



RShell Reference Manual

Version 7.4

Copyright © 2012 - 2020 Impinj, Inc. All rights reserved

<http://www.impinj.com>

Impinj, Octane, Speedway, xSpan and xArray are either registered trademarks or trademarks of Impinj, Inc. Visit www.impinj.com/trademarks for additional information about Impinj trademarks.

Contents

| | | |
|----------|----------------------------------|-----------|
| 1 | Introduction | 3 |
| 2 | Document Conventions | 4 |
| 2.1 | Syntax | 4 |
| 2.2 | Examples | 4 |
| 3 | Overview | 5 |
| 3.1 | Help | 6 |
| 3.2 | Response Format | 8 |
| 3.3 | Compatibility | 9 |
| 4 | Command Reference | 11 |
| 4.1 | Reboot Command | 11 |
| 4.2 | Config Command | 11 |
| 4.2.1 | Config Access Command | 11 |
| 4.2.2 | Config Image Command | 12 |
| 4.2.3 | Config Logging Command | 16 |
| 4.2.4 | Config Network Command | 19 |
| 4.2.5 | Config RFID Menu | 34 |
| 4.2.6 | Config SNMP Command | 39 |
| 4.2.7 | Config System Menu | 45 |
| 4.2.8 | Config Feature Menu | 49 |
| 4.3 | Show Command | 50 |
| 4.3.1 | Show Image Menu | 51 |
| 4.3.2 | Show Logging Menu | 58 |
| 4.3.3 | Show Network Menu | 60 |
| 4.3.4 | Show RFID Menu | 71 |
| 4.3.5 | Show SNMP Menu | 77 |

| | | |
|----------|-------------------------------|-----------|
| 4.3.6 | Show System Menu | 78 |
| 4.3.7 | Show Feature Menu | 83 |
| 4.3.8 | Show Anthub Command | 84 |
| 5 | Revision History | 85 |
| 6 | Notices | 88 |

1 Introduction

The Command Line Interface (CLI) for the Impinj Speedway Reader, the Impinj R700 RAIN RFID Reader, and the xArray and xSpan Gateways is called RShell. RShell can be accessed after you log in via a serial or SSH connection. You can use the CLI to configure, maintain, and query the status of an RFID Reader.

2 Document Conventions

This document covers the Impinj Octane 7.4 and Impinj R700 RAIN RFID Reader 7.4 software releases. The term “Reader” is used to refer to the Impinj R700 RAIN RFID Reader, the Impinj Speedway Reader, and the xArray and xSpan Gateways.

2.1 Syntax

The following markings are used throughout this document:

[] - optional

() - grouping

| - either

<> - placeholder

Literal (reduced size +bold) - a literal term

Syntax example:

Usage: `command1` [`<paramA>` (`on|off`)]

The syntax example indicates that `command1` had optional parameters. If `paramA` is specified, it must be followed by ‘on’ or ‘off’.

2.2 Examples

Code examples are provided throughout this reference manual. To help differentiate from descriptive text, the code is shown in a fixed font or using double quotes.

In addition, the input is shown in bold in the examples. In the following example, “help help” is typed, the remainder is the Reader’s response.

```
> help help
```

```
help - Displays this help message.
```

```
Usage: help [<subcommand>]
```

3 Overview

You can navigate to any of the RShell menus simply by entering the menu name at the RShell prompt, as shown below:

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

For machine execution, all RShell 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 a well-defined format.

```
show network > dns
```

```
Status='0,Success'
Domain1Dynamic='impinj.com'
Server1Dynamic='10.10.4.11'
Server2Dynamic='10.0.4.10'
```

For all menus, the **exit** command or simply **.'** will return you to the previous menu's context. To exit RShell and terminate your session, the **exit** command must be executed from the root menu (the period only will not suffice):

