

| Argument | Format | Description |
|----------|--------|-------------|
| SeverityLevel | Same as above | The syslog logging severity level as set by the "config logging syslog level" command. This determines what will be passed from internal to syslog logs (see Section 8.5.3) |
| SyslogServerAddress1 | IP Address or host-name String | The first syslog server as set by the "config logging syslog add" command. |
| … | … | … |
| SyslogServerAddress<N> | IP Address or host-name String | The last syslog server as set by the "config logging syslog add" command. |

```
show all > config
Status=0,'success'
ConfigCategory=Network
domainStatic=
ipAddressMode=dynamic
hostname=speedway-00-02-01
sendHostname=on
userClass=''
ConfigCategory=SNMP
SnmpServiceStatus=enabled
ROCommunity='public'
RWCommunity='private'
WriteEnabled=true
NonRfidTrapEnabled=false
TrapReceiver0='sqa:162 public'
TrapLogEnabled=true
TrapLogLevel=error
epcgRmMibRevision='200703080000Z'
epcgRdrDevDescription='IMPINJ Speedway'
epcgRdrDevRole='My reader role '
epcgNotifChanName1='Mach1 Internal'
epcgNotifChanName2='Mach1 External'
epcgNotifChanName3='LLRP Client'
epcgNotifChanName4='LLRP Reader '
epcgRdrDevOperNotifStateLevel=error
epcgReadPointOperStateNotifyEnable=true
epcgReadPointOperNotifyStateLevel=error
epcgSrcOperStatusNotifEnable=true
epcgSrcOperStatusNotifyLevel=error
```

```
epcgNotifChanOperNotifEnable=true
epcgNotifChanOperNotifLevel=error

ConfigCategory=SystemInfo
sysDesc='Impinj Speedway'
sysContact='unknown'
sysName='speedway-00-02-01'
sysLocation='unknown'
sysTime='Mon Aug 14 20:38:00 UTC 2006'

ConfigCategory=UpgradeAgent
MetafileUri=' '
RetrieveMode=push

ConfigCategory=Logging
ApplicationLevel=emergency
ConfigurationLevel=emergency
MgmtLevel=emergency
NetworkLevel=emergency
RFIDParameters=emergency
RFIDSingulation=emergency
RFIDAccess=emergency
System=emergency
```

## 8.6.3 show image Command

The **show image** command has two subcommands, **metafile** and **summary**. The **show image metafile** command displays the information for the current upgrade metafile. If no metafile has ever been successfully downloaded, only the first two fields are available. The **show image metafile** command response parameters are shown in Table 8-29. The **show image summary** command specifies the image summary information, with all response parameters defined in Table 8-30. Following an upgrade command, **UpgradeStatus** can take any of the values shown in Table 8-30. For each abnormal status, a Reason parameter is given to indicate the reason for the status. The reason values are also given in Table 8-30

### Table 8-29 "show image metafile" Response Parameters

| Argument | Format | Description |
|----------|--------|-------------|
| MetafileUri | String | The current upgrade metafile URI |
| Retrieve-Mode | pull \| push | The current retrieve mode |
| RetrievePe-riod | Integer | The current retrieve period, present only if retrieve mode is pull. This period is specified in seconds. |
| Upgrade-Mode | auto \| force | The upgrade mode if metafile is currently available |

**Table 8-29 "show image metafile" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| CommitMode | immediate \| scheduled \| wait-4-cmd | The commit mode if metafile is currently available |
| CommitTime | String | The schedule commit time, present only if commit mode is scheduled. Its format is \<timezone-yyyy-mm-dd-hh-mm-ss\>, where time zone is the readers time which is gmt. |
| EarlyActiva-teOk | yes \| no | Indicates whether an early activation of the upgrade image is valid when the commit is scheduled. Present only if the metafile has the early-act-ok field. |
| UpgFileUri | String | The upgrade file URI, present if the current metafile is available and has the upgrade-file-uri field. |

```
> show image summary
Status=0,'Success'
UpgradeStatus=Download Failed
Reason=File Not Found
DownloadFile=Upgrade Image
primaryImageType=2
primaryImageSystemVersion='2.0.1.240'
primaryImageConfigVersion='255.255.255.255'
secondaryImageType=2
secondaryImageSystemVersion='2.0.1.48'
secondaryImageConfigVersion='255.255.255.255'
```

**Table 8-30 "show image summary" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| UpgradeStatus | | The upgrade status of the last executed upgrade |
| | Idle \| | The reader is idle in terms of upgrade. |
| | Contacting Server | Reader is contacting server for file download. |
| | Downloading | File is being downloaded. |
| | Download Failed | Failed to download either the meta-file or the upgrade image. |
| | Bad Config | The upgrade configuration metafile is invalid. |
| | Bad Image | The image downloaded is invalid. |
| | No Upgrade | No need to upgrade |
| | Erasing | Reader is erasing flash memory before writing new image. |
| | Programming | Reader is programming new image into flash memory. |
| | Done | Upgrade is complete. |
| | Set Metafile Failed | The configureUri command failed. |
| | Set Upgrade Failed | The updateUri command failed. |
| | FDR Failed | The factory command failed. |
| | Set Retrieve-Mode Failed | The retrievemode command failed. |

**Table 8-30 "show image summary" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| UpgradeStatus, continued | Failed | Any other failures not covered above. Usually explained by Reason field |
| Reason | | This supplements the UpgradeStatus field to give a reason for the status |
| | Unknown Host | Download failed because of an unknown host. |
| | Unsupported Scheme | Download failed because of unsupported URI scheme (only FTP, HTTP and TFTP are supported). |
| | Syntax Error | Metafile has a syntax error. |
| | Timeout | Download timed out. |
| | File Not Found | Download file not found. |
| | Access Denied | Download failed because of access denied by server, e.g., bad password. |
| | Not Matching Metafile | Bad upgrade image because it did not match the metafile. |
| | Bad File Format | Bad upgrade image file format. |
| | Bad CRC | Bad image CRC. |
| | Bad Hw Version | Image Hw version does not match the reader. |
| | No Newer Version | Upgrade not needed because no newer version in the metafile or upgrade image. |
| | File Mismatch | Metafile has mismatched partition image types. |
| | No File | Metafile does not contain upgrade file information. |

**Table 8-30 "show image summary" Response Parameters (Continued)**

| Argument | Format | Description |
| --- | --- | --- |
| Reason, continued | Missing SOP | Metafile does not contain SOP partition while SCP is present. |
| | Duplicated Partition | Upgrade failed because either the metafile or the upgrade file has a duplicated partition in it. |
| | Incompatible Upgrade/Downgrade Path | Upgrade failed because upgrading/downgrading to the intended SOP version or type is not allowed by current image. |
| | Flash Programming Failed | Failed to write the flash memory. |
| | Current Image Invalidated | The current image has been invalidated by a previous "fallback" command. |
| | No Fallback Image Available | This reason applies to the rejection of multiple commands following a "fallback" command. |
| | Generic Error | Download error other than those specified above. |
| PrimaryImageType | String | The type of image stored in the primary partition (currently defaults to Linux) |
| PrimaryImageSystemVersion | String | The version string of the primary image system partition |
| PrimaryImageConfigVersion | String | The version string of the primary image configuration partition |
| SecondaryImageType | String | The type of image stored in the secondary partition (currently defaults to Linux) |
| secondaryImageSystemVersion | String | The version string of the secondary image system partition |

**Table 8-30 "show image summary" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| secondaryImageConfig-Version | String | The version string of the secondary image configuration partition |

## 8.6.4 show logging Command

The **show logging** command is used to display the logging parameters for the system and for displaying the log information in text form. The commands are described in Table 8-31. Log entries are reported from most recent to oldest. Response parameters for the **show logging <syslog|internal-log>** are shown in Table 8-32. Response parameters for the logging summary command are shown in Table 8-33.

**Table 8-31 "show logging" Command Parameters**

| Command | Argument | Format | Description |
|---|---|---|---|
| internallog | eventcount | Integer | Uses the eventcount number to determine how many of the last internal log entries to display. |
| summary | | | Displays the current logging configuration for the internal log and the syslog security level. See Section 8.5.3 for details on what the system will forward from internal log to syslog. |
| syslog | | | Uses the eventcount number to specify how many log entries to display. |

**Table 8-32 "show logging <syslog | internallog>" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| EventN | String | The string responses from the log events |
| EventN-1 | String | |
| … | … | … |
| Event1 | String | |

An example show logging internallog command is shown below:

```
> show logging internallog 1
Status=0,'Success'
Event1=1156073965.245217 -- UpgradeAgent          LAPI
Logging service started at: Sun Aug 20 11:39:25 2006
>
```

**Table 8-33 "show logging summary" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| ApplicationLevel | Emergency\| Alert \| Critical \| Error \| Warning \| Notice \| Info \| Debug | The level at and above which application-level logs are sent to the log database |
| ConfigurationLevel | | Log level for configuration |
| MgmtLevel | | Log level for management |
| NetworkLevel | | Log level for networking |
| RFIDParameters | | Log level for RFID parameters |
| RFIDSingulation | | Log level for RFID singulation |
| RFIDAccess | | Log level for RFID access |
| System | | Log level for system |
| severityLevel | | The syslog security level. Only logs at or above this level will be forwarded to syslog. |

Samples of the commands are shown below:

```
> show logging summary
Status=0,'Success'
ApplicationLevel=critical
ConfigurationLevel=emergency
MgmtLevel=emergency
NetworkLevel=emergency
RFIDParameters=emergency
RFIDSingulation=emergency
RFIDAccess=emergency
System=emergency
severityLevel=warning
>

> show logging syslog 3
```

```
Status=0,'Success'
Event3=Aug 20 11:39:25 (none) ntpd[625]: bind() fd 4, family 2,
port 123, addr 10.0.10.231, in_classd=0 flags=1 fails: Address
already in use
Event2=Aug 20 11:39:26 (none) thttpd[631]: socket :: - Address
family not supported by protocol
Event1=Aug 20 11:39:54 (none) dhclient: receive_packet failed on
ixp0: Network is down
```

## 8.6.5 show network Command

The **show network** menu contains commands to display networking parameters and statistics. All commands are single word commands and take no arguments. Commands are shown in Table 8-34, while the response parameters are shown in Table 8-35 through Table 8-46.