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

3.1 Help

For all menus, the "**help**" command or simply the question mark (?) opens a list of all active menu commands available from the Reader, as well as the submenus that can be accessed from the active menu.

```
> help
```

Commands:

```
reboot - Reboot the reader.  
exit - Exit RShell.  
help - Display this help message.  
? - Display this help message.
```

Submenus:

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

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

```
> show help
```

or

```
> show ?
```

Commands:

```
exit - Exit this submenu and return to the parent menu.  
help - Display this help message.  
. - Exit this submenu and return to the parent menu.  
? - Display this help message.
```

Submenus:

```
image - Image status commands.  
logging - Logging status commands.  
network - Network status commands.  
rfid - RFID status commands.
```

snmp - SNMP status commands.
system - System status commands.
feature - Feature status commands.
anthub - Antenna Hub status commands

For all menus, entering the **help** command or question mark (?) prior to a command or menu returns a short description of the command and the syntax for its usage (if any). For example:

```
> ? show
```

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

Usage: show [<subcommand> ...]

or

```
> ? show system platform
```

platform - Display generic platform statistics.

Usage: show system platform

Entering the question mark (?) between a menu and sub-menu/command returns 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. Entering **show ? image** opens a usage help menu that indicates 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 - Displays information about the current image upgrade metafile.

Usage: image metafile

3.2 Response Format

The first line of every command response has the following format.

Status='errorCode,errorString'

The *errorCode* is a numeric value and *errorString* is a human-readable error code. The error codes are defined in Table 3.1.

Table 3.1: General Status Codes*

| Error Code | Error String | Description |
|-------------------|------------------------------|---|
| 0 | Success | The command completed successfully. |
| 1 | Invalid-Command | Command could not be parsed and identified as an interface supported command. |
| 2 | Invalid-Command-Parameter | One or more parameter types were unrecognized for this command. |
| 3 | Invalid-Parameter-Value | One or more parameter values were illegal or out-of-range for this command. |
| 4 | Parameter-Dependency-Error | Parameter value 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 in the system. For example: the Reader 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. |
| 9 | Previous-Command-In-Progress | The command was rejected because a previous command is still in progress and the new command could not be processed. |
| 10 | Command-Being-Processed | The command cannot be finished right away: It is being processed. |
| 11 | Failure | The command failed internally for an unexpected reason. |

| Error Code | Error String | Description |
|-------------------|-----------------------------------|--|
| 12 | Provider-Unavailable | The process responsible for handling the requested operation is currently unavailable and therefore cannot complete the requested operation. |
| 13 | Status-Was-Lost | The command failed internally and produced an invalid result. |
| 14 | Success-Reboot-Required | The command completed successfully and the Reader requires a reboot before any changes take effect. |
| 15 | Incompatible-With-Enabled-Feature | The feature is not compatible with another feature which is already enabled. |

A sample error parameter string shows below with the command deliberately misspelled:

```
> config foobar
```

```
Status='1,Invalid-Command'
```

When a command action generates results, the results follow the status line, one parameter per line in the following format:

```
ParameterName='value'  
ParameterName='value'  
...  
ParameterName='value'
```

The specific response parameters for each command are detailed in Section 4. Many commands display only a relevant subset of their possible parameters. In these cases, failure to find the parameter would not be a protocol error. Some command responses are transient, meaning that their value will change as an activity progresses.

3.3 Compatibility

The RShell CLI is designed to be both a machine interface and a human interface. Impinj strives to maintain backward compatibility within the Speedway and xArray/xSpan product lines. For the new R700 product line, existing command inputs and outputs should be relatively stable.

To ensure future compatibility, applications designed to interpret the CLI responses should ignore unrecognized parameters and should not read any significance into the order of the parameters. This allows for new result parameters to be displayed without forcing a change on the interpreting application.

For example, in the firmware version Octane 7.4, the **show network summary** command provides the following response:

```
> show network summary
```

```
Status='0,Success'  
PrimaryInterface='eth:eth0'  
ActiveInterface='eth:eth0'  
Hostname='SpeedwayR-10-46-B2'  
connectionStatus='Connected'  
ipAddressMode='Dynamic'  
ipAddress='10.0.11.27'  
ipMask='255.255.0.0'  
gatewayAddress='10.0.0.20'  
broadcastAddress='10.0.255.255'  
MACAddress='00:16:25:10:46:B2'  
HTTPService='active'
```

4 Command Reference

This section describes all the commands available within the RShell command line interface and the possible responses.

4.1 Reboot Command

The **reboot** command instructs the Reader to reboot. This command would typically be used after a manual upgrade of the Reader’s firmware or application software. The **reboot** command is only available from the root menu.

4.2 Config Command

The **config** command has several submenus, shown in the following table, all of which are described in the following sections.

Table 4.1: Config Command Parameters

| Command | Description |
|---------|--|
| access | Submenu of access configuration commands. |
| image | Submenu of image and upgrade configuration commands. |
| logging | Submenu of logging configuration commands. |
| network | Submenu of network configuration commands. |
| rfid | Submenu of RFID configuration commands. |
| snmp | Submenu of SNMP configuration commands. |
| system | Submenu of system configuration commands. |
| feature | Submenu of feature configuration commands. |

4.2.1 Config Access Command

The **config access mypasswd** command changes the password for the logged-in user. “Root” is the only user login defined for the Reader. The Reader default password is set to ‘impinj’. Other Reader types might use alternative default passwords.

The user account name and password are used to access the command line interface via serial and ssh. The **config access** submenus and the **config access mypasswd** command arguments are described in the following two tables.

Table 4.2: Config Access Command Options

| Command Parameters | Description |
|---|--|
| mypasswd <old password> <new password> | Change the password of the logged-in user from the old (current) password to a new password. |

Table 4.3: Config Access Command Parameters

| Argument | Options | Format | Description |
|----------|----------------------------------|------------------|---|
| mypasswd | <old password> <new password> | string string | Password to set as account's active password (use printable characters only). Passwords up to 20 characters in length have been tested. Passwords entered on the command line are clear text. |

Usage: **config access mypasswd <old password> <new password>**

4.2.2 Config Image Command

The **config image** command provides options for image and upgrade configurations. A detailed explanation of how to upgrade images is given in the *Firmware Upgrade Reference Manual*.

Table 4.4: Config Image Command Parameters

The command parameters for the **config image** command are shown in the following table.

| Command | Description |
|--------------|---|
| default | Restore the image to the default configuration. |
| fallback | Fall back to the previous image (if valid). |
| removecap | Remove the Custom Application Partition (CAP). |
| metafile | Perform an upgrade using a metafile from the specified URI. |
| retrievemode | Configure the mode used to upgrade the image. |
| upgrade | Perform an upgrade using the image file at the specified URI. |

Config Image Default Command

The **config image default** command restores the configuration to the default settings. When complete, the command is automatically followed by a reboot. The custom application (if any) is notified after the reboot, so that configuration specific to the custom application (if any) can also be restored to the defaults. This command takes no parameters.

During restoration to the configuration defaults, the **show image summary** command reports the

UpgradeStatus as 'WaitingForCDR'. When this command is executed, the **metafile retrieve-mode** is set to **manual**, which cancels any previously scheduled periodic upgrade. When the Reader subsequently boots, the Reader will be running default configuration for the same system version as the system from which it performed the configuration default restore.

If the Reader is in the **auto** upgrade mode when the **config image default** command is issued, it is possible that the Reader could be retrieving the metafile or performing an upgrade at the same time. In this case, this command may return "Previous-Command-In-Progress." If this occurs, wait for the metafile to be retrieved or the upgrade to complete before executing this command again. A short wait allows the command in progress to complete.