**Table 8-34 "show network" Command Parameters**

| Command | Description |
|---------|-------------|
| dhcp | Summary of DHCP Client configuration. |
| dns | Summary of DNS settings. |
| dnssd | Summary of DNS-SD settings. |
| icmp | ICMP statistics |
| iface | Interface status |
| ip | IP statistics |
| mdns | Summary of mDNS settings |
| ntp | Summary of NTP settings |
| summary | summary of network settings |
| tcp | tcp statistics |
| trace | status of current net trace activity |
| udp | udp statistics |

**Table 8-35 "show network dhcp" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| sendHostname | on\|off | Indicates the current setting for sending the host-name during DHCP negotiation. |
| UserClass | String | Displays the current setting for the user class DHCP option. If this string is empty, the user class option is not sent via DHCP. Otherwise the value indicates the string that is sent. |

**Table 8-36 "show network dns" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| DomainStatic | String | Statically configured domain, if available |
| domainDynamic | String | DNS domain obtained from DHCP, if available |
| dnsServerAddress1Stat | IPAddress | Address of first static DNS server |
| dnsServerAddress2Stat | IPAddress | Address of second statically added DNS server |
| … | … | … |
| dnsServerAddress<N>Stat | IPAddress | Address of last statically added DNS server |
| dnsServerAddress1Dyn | IPAddress | Address of first dynamic DNS server obtained from DHCP server |
| … | … | … |
| dnsServerAddress<N>Dyn | IPAddress | Address of last dynamic DNS server obtained from DHCP server |

**Table 8-37 "show network dnssd" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| rfidService-Discovery | String | "enabled" (RFID service announcement is enabled) |
| | | "disabled" (RFID service announcement is disabled) |
| llrpService-Discovery | String | "enabled" (LLRP service announcement is enabled) |
| | | "disabled" (LLRP service announcement is disabled) |
| httpService-Discovery | String | "enabled" (HTTP service announcement is enabled) |
| | | "disabled" (HTTP service announcement is disabled) |

**Table 8-38 "show network icmp" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| icmpInMsgs | Counter | See MIB-2 RFC 1213 |
| icmpInErrors | Counter | |
| icmpInDestUnreachs | Counter | |
| icmpInTimeExcds | Counter | |
| icmpInParmProbs | Counter | |
| icmpInSrcQuenchs | Counter | |
| icmpInRedirects | Counter | |
| icmpInEchos | Counter | |
| icmpInEchoReps | Counter | |
| icmpInTimestamps | Counter | |
| icmpInTimestampReps | Counter | |

**Table 8-38 "show network icmp" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| icmpInAddrMasks | Counter | |
| icmpInAddrMaskReps | Counter | |
| icmpOutMsgs | Counter | |
| icmpOutErrors | Counter | |
| icmpOutDestUnreachs | Counter | |
| icmpOutTimeExcds | Counter | |
| icmpOutParmProbs | Counter | |
| icmpOutSrcQuenchs | Counter | |
| icmpOutRedirects | Counter | |
| icmpOutEchos | Counter | |
| icmpOutEchoReps | Counter | |
| icmpOutTimestamps | Counter | |
| icmpOutTimestampReps | Counter | |
| icmpOutAddrMasks | Counter | |
| icmpOutAddrMaskReps | Counter | |

**Table 8-39 "show network iface" Response Parameters**

| Argument | format | Description |
|---|---|---|
| IfIface | String | Interface Name |
| IfMTU | Integer | Maximum Transfer Unit Size |
| IfMet | Integer | Interface Metric |

**Table 8-39 "show network iface" Response Parameters (Continued)**

| Argument | format | Description |
|---|---|---|
| ifRX-OK | Integer | Successful Receive Frames |
| ifRX-ERR | Integer | Errored Receive Frames |
| ifRF-DRP | Integer | Dropped Receive Frames |
| ifRF-OVR | Integer | Receiver Overruns |
| ifTX-OK | Integer | Successful Transmit Frames |
| ifTX-ERR | Integer | Errored Transmit Frames |
| ifTx-DRP | Integer | Dropped Transmit Frames |
| ifTx-OVR | Integer | Transmitter Overruns |
| IfFlg | String | B--Broadcast address has been set<br>L--This interface is a loopback device<br>M--All packets are received (promiscuous mode)<br>O--ARP is turned off for this interface<br>P--This is a point-to-point connection<br>R--Interface is running<br>U--Interface is up |

**Table 8-40 "show network ip" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| ipForwarding | Integer | See MIB-2 RFC 1213 |
| ipDefaultTTL | Integer | |
| ipInReceives | Counter | |
| IpInHdrErrors | Counter | |
| ipInAddrErrors | Counter | |
| ipForwDatagrams | Counter | |

Octane 3.0 User Guide

**Table 8-40 "show network ip" Response Parameters** (Continued)

| Argument | Format | Description |
|---|---|---|
| ipInUnknownProtos | Counter | |
| ipInDiscards | Counter | |
| ipInDelivers | Counter | |
| ipOutRequests | Counter | |
| ipOutDiscards | Counter | |
| ipOutNoRoutes | Counter | |
| ipReasmTimeout | Integer | |
| ipReasmReqds | Counter | |
| IpReasmOKs | Counter | |
| IpReasmFails | Counter | |
| ipFragOKs | Counter | |
| ipFragFails | Counter | |
| ipFragCreates | Counter | |
| IpRoutingDiscards | Counter | |

**Table 8-41 "show network mdns" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| mDNSStatus | String | "enabled" (multicast DNS protocol is enabled) |
| | | "disabled" (multicast DNS protocol is disabled) |

Copyright © 2008, Impinj, Inc.

**Table 8-42 "show network ntp" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| NtpServerAddress1Stat | String | Hostname or IP address of the first statically added NTP server |
| NtpServer1State | Synchronized \| Polled \| SymmetricActive \| SymmetricPassive \| ReceivingBroadcast \| SendingBroadcast | The current state of the server[a] |
| NtpServer1Stratum | Integer | The stratum number of the server |
| NtpServer1Reach | Octal integer | The reachability register of the server |
| … | … | … |
| NtpServerAd-dress<N>Stat | String | Hostname or IP address of the last statically added NTP server |
| NtpServerAddress1Dyn | String | Address of the first NTP server obtained from DHCP server |
| NtpServer1DynState | Synchronized \| Polled \| SymmetricActive \| SymmetricPassive \| ReceivingBroadcast \| SendingBroadcast | The current state of the first dynamic NTP server. (When the reader is trying to use a server, it will remain in the state, "Polled," until it has suc-cessfully communicated with the server eight times. During this process, the "NtpServerN-DynReach parameter will gen-erally transition through 1, 3, 7, 37, 77, 177, and 377. When the reader has selected a server and locked on, the state parameter will become "Synchronized." |
| NtpServer1DynStratum | Integer | The current stratum number of the first NTP server |

**Table 8-42 "show network ntp" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| NtpServer1DynReach | Octal integer | The reachability register of the first NTP server |
| … | … | … |
| NtpServerAd-dress<N>Dyn | String | Address of the last NTP server obtained from DHCP server |

a. For details in NTP server state, stratum and reachability register, see NTP protocol (RFC1305)

**Table 8-43 "show network summary" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| ipAddressMode | String | If configuration is currently dynamic, the dynamic values returned by DHCP are given |
| ipAddress | ipAddress | |
| IpMask | ipAddress | |
| gatewayAddress | ipAddress | |
| broadcastAddress | ipAddress | |
| hostname | String | |
| llaStatus | String | Indicates whether link-local access feature is enabled or disabled |

**Table 8-44 "show network tcp" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| tcpRtoAlgorithm | Integer | See MIB-2 RFC 1213 |
| tcpRtoMin | Integer | |
| tcpRtoMax | Integer | |

**Table 8-44 "show network tcp" Response Parameters (Continued)**

| Argument | Format | Description |
|----------|--------|-------------|
| tcpMaxConn | Integer | |
| tcpActiveOpens | Counter | |
| tcpPassiveOpens | Counter | |
| tcpAttemptFails | Counter | |
| tcpEstabResets | Counter | |
| tcpCurrEstab | Gauge | |
| tcpInSegs | Counter | |
| tcpOutSegs | Counter | |
| tcpRetransSegs | Counter | |
| tcpInErrs | Counter | |
| tcpOutRsts | Counter | |

**Table 8-45 "show network udp" Response Parameters**

| Argument | Format | Description |
|----------|--------|-------------|
| udpInDatagrams | Counter | See MIB-2 RFC 1213 |
| udpNoPorts | Counter | |
| udpInErrors | Counter | |
| udpOutDatagrams | Counter | |

**Table 8-46 "show network trace" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| Active | String | "Yes" or "No," to indicate if a net trace is currently active. |

## 8.6.6 show rfid Command

The **show rfid** menu contains commands to display RFID parameters and statistics. Submenu commands are shown in Table 8-47.