Usage: **config image default**

Config Image Fallback Command

The **config image fallback** command is used to revert back to the previous image. The successful processing of this command is followed by an automatic reboot. This command accepts no parameters.

If there is no valid previous image available to fall back to, "Permission-Denied" is the command response. In the meantime, the Reader operates normally, except that all of the **config image** commands will be rejected with the reason "Current Image Invalidated." In addition, if **retrieve-mode** is set to **auto**, the fallback command will cancel any previously scheduled periodic upgrades. When the Reader is rebooted, the previous image will be running.

If the Reader is in auto mode during execution of the **config image fallback** command, it is possible that the Reader could be retrieving the metafile or performing an upgrade at the same time. If this is the case, this command might return "Previous-Command-In-Progress."

A fallback uses all the old configuration settings, including the upgrade metafile settings as if the upgrade to the newer image was never performed. This 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.

Config Image RemoveCAP Command

The **config image removecap** command is used to remove the Custom Application Partition (CAP). The successful processing of this command follows with an automatic reboot. This command takes no parameters.

The effect of this command can be reversed. In other words the CAP can be restored by issuing a **config image fallback** command. Performing the **config image removecap** twice ensures that the removed CAP cannot be restored.

If the Reader is in **auto** mode during execution of this command, it is possible that the Reader could be retrieving the metafile or performing an upgrade at the same time. If this is the case, this command might return "Previous-Command-In-Progress."

Config Image Metafile Command

This command takes the Universal Resource Identifier (URI) of the upgrade configuration metafile as its parameter. It commands the Reader to perform upgrades based on the information in the metafile identified by the URI.

Usage: config image metafile <URI>

Upon receiving this command, the Reader updates its local upgrade configuration URI. It then retrieves the (new) upgrade configuration metafile, and performs the upgrade in accordance with the metafile. If the upgrade is successful, the way the new image is activated depends on the commit-mode specified in the metafile. For more information, see the *Firmware Upgrade Reference Manual*.

If the Reader is in auto mode during the execution of this command, it is possible that the Reader could be retrieving the metafile or performing an upgrade at the same time. If this is the case, this command will return “Previous-Command-In-Progress.”

Config Image RetrieveMode Command

This command sets the Reader’s **metafile retrieve** mode and can also set the retrieval period if the mode is set to **auto**, as described in the following table. When the retrieve-mode is set to **manual**, the Reader will take no upgrade actions. To perform an upgrade in manual mode the user must issue a **config image upgrade** command, which directly downloads an upgrade image.

Table 4.5: Config Image RetrieveMode Command Parameters

| Command | Argument | Format | Description |
|--------------|----------|--------|---|
| retrievemode | manual | enum | In manual mode the user must specify a new metafile URI or re-issue the command an upgrade. |

| Command | Argument | Format | Description |
|---------|------------------|-----------------|--|
| | Auto <period> | enum integer | In auto mode, the Reader periodically retrieves the metafile from the most recent metafile URI at the rate specified by the <period> in minutes. The retrieve period is used only until the Reader retrieves a valid metafile, at which time the retrieve period contained in the metafile is adopted. |

Usage: config image retrievemode manual

Usage: config image retrievemode auto <period>

<period> is the duration between successive retrievals of the metafile (in minutes) from the most recently specified URI.

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

Config Image Upgrade Command

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

Usage: config image upgrade <URI>

Upon receiving this command, the 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 upgrade version matches the current version. If the upgrade is successful, the new image is not activated until the user reboots the system.

If the Reader is in **auto** mode during the execution of this command, it is possible that the Reader could be retrieving the metafile or performing an upgrade at the same time. In this case, the command might return “Previous-Command-In-Progress.”

Note: This command does not change the Reader's upgrade configuration URI, but it sets the retrieve-mode to **manual**. This means that the Reader will not periodically retrieve the upgrade configuration metafile until the retrieve-mode is reset to auto.