**Table 8-47 "show rfid" Command Parameters**

| Command | Description |
|---|---|
| stat | Display RFID statistics for reader. |
| llrp | Leads to submenu of LLRP status statistics |
| mach1 | Leads to a submenu of Mach1 status statistics |

### 8.6.6.1 show rfid stat

The **show rfid stat** command displays the RFID statistics for that reader.

**Table 8-48 "show rfid stat" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| LastStatisticReset | Integer | The last time the statistical count was reset, in seconds |
| Antenna<n>EnergizedTime | Integer | Time Antenna <n> has been powered, in milliseconds; <n> is 1–4 |
| ReaderOperationalStatus | enabled \| disabled | Indicates whether RFID applications are running on the reader |
| ReaderAdministrativeStatus | enabled | Desired status by adminstration—always enabled |

Copyright © 2008, Impinj, Inc.

**Table 8-48 "show rfid stat" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| Antenna\<n>Operational-Status | enabled \| disabled \| unknown | Indicates if an antenna is physically connected to the reader and operating properly. If no RFID operation has been performed, and no in-band (Mach1 or LLRP) checks on antenna status have been performed, the reader will assign unknown to this statistic. Once an RFID operation has occurred, or an in-band check is performed, the reader will update the statistic.<br><br>Enabled=connected antenna; Disabled=disconnected from antenna.<br><br>Note that accurate reports are only available on in-use antennas. |
| Antenna\<n>AdministrativeStatus | enabled | Desired status of antenna by administration—always enabled; \<n> is 1–4 |
| Antenna\<n>LastPower-Level | Integer | 100 times the dBm setting of Antenna \<n>; \<n> is 1–4 |
| Antenna\<n>LastNoiseLevel | Integer | Always 0 |
| Antenna\<n>UniqueInventoryCount | Integer | Number of unique tags seen at Antenna \<n>; \<n> is 1–4 |
| Antenna\<n>TotalInventory-Count | Integer | Total Inventory Count for Antenna \<n>; \<n> is 1–4 |
| Antenna\<n>FailedInventoryCount | Integer | Always 0 |
| Antenna\<n>ReadCount | Integer | Number of tags read at Antenna \<n> that matched the configured filters; \<n> is 1–4 |
| Antenna\<n>FailedReadCount | Integer | Number of tags where a read was attempted at Antenna \<n> because the tag matched the configured filters, but the read failed; \<n> is 1–4 |
| Antenna\<n>WriteCount | Integer | Number of tags written at Antenna \<n> that matched the configured filters; \<n> is 1–4 |

**Table 8-48 "show rfid stat" Response Parameters (Continued)**

| Argument | Format | Description |
| --- | --- | --- |
| Antenna<n>FailedWrite-Count | Integer | Number of tags where a write was attempted at Antenna <n> because the tag matched the configured filters, but the write failed; <n> is 1–4 |
| Antenna<n>LockCount | Integer | Number of tags locked at Antenna <n> that matched the configured filters; <n> is 1–4 |
| Antenna<n>FailedLock-Count | Integer | Number of tags where a lock was attempted at Antenna <n> because the tag matched the configured filters, but the lock failed; <n> is 1–4 |
| Antenna<n>KillCount | Integer | Number of tags killed at Antenna <n> that matched the configured filters; <n> is 1–4 |
| Antenna<n>FailedKillCount | Integer | Number of tags where a kill was attempted at Antenna <n> because the tag matched the configured filters, but the kill failed; <n> is 1–4 |
| Antenna<n>EraseCount | Integer | Number of tags erased at Antenna <n> that matched the configured filters; <n> is 1–4 |
| Antenna<n>FailedEraseC-ount | Integer | Number of tags where a erase was attempted at Antenna <n> because the tag matched the configured filters, but the erase failed; <n> is 1–4 |
| Gpi<n>TransitionCount | Integer | Number of times a GPI event matched the configuration; <n> is 1–4 |

### 8.6.6.2 show rfid llrp Command

The **show rfid llrp** command provides statistics on the llrp interface and has the subcommands listed in Figure 8-49.

**Table 8-49 "show rfid llrp" Command Parameters**

| Command | Argument | Format | Description |
|---|---|---|---|
| accessspec | id | integer | Displays a specific AccessSpec |
| capabilities | | | Displays the LLRP capabilities. |
| config | | | Displays the LLRP configuration. |
| inbound | | | Displays the LLRP client-initiated connection settings |
| outbound | | | Displays the LLRP reader-initiated connection settings. |
| region | | | Displays information about the regulatory region where the reader may operate. Also will display sub-regulatory region information when configured by LLRP extensions |
| rospec | id | integer | Displays the in-band configuration items of the reader in XML format. |
| stat | | | Displays the LLRP statistics. |
| summary | | | Displays a summary of the LLRP information |

### 8.6.6.3 show rfid mach1 Command

The **show rfid mach1** command provides a submenu of Mach1 status commands as shown in Table 8-50.

**Table 8-50 "show rfid mach1" Command Parameters**

| Command | Description |
|---------|-------------|
| inbound | Displays the Mach1 external client-initiated connection settings |
| stat | Displays the Mach1 statistics |
| summary | Displays a summary of the Mach1 information |

## 8.6.7 show snmp Command

The show snmp command has submenu commands to display the SNMP configurations, as shown in Table 8-51. The response parameters for **show system summary** are shown in Table 8-52. The response parameters for **show system epcg** are shown in Table 8-53.

**Table 8-51 "show snmp" Command Parameters**

| Command | Description |
|---------|-------------|
| all | All SNMP settings |
| summary | summary of generic SNMP settings |
| epcg | EPCG RM specific settings |

**Table 8-52 "show snmp summary" Response Parameters**

| Argument | Format | Description |
|----------|--------|-------------|
| SnmpServiceStatus | enabled \| disabled | The status of SNMP service |
| ROCommunity | String | The RO community string |
| RWCommunity | String | The RW community string |

**Table 8-52 "show snmp summary" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| WriteEnabled=true | enabled \| disabled | Indicates whether SNMP write is enabled |
| NonRFIDTrapEnabled | true \| false | Indicates whether non RFID traps are enabled |
| TrapReceiver<n> | String | Trap receiver(s) currently configured. <n> is an index starting from 0. The value is a string in the form of '<host>:<port> <community>' where <host> is the receiver's hostname or IP address, <port> is the port number and <community> is the community string |
| TrapLogEnabled | true \| false | Indicates whether logging of traps is enabled |
| TrapLogLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The log level of the non-RFID traps |

**Table 8-53 "show snmp epcg" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| epcgRmMibRevision | String | The Epcglobal reader management MIB revision, e.g., 200703080000Z |
| epcgRdrDevDescription | DisplayString | Reader description |
| epcgRdrDevRole | DisplayString | Device role |
| epcgRdrDevOperNotif-StateLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The severity level of epcgRdrDevOperNotifState trap |
| epcgReadPointOper-StateNotifyEnable | true \| false | Indicates whether epcgReadPointOperStateNotify trap is enabled |

**Table 8-53 "show snmp epcg" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| epcgReadPointOperNo-tifyStateLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The severity level of epcgRead-PointOperNotifyState trap |
| epcgSrcOperStatusNo-tifEnable | true \| false | Indicates whether epcgSrcOper-StatusNotif trap is enabled |
| epcgSrcOperStatusNoti-fyLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The severity level of epcgSrcO-perStatusNotify trap |
| epcgNotifChanOperNo-tifEnable | true \| false | Indicates whether epcgNotifChan-OperNotif trap is enabled |
| epcgNotifChanOperNoti-fLevel | emergency \| alert \| critical \| warning \| notice \| info \| debug | The severity level of the epcgNo-tifChanOperNotif trap |

## 8.6.8 show system Command

The **show system** menu displays information on the system state of the reader. Table 8-54 provides a list of the available show system subcommands. Table 8-55 through Table 8-57 summarize the respective response parameters.

**Table 8-54 "show system" Command Parameters**

| Command | Description |
|---|---|
| cpu | Platform memory usage and available application space statistics |
| platform | Displays generic platform statistics |
| summary | Displays system information |

**Table 8-55 "show system cpu" Response Parameters**

| Argument | Format | Description |
|---|---|---|
| TotalMemory | Unsigned32 | Total available RAM in bytes |
| FreeMemory | Unsigned32 | Total free RAM in bytes |
| CpuUtilization | Unsigned32 | CPU utilization in percent |
| TotalConfigurationStorageSpace | Unsigned32 | Total configuration partition space in bytes |
| FreeConfigurationStorageSpace | Unsigned32 | Free configuration partition space in bytes |
| TotalApplicationStorageSpace | Unsigned32 | Total application partition space in bytes |
| FreeApplicationStorageSpace | Unsigned32 | Free application partition space in bytes |

**Table 8-56 "show system platform" Response Parameters**

| Argument | Format | Description |
|----------|--------|-------------|
| OTPVersion | String | Internal data version used for debugging |
| hardwareVersion | String | Returns the current hardware version information |
| serialNumber | String | Returns the hardware serial number |
| MacAddress | String | MAC Address of unit's Ethernet port |
| custID | String | Manufacturing routing data used by the factory |
| OSValid | String | Data field used to indicate OS/HW compatibility |
| regionsValid | Integer | Indicates the numerical values of the regions allowed on this hardware. This number matches the region number mapping as specified in Mach1 documentation |
| FeaturesValid | String | Indicates features enabled on this hardware version |
| BIOSVersion | String | Returns the version information for the reader BIOS |
| UptimeSeconds | Integer | Time since last reboot in seconds |

**Table 8-57 "show system summary" Response Parameters**

| Argument | Format | Description |
|----------|--------|-------------|
| SysDesc | String | A system description—defaults to make and model number of reader |
| SysContact | String | The system contact information—defaults to unknown |
| SysName | String | A system name—defaults to speedway-XX-XX-XX where XX-XX-XX are the last three octets of the MAC address. (See Section 4.) |

**Table 8-57 "show system summary" Response Parameters (Continued)**

| Argument | Format | Description |
|---|---|---|
| SysLocation | String | A system location—defaults to 'unknown' |
| SysTime | String | A time in UTC |

# 8.7 Transfer Command

The **transfer** command has two subcommands, as shown in Table 8-58.

**Table 8-58 "transfer" Command Parameters**

| Command | Description |
|---|---|
| from-reader | Transfer a file from the reader to a remote URI |
| status | Display status of currently active transfer |

The **transfer from-reader** command uploads files from the reader. The command requires two arguments: the first specifies the file to upload, the second specifies the URI destination for the file. The file upload options are **internallog** or **syslog**. The internallog and syslog options upload the internal log and syslog, respectively, to a file specified by the URI that must end in .txt.gz. The command usage is shown below:

```
Usage:  from-reader <internallog|syslog> <URI>
```

The following URI formats are accepted by this command:

```
tftp://<servername>/<directory>/<file>.txt.gz
ftp://<user>:<password>@<servername>/<directory>/<file>.txt.gz
```

A sample command is shown below:

```
> transfer from-reader syslog tftp://10.0.10.37/syslog.txt.gz
Status=0,'Success'
>
```

The **transfer status** command displays the current status of the transfer sub-system. The command response parameters are given in Table 8-59. This command takes no arguments.

**Table 8-59 "transfer status" Command Response**

| Argument | Format | Description |
|---|---|---|
| Transfer-Status | Unknown \| Contacting Server \| Transferring \| Transfer Failed \| Done> | The status of the transfer. Unknown means there is no outstanding transfer command. |
| Reason | Unknown Host \| Access Denied \| File Not Found \| Timeout \| Invalid URI Format \| Invalid URI Format (username:password@host) | Reason for failure of transfer. Note that when using TFTP to upload, the remote file may have to be already on the server with the right permission, otherwise transfer fails with reason "File Not Found" or "Access Denied". If the remote URI is invalid, transfer fails with reason "Invalid URI Format" and if FTP is used, the correct form is given in the Reason string. |

An example of a failed transfer has the following status response:

```
> transfer status
Status=0,'Success'
TransferStatus=Transfer Failed
Reason=Unknown Host
>
```

# 9 Troubleshooting

This section comprises a set of guidelines to enable the user to troubleshoot and isolate common configuration problems that may occur when using Speedway readers. It provides a series of basic tests that will enable the reader to either correct a problem with the Speedway reader, or determine that the reader must be returned for factory repair.

## 9.1 Test Instrumentation & Software Requirements

### 9.1.1 Power/Cabling

- 24V Power Adapter: CUI, Inc. P/N DSA-60W-20 1 24060
- 6 foot, RS-232 cable with DB-9 Male and Female connectors

### 9.1.2 Measurement Equipment and Accessories

- Reference antenna, Impinj Model Number IPJ-A0400-USA, CSL CS-777-2 (Brickyard) or equivalent
- Two or more UHF Gen 2 tags or labels.

### 9.1.3 Computer-related Equipment

- Microsoft Windows 2000 or XP compatible benchtop PC configured with DHCP server
- Two CAT5 Ethernet patch cables
- Ethernet router

### 9.1.4 Software

- Java Runtime Environment (JRE) of version 1.4.2 or later installed on computer. The latest version of JRE may be installed from: http://java.com/en/download/manual.jsp
- Bonjour for Windows v1.0.4 (or higher).  The latest version of Bonjour for Windows can be downloaded from: http://developer.apple.com/networking/bonjour/
- Reader terminal tool such as Hyperterm

## 9.2 Basic Test Setup

Figure 9-1shows the basic reader test configuration. A serial connector enables connection from the DB9 port on the computer to the serial port on the reader. If your computer does not have a DB9 port, you can obtain a USB-to-serial adaptor, which is commonly available at office supply or computer stores.

If you intend to operate the reader with DHCP configuration, it must be connected to a router. This configuration will provide a network address to the reader. For fixed IP address applications, a 4-port switch or crossover network cable must be used to connect to the reader.



**RF cable**

**Ethernet**

**Serial Cable**

**Ethernet**

PC
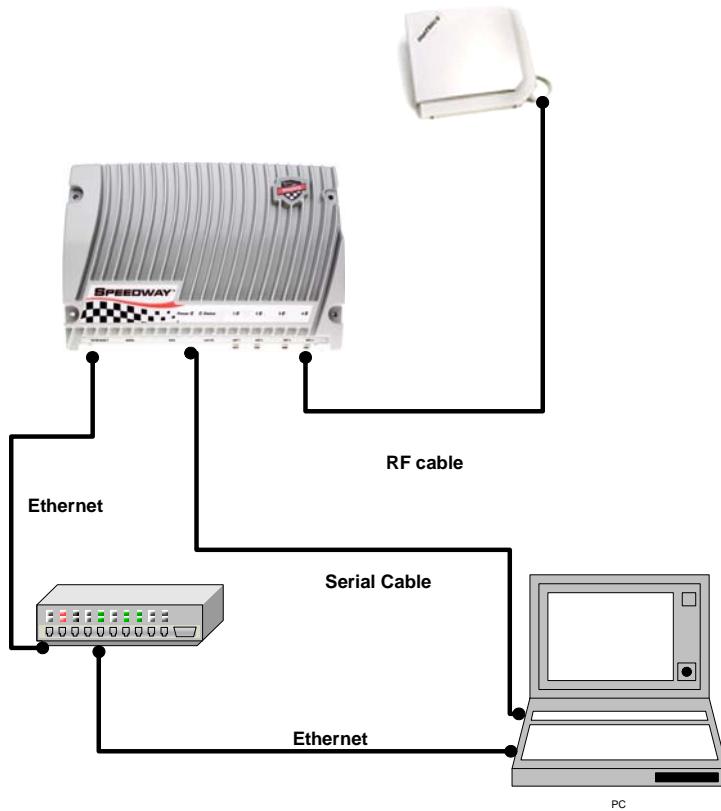
**Figure 9-1  Basic Reader Configuration**

## 9.3  Troubleshooting Flowcharts

To simplify the troubleshooting process, this guide will focus on four major areas:
  • Reader power up
  • Reader network communication
  • Running reader applications, including the factory-installed Java applet
  • RF-related issues including tag communication, antenna problems, and sensitivity issues.