4.2.3 Config Logging Command

The **config logging** commands provide configuration options for the storage and forwarding of logged events. Logged events are forwarded using the standard Syslog protocol to a remote Syslog server. Internally the logged events are stored in the Reader's file system, accumulating and persisting across reboots. All logged events have an associated severity level. Only events of severity greater than or equal to the user configured level are retained. Logs are classified into management, rfid, and system categories.

The user log severity can be set to one of eight levels in decreasing order from most severe to least severe: emergency, alert, critical, error, warning, notice, info, and debug. For example, if the log level is set to alert, then only logs classified as emergency or alert are processed.

Regardless of how the user configures the log settings, all error (and higher severity) logs in all categories are retained in an error log independent of the user controlled 'application' log.

Figure 4.1 illustrates a configuration where the Reader management category of logs is set to critical (and above), the RFID related logs are set to warning (and above), and the system logs are set to alert (and above).

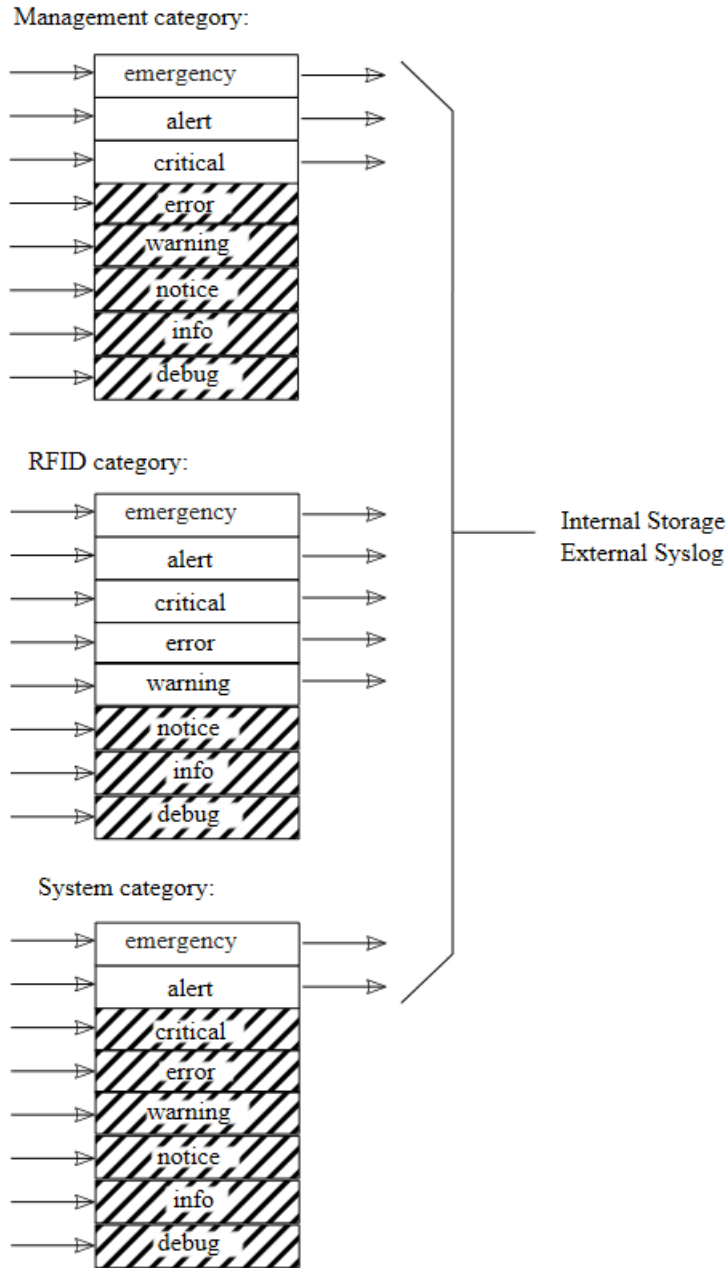


Figure