## 9.3.1 Reader Power Up

The flow chart in Figure 9-2 shows the basic steps to verify that the reader powers up correctly. Following these steps will identify problems related to power supply, reader power connection, or possible circuit failure within the reader.
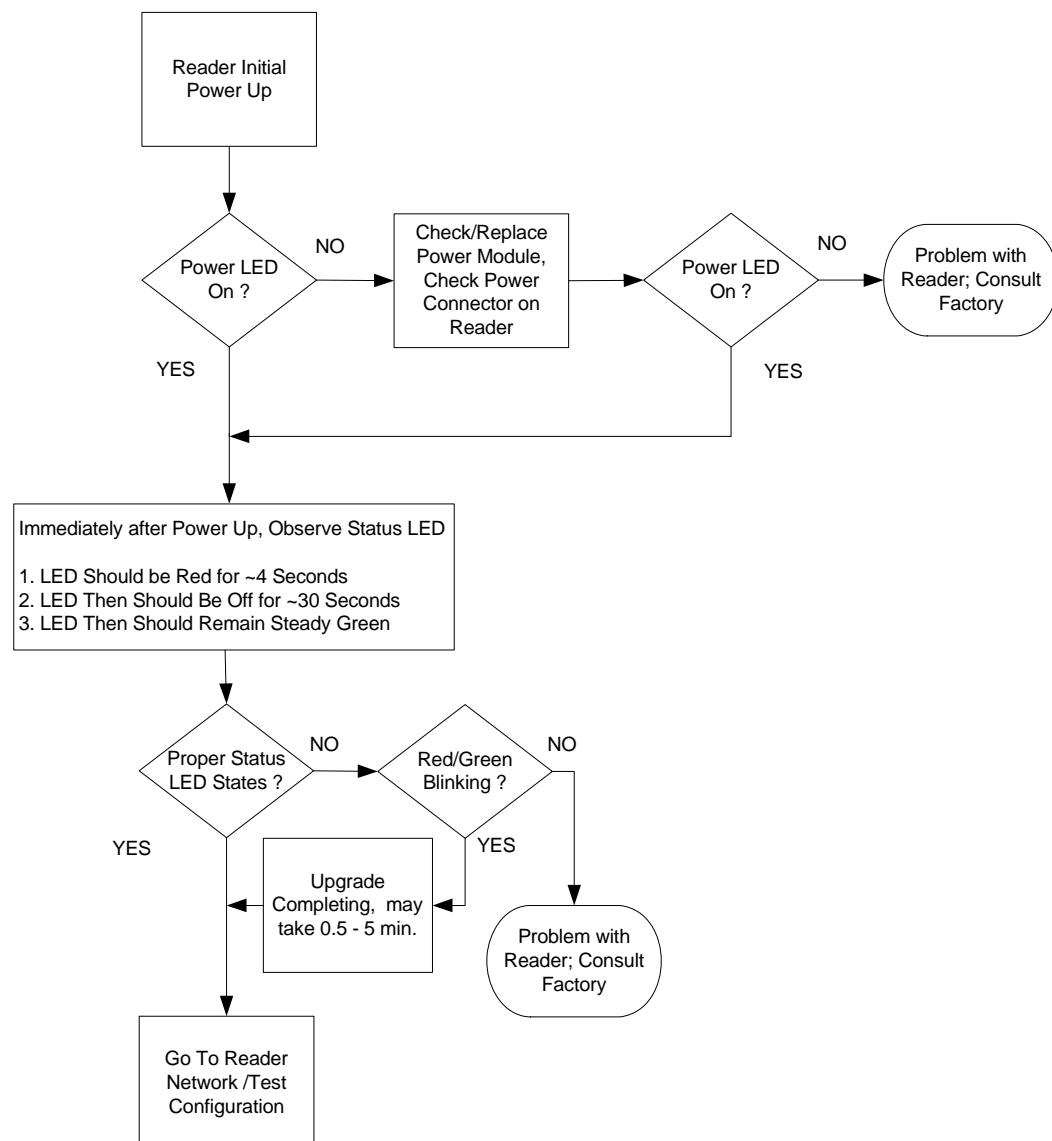
**Figure 9-2  Reader Initial Power Up**

## 9.3.2  Reader Network/Test Configuration

Section 9.3.2.1 through Section 9.3.2.4, and the flowchart in Figure 9-3 describe how to identify and reconfigure the reader network configuration. At the end of Section 9.3.2, you will have verified network connectivity and will have the reader's current IP address. This address is required to run reader application programs.

### 9.3.2.1 Reader Serial Configuration to Monitor and Configure Reader

1.  Configure the terminal tool to use on the laptop (hyperterminal or other) to control the serial port. The serial port configuration should be set to:
    *   Data rate: 115.2 kbps
    *   Data format: 8 bits, no parity, one stop bit
    *   Flow control: none

2.  Apply power and monitor the reader boot progress:
    *   Verify the status LED is providing the state of the boot operation (see Figure 9-1).
    *   Observe redboot providing information about its boot process on the terminal console.

(The reader has completed booting and is ready for configuration once the status light is solid green.)

**Notice** that the terminal program provides a login prompt:

```
Speedway-XX-XX-XX login:
```

where the XX-XX-XX are the last three bytes of the MAC address, printed on the Speedway reader label and expressed in hexadecimal. This naming convention is the Speedway factory default. If the name is different, the host name has been changed after shipment.

### 9.3.2.2  Identify Current Reader Network Parameters

**Login** to the reader via the serial port.

```
    Username: root
    Password: Impinj
```

**At the ">" command prompt type:**
```
        > show network summary
```

1.  If DHCP has been configured, the reader will respond a message similar to the example below:

```
Speedway-00-00-10 login: root
Password:
 > show network summary
Status=0,'Success'
ipAddressMode=dynamic
ipAddress=10.10.10.63
ipMask=255.255.0.0
gatewayAddress=10.10.0.1
broadcastAddress=10.10.255.255
hostname=Speedway-00-00-10
llaStatus=enabled
```

2.  If the current mode is fixed IP, the second line will indicate:
```
ipAddressMode=static
```

3. llaStatus should be enabled. (Enabling llaStatus provides an autonomous address mode if DHCP is not available.)
   - If llaStatus is not enabled, at the command line type:
     ```
     > config network lla enable
     ```
   - The reader will respond with:
     ```
     > Status=0,'Success'
     ```

4. Mdns must be enabled to use Bonjour (discussed later) for reader identification and communication
   - At the prompt, type:
     ```
     > config network mdns enable
     ```
   - The reader will respond with:
     ```
     Status=0,'Success'
     ```

5. If you are not satisfied with the current configuration, see Section 9.3.3, Section 9.3.2.3, and Section 9.3.2.4, which indicate how to reconfigure the network configuration.

### 9.3.2.3  Configuring Reader for Fixed IP Address

1. **Make sure** to use the same subnet as your laptop. For instance, if the laptop is configured on the 192.168.20 subnet, the following configuration could be used:
   ```
   > config network ip static 192.168.20.95
   192.168.255.255 192.168.20.1 192.168.20.255
   ```

2. **Verify** the network configuration.
   ```
   > show network summary
   ```

3. **Verify** access to the reader via Ethernet. Use either of the following methods:
   - SSH to the fixed IP address of the reader.
   - Start a command line on the laptop and ping the reader IP address.

4. Note the IP address for future reference.

### 9.3.2.4  Configuring the Reader for DHCP (Dynamic Addressing)

1. Type "config network ip dynamic." The reader will respond with 'Success'
   ```
   > config network ip dynamic
   Status=0,'Success'

   >
   ```
2. **Verify** the network configuration.
   ```
   > show network summary
   ```

3. **Verify** access to the reader via Ethernet. Use either of the following methods:
   - SSH to the fixed IP address of the reader.
   - Start a command line on the laptop and ping the reader IP address.

4. Note the IP address for future reference.
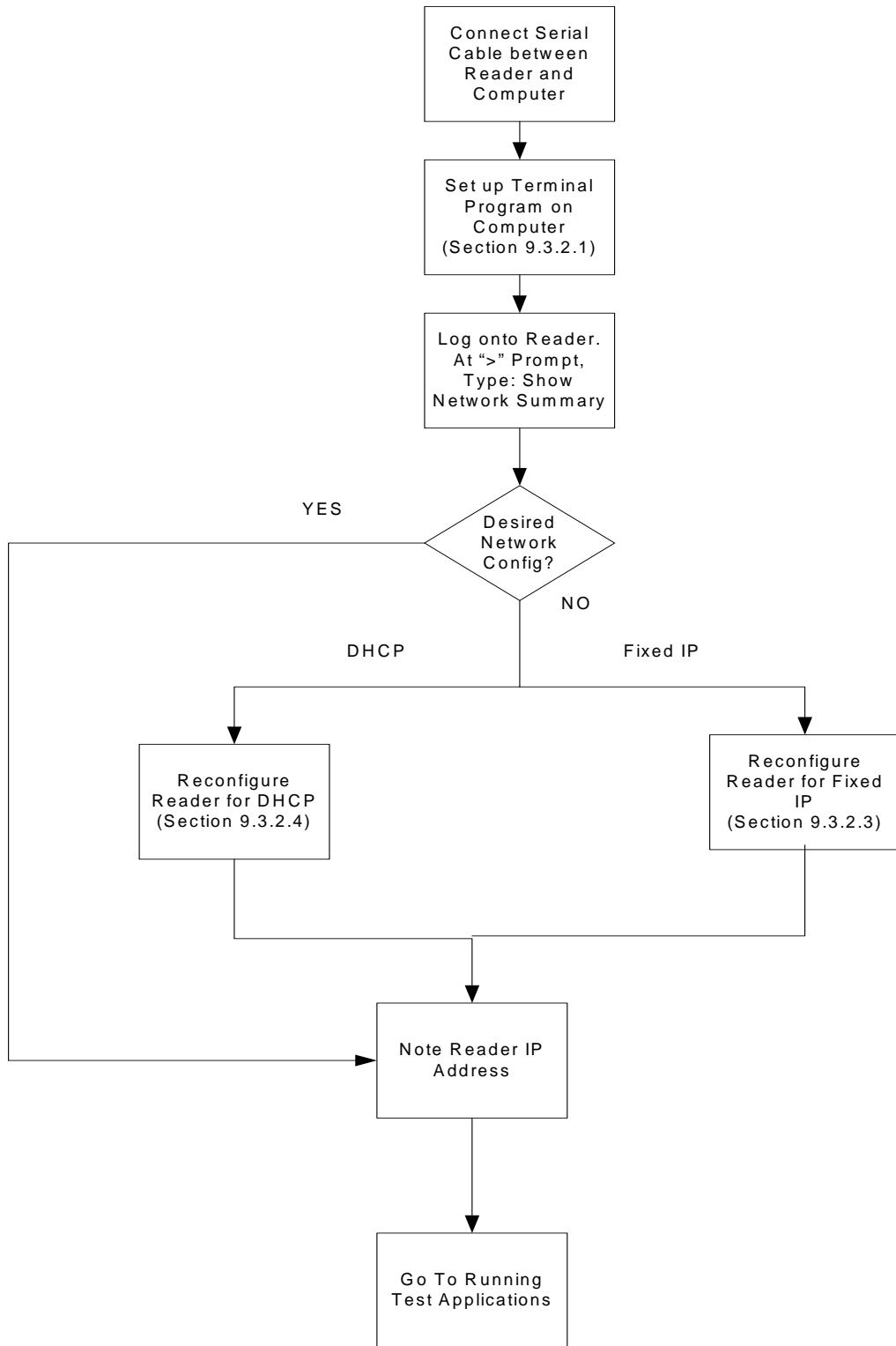
**Figure 9-3  Reader Network Configuration Flowchart**

### 9.3.3 Using Apple Bonjour to Find and Connect to Networked Reader

If the reader has been installed on a network, Bonjour can be used to find and connect to it. In order to use this application, the reader must have mdns and lla modes enabled (refer to Section 9.3.2.2).

After installing the Bonjour for Windows application, open a web browser. The Bonjour Icon, 🌀, should appear on the toolbar. Clicking this icon opens a new window on the browser that shows all Bonjour-enabled devices (mainly printers) and every Speedway reader currently on the network. Simply select the desired Speedway reader by clicking on its host name.

## 9.3.4 Reader Test Application

This section and the flowchart in Figure 9-4 describe how to run the internal reader test program. This program will be used to further test the reader.
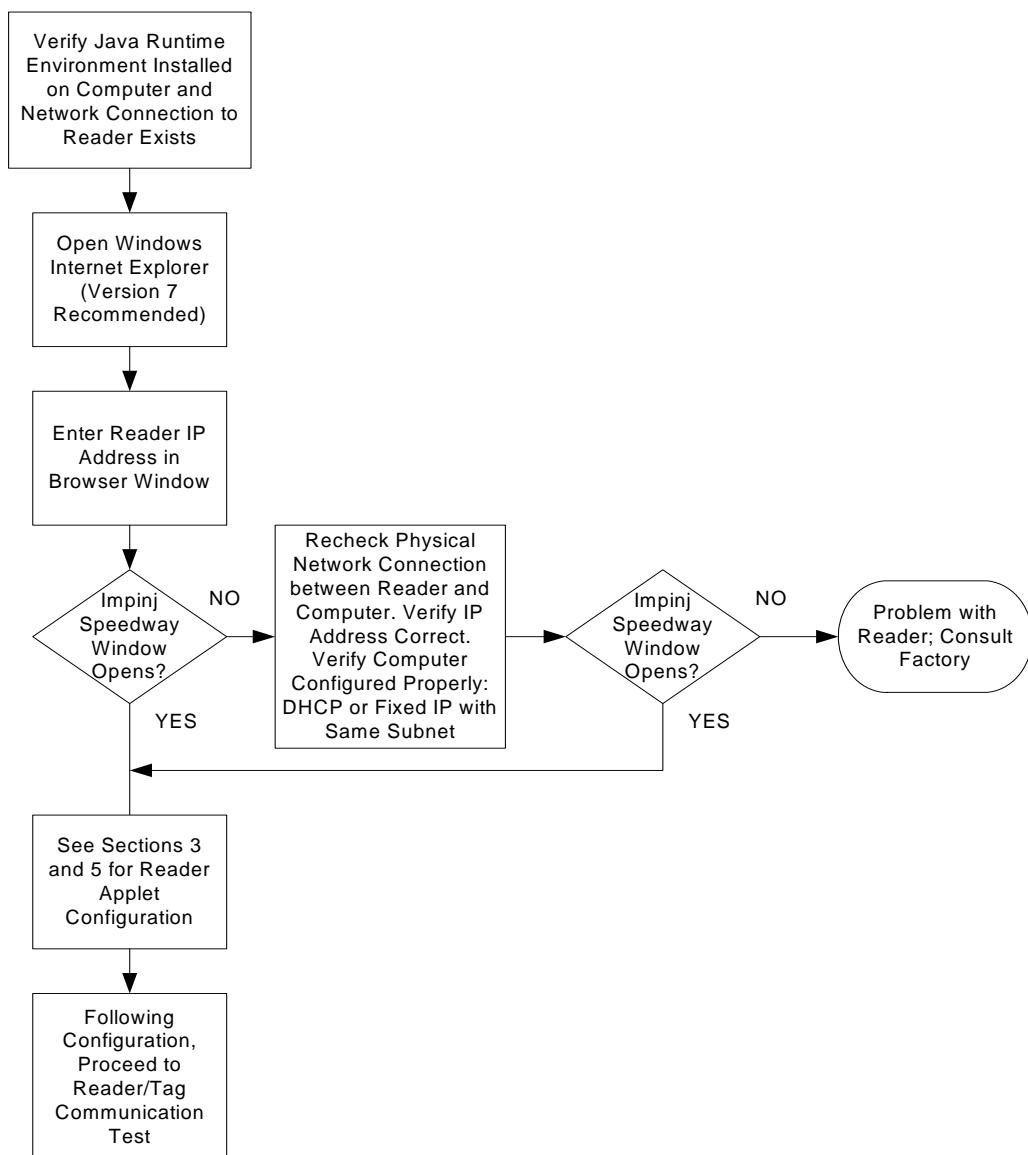


**Figure 9-4  Reader Application Flowchart**

### 9.3.4.1 Running the Application

After verifying that your computer has Java installed, open a Web browser (Microsoft Internet Explorer Version 7 is recommended) and enter the reader IP address (that you noted from Section 9.3.2.4) in the browser address window. The home page of the reader application should open on the computer. Follow the instructions in Section 3 and Section 5 to configure and operate the reader application.

### 9.3.4.2 Reader to Tag Communication Test

The flowchart in Figure 9-4 describes how to use the reader test application to determine if the reader is working properly by communicating with a Tag. The following settings should be selected for the reader test program:

- Mode: Maximum throughput (Mode 0)
- Session 2
- TX Power: 30dBm

After configuration and verification that the antenna is properly connected to Antenna 4 of the reader, select Operation and press the Start button. At this point, a 24-digit hexadecimal number representing the Tag EPC value should appear on the screen. The tag should continually read and the read rate should be greater than 50 reads/sec.

## 9.4 Conclusion of Tests

The tests described in this document have provided a basic methodology to isolate and correct the most common problems associated with reader operation.

For additional technical support, go to http://rfid-support.impinj.com. For units not purchased directly from Impinj, please contact your VAR directly.
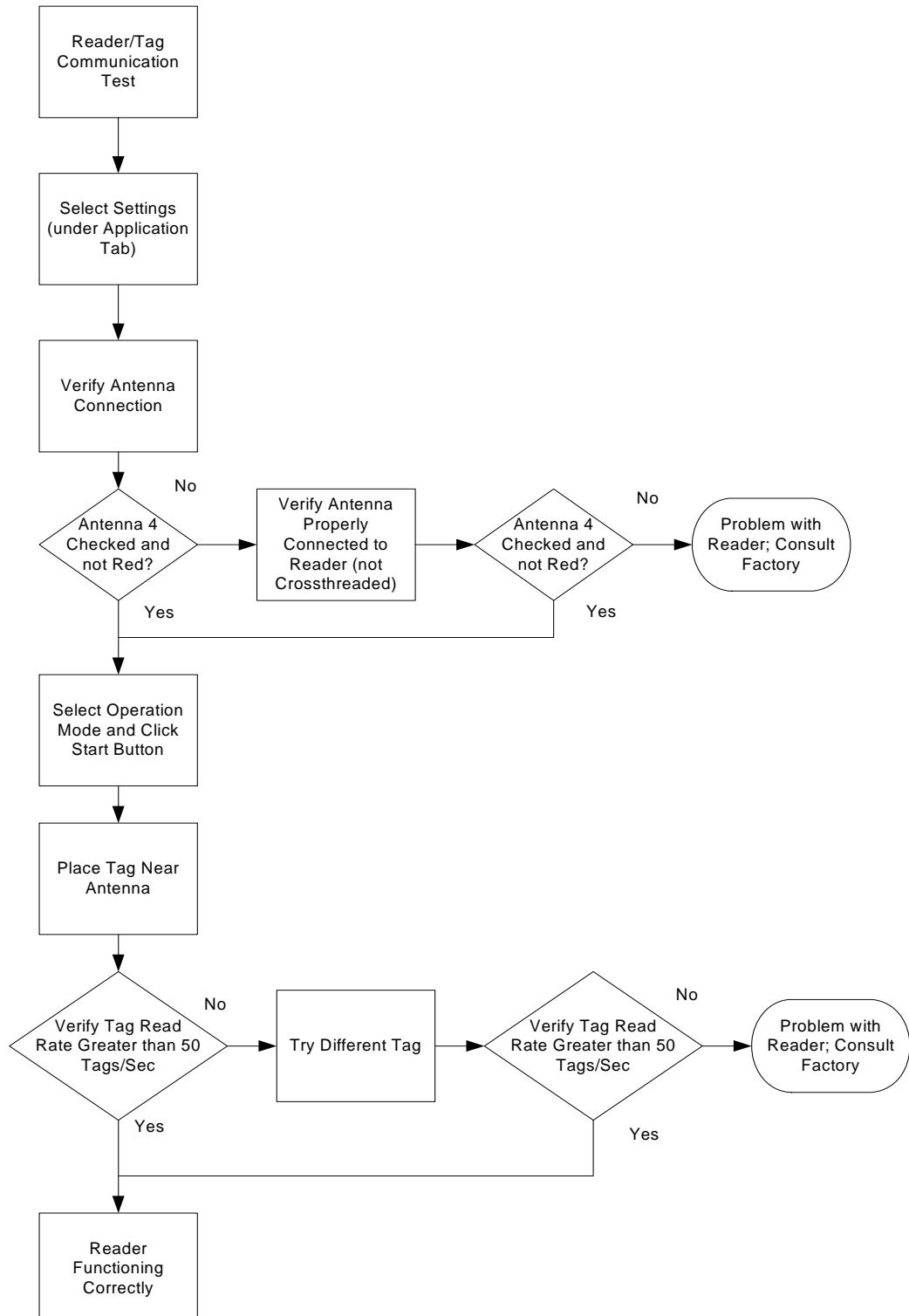
**Figure 9-5 Testing Reader Communication**

# 10 References

**Table 10-1 References**

| Reference | Description |
| --- | --- |
| MIB-2 RFC 1213 | Management Information Base for Network Management of TCP/IP-based internets:MIB-II. K. McCloghrie, M. Rose. March 1991. |
| RFC 3986 | Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, R. Fielding, L. Masinter. January 2005. |
| RM Standard v. 1.0.1 | Reader Management Standard defines version 1.0 of the wire protocol used by management software to monitor the operating status and health of EPCglobal compliant tag readers. See http://www.epcglobalinc.org/standards/rm for more information |
| RM MIB file location | http://www.epcglobalinc.org/standards/rm/rm_1_0_1-schema-20070531 |
| LLRP Standard v. 1.0.1 | The Low Level Reader Protocol Standard specifies the interface between RFID readers and their clients. See http://www.epcglobalinc.org/standards for more information. |

# Appendix A  Impinj Factory Default Configuration

Detailed below are the factory default configuration settings for the Speedway reader. Except for the username and password, all entries are shown when the "show all config" command is issued on a Speedway reader in its factory default configuration.

```
Username: root
Password: impinj
```

## Networking Category

```
Static domain: None
IpAddressMode: dynamic  # (using DHCP to obtain IP address)
hostname: speedway-nn-nn-nn,  # where nn-nn-nn are the last three
bytes of the reader's MAC address (in hex)
SendHostname: on
Userclass: None
Static DNS server: None
Static NTP server: None
mDNS: enabled
DNS-SD HTTP: enabled
DNS-SD RFID: enabled
LLA status: enabled
```

## SNMP Category

```
SNMP Category
SnmpServiceStatus: enabled
ROCommunity: public
RWCommunity: private
WriteEnabled: false
NonRfidTrapEnabled: true
Trap Receivers: None
TrapLogEnabled: true
TrapLogLevel: error
epcgRdrDevDescription: Same as system Description.
epcgRdrDevRole:  'My reader role'
epcgNotifChanName1: 'Mach1 Internal'
epcgNotifChanName2: 'Mach1 External'
epcgNotifChanName3: 'LLRP Client'
epcgNotifChanName4: 'LLRP Reader '
epcgRdrDevOperNotifStateLevel: error
epcgReadPointOperStateNotifyEnable: true
epcgReadPointOperNotifyStateLevel: error
epcgSrcOperStatusNotifEnable: true
epcgSrcOperStatusNotifyLevel: error
epcgNotifChanOperNotifEnable: true
epcgNotifChanOperNotifLevel: error
```

## System Info Category

```
system Description: 'Impinj Speedway'
system Contact: 'http://www.supplier.com/techsupport'
```

```
system name: 'speedway-nn-nn-nn'    # same as default hostname
system Location: 'unknown'
```

### Upgrade Agent Category

```
MetafileUri: Empty
RetrieveMode: push
```

### Logging Category

```
ApplicationLevel: emergency
ConfigurationLevel: emergency
MgmtLevel: emergency
NetworkLevel: emergency
RFIDParameters Level : emergency
RFIDSingulation Level: emergency
RFIDAccess Level: emergency
System Level: emergency
syslog severityLevel: error
static syslog server: none
```

# Appendix B  Command Line Editing in Rshell

| Key | Sequence | Action |
| --- | --- | --- |
| Printable char | | Insert character at cursor position then move cursor right one. |
| KEY_LEFT | Control-B, \033[D | Move cursor left one. Sticks at begin-of-line. |
| KEY_RIGHT | Control-F, \033[C | Move cursor right one. Sticks at end-of-line. |
| KEY_HOME | Control-A, \033[1~ | Move cursor to begin-of-line. |
| KEY_END | Control-E, \033[4~ | Move cursor to end-of-line |
| KEY_DELETE | Control-D, \033[3~ | Delete character at cursor position. Leave cursor at same position. |
| KEY_BACKSPACE | Control-H | Move cursor left one then same as KEY_DELETE. Does nothing at begin-of-line. |
| KEY_ERASELINE | Control-U | Erase entire line, place cursor at begin-of-line |
| KEY_ENTER | Control-J, Control-M | Move cursor to end-of-line. Return the line to the caller for processing. |
| KEY_UP | Control-P, \033[A | Move up (earlier) the history list. Erases current line, copies in and displays history entry, places cursor at end-of-line. |
| KEY_DOWN | Control-N, \033[B | Move down (later) the history list. Erases current line, copies in and displays history entry, places cursor at end-of-line. |
| anything else | | Ignored |

# Appendix C  Software Compatibility Matrix

The table below provides compatibility information of the Speedway® reader firmware with Multi-Reader™ and Mach1™. If you do not see your Speedway reader firmware version below or have additional questions, please contact your sales representative.

| Speedway Firmware Version | Mach1 Version | DLL Version | MultiReader Version |
|---|---|---|---|
| 1.4.6 | 2.0.4 | 2.0.4 | 2.1.4 |
| 2.0.2 | 2.2.0 | 3.0.1 | 2.4.4 |
| 2.2.4 | 2.4.0 | 3.2.0 | 3.2.4 |
| 2.4.X | 2.6.0 | 3.4.0 | 4.1.X |
| 2.6.0 | 2.8.0 | 3.6.0 | 4.2.X |
| Octane 3.0 | 3.0 | 3.10.0 | 5.0.0.X |

# Appendix D LLRP Basic Capabilities

The Table 11-1 shows the LLRP capabilities supported. Where relevant, these capabilities are reported via the LLRP GET_READER_CAPABILITIES_RESPONSE message.

**Table 11-1 LLRP Basic Capabilities**

| Feature | Capacity | Notes |
|---|---|---|
| GPI | 4 | These 4 GPI (referenced in LLRP as GPI 1-4) correspond to GPIN0-GPIN3 |
| GPO | 8 | These 8 GPO (referenced in LLRP as GPO 1-8) correspond to GPOUT0-GPOUT7 |
| Antennas | 4 | The 4 antennas correspond to antenna ports 1-4, respectively |
| UTC (real world) clock | Yes | |
| Air protocols supported | EPCglobal Class1Gen2 | |
| Maximum number of ROSpecs | 1 | The total AISpec capacity of the reader is 16. Attempts to add ROSpecs where the total number of AISpecs defined on the reader exceeds 16 will result in an error. |
| Maximum number of priorities | 1 | Must be 0. Multiple ROSpecs are executed to completion. There is no preemption or multiplexing of active ROSpecs |
| RFSurvey suppot | No | |
| Maximum number of AISpecs per ROSpec | 8 | The total AISpec capacity of the reader is 16. Attempts to add ROSpecs where the total number of AISpecs defined on the reader exceeds 16 will result in an error. |
| Maximum number of InventoryParameter-Specs per AISpec | 1 | |
| State aware singulation support | No | |

Octane 3.0 User Guide

**Table 11-1 LLRP Basic Capabilities**

| Feature | Capacity | Notes |
|---|---|---|
| Maximum InventoryFilters per InventorySpec | 2 | See footnote [1] |
| Truncate flag support | No | Must be 0 |
| Maximum number of AccessSpecs | 64 | |
| Maximum number of OpSpecs per AccessSpec | 8 | |
| ClientOpSpec support | No | |
| Number of Gen 2 modes | 5 | |
| Can set Tari | No | |
| Buffer overflow warnings | Yes | Optional |
| Can control events and reports upon reconnect | Yes | By default, HoldEventsAndReports is False. Buffered event and report data will be sent by the reader immediately after the ConnectionStatusEvent. |
| Maximum AirPortocolInventoryCommandSettings per Antenna Configuration | 1 | |
| Can set power per antenna | Yes | |
| Can set sensitivity per antenna | Yes | |
| Can set frequency per antenna | No | See footnote 1 |
| Can set Gen 2 mode per antenna | No | See footnote 1 |

**Table 11-1 LLRP Basic Capabilities**

| Feature | Capacity | Notes |
|---|---|---|
| Can set Gen 2 session per antenna | No | See footnote 1 |
| Can set estimate population and time in field per antenna | No | See footnote 1 |
| Disconnected operation support | Yes | Reader will continue to execute ROSpecs and AccessSpecs when disconnected. To stop disconnected operation, disable or delete all ROSpecs and AccessSpecs before disconnecting |
| Reader initiated connections | Yes | Refer to the User's guide to configure the reader to make an outgoing connection |
| Maximum receive message size | 10,000 bytes | Messages longer than 10,000 bytes will cause the connection to be closed by the reader |
| Maximum TagDataReport per RO_Access_Report | 2000 reports | With no OpSpecResults. Reader transmit buffer is limited to 512 kbytes. |

1. The LLRP protocol allows the client to specify different settings on a per-antenna basis. Where noted in the Table 11-1, the Speedway firmware requires these settings to be the same across all antennas specified within a single AISpec.

# Appendix E LLRP Default Configuration

The following shows the LLRP default values for Speedway firmware release 3.0. An LLRP factory default will reset the unit to these settings. The definitions below are instances of llrp.xsd, which is an abstract representation of the LLRP protocol available at http://www.sourceforge.net/projects/llrp-toolkit/.

**AccessSpecs**: There are no accessSpecs defined by default in the Speedway implementation of LLRP

**ROSpecs**: There are no accessSpecs defined by default in the Speedway implementation of LLRP

**KeepAlive**: No keep-alives are generated by default
```
<KeepaliveSpec>
  <KeepaliveTriggerType>Null</KeepaliveTriggerType>
  <PeriodicTriggerValue>0</PeriodicTriggerValue>
</KeepaliveSpec>
```

**Reader Event Notifications:** The following is the default event reporting configuration
```
<ReaderEventNotificationSpec>
 <EventNotificationState>
  <EventType>Upon_Hopping_To_Next_Channel</EventType>
  <NotificationState>0</NotificationState>
 </EventNotificationState>
 <EventNotificationState>
  <EventType>GPI_Event</EventType>
  <NotificationState>0</NotificationState>
 </EventNotificationState>
 <EventNotificationState>
  <EventType>ROSpec_Event</EventType>
  <NotificationState>0</NotificationState>
 </EventNotificationState>
 <EventNotificationState>
  <EventType>Report_Buffer_Fill_Warning</EventType>
  <NotificationState>0</NotificationState>
 </EventNotificationState>
 <EventNotificationState>
  <EventType>Reader_Exception_Event</EventType>
  <NotificationState>1</NotificationState>
 </EventNotificationState>
 <EventNotificationState>
  <EventType>RFSurvey_Event</EventType>
  <NotificationState>0</NotificationState>
 </EventNotificationState>
 <EventNotificationState>
  <EventType>AISpec_Event</EventType>
  <NotificationState>0</NotificationState>
 </EventNotificationState>
 <EventNotificationState>
  <EventType>AISpec_Event_With_Details</EventType>
  <NotificationState>0</NotificationState>
 </EventNotificationState>
 <EventNotificationState>
  <EventType>Antenna_Event</EventType>
  <NotificationState>0</NotificationState>
```

```
            </EventNotificationState>
          </ReaderEventNotificationSpec>
```

**RO Reporting:** The following is the default report data for LLRP tag reports.

```
    <ROReportTrigger>Upon_N_Tags_Or_End_Of_ROSpec</ROReportTrigger>
    <N>0</N>
    <TagReportContentSelector>
      <EnableROSpecID>0</EnableROSpecID>
      <EnableSpecIndex>0</EnableSpecIndex>
      <EnableInventoryParameterSpecID>0</EnableInventoryParameterSpecID>
      <EnableAntennaID>0</EnableAntennaID>
      <EnableChannelIndex>1</EnableChannelIndex>
      <EnablePeakRSSI>1</EnablePeakRSSI>
      <EnableFirstSeenTimestamp>1</EnableFirstSeenTimestamp>
      <EnableLastSeenTimestamp>1</EnableLastSeenTimestamp>
      <EnableTagSeenCount>1</EnableTagSeenCount>
      <EnableAccessSpecID>0</EnableAccessSpecID>
    </TagReportContentSelector>
  </ROReportSpec
```

**Access Reporting:** The following is the default report data for LLRP tag reports.

```
<AccessReportSpec>
    <AccessReportTrigger>Whenever_ROReport_Is_Generated</AccessReportTrigger>
  </AccessReportSpec
```

**Antenna Configuration:** The antenna configuration identical for all antennas. Below is the configuration for Antenna 1.

```
 <AntennaConfiguration>
    <AntennaID>1</AntennaID>
    <RFReceiver>
     <ReceiverSensitivity>0</ReceiverSensitivity>
    </RFReceiver>
    <RFTransmitter>
     <HopTableID>1</HopTableID>
     <ChannelIndex>0</ChannelIndex>
     <TransmitPower>60</TransmitPower>
    </RFTransmitter>
    <C1G2InventoryCommand>
     <TagInventoryStateAware>0</TagInventoryStateAware>
     <C1G2RFControl>
       <ModeIndex>2</ModeIndex>
       <Tari>0</Tari>
     </C1G2RFControl>
     <C1G2SingulationControl>
       <Session>1</Session>
       <TagPopulation>32</TagPopulation>
       <TagTransitTime>0</TagTransitTime>
     </C1G2SingulationControl>
    </C1G2InventoryCommand>
  </AntennaConfiguration>
```

**GPI Configuration:** All GPI ports are disabled by default.

```
<GPIPortCurrentState>
    <GPIPortNum>1</GPIPortNum>
    <Config>0</Config>
    <State>Unknown</State>
  </GPIPortCurrentState>
```

```
<GPIPortCurrentState>
 <GPIPortNum>2</GPIPortNum>
 <Config>0</Config>
 <State>Unknown</State>
</GPIPortCurrentState>
<GPIPortCurrentState>
 <GPIPortNum>3</GPIPortNum>
 <Config>0</Config>
 <State>Unknown</State>
</GPIPortCurrentState>
<GPIPortCurrentState>
 <GPIPortNum>4</GPIPortNum>
 <Config>0</Config>
 <State>Unknown</State>
</GPIPortCurrentState>
```

**GPO Configuration:** All GPO ports are low by default
```
<GPOWriteData>
  <GPOPortNumber>1</GPOPortNumber>
  <GPOData>0</GPOData>
 </GPOWriteData>
 <GPOWriteData>
  <GPOPortNumber>2</GPOPortNumber>
  <GPOData>0</GPOData>
 </GPOWriteData>
 <GPOWriteData>
  <GPOPortNumber>3</GPOPortNumber>
  <GPOData>0</GPOData>
 </GPOWriteData>
 <GPOWriteData>
  <GPOPortNumber>4</GPOPortNumber>
  <GPOData>0</GPOData>
 </GPOWriteData>
 <GPOWriteData>
  <GPOPortNumber>5</GPOPortNumber>
  <GPOData>0</GPOData>
 </GPOWriteData>
 <GPOWriteData>
  <GPOPortNumber>6</GPOPortNumber>
  <GPOData>0</GPOData>
 </GPOWriteData>
 <GPOWriteData>
  <GPOPortNumber>7</GPOPortNumber>
  <GPOData>0</GPOData>
 </GPOWriteData>
 <GPOWriteData>
  <GPOPortNumber>8</GPOPortNumber>
  <GPOData>0</GPOData>
   </GPOWriteData>
```

**Events and Reports:** Events are reports are disabled by default
```
<EventsAndReports>
   <HoldEventsAndReportsUponReconnect>0</HoldEventsAndReportsUponReconnect>
</EventsAndReports
```

**Notices**

The information contained in this user guide is confidential and proprietary to Impinj, Inc. This document is conditionally issued, and neither receipt nor possession hereof confers or transfers any right in, or license to, use the subject matter of any drawings, design, or technical information contained herein, nor any right to reproduce or disclose any part of the contents hereof, without the prior written consent of Impinj and the authorized recipient hereof.

Impinj reserves the right to change its products and services at any time without notice.

Impinj assumes no responsibility for customer product design or for infringement of patents and/or the rights of third parties, which may result from assistance provided by Impinj. No representation of warranty is given and no liability is assumed by Impinj with respect to accuracy or use of such information.

Impinj products are not designed for use in life support appliances, devices, or systems where malfunction can reasonably be expected to result in personal injury, death, property damage, or environmental damage.

<div align="center">

Impinj, Inc.

701 N. 34<sup>th</sup> Street, Suite 300

Seattle, WA  98103

www.impinj.com

</div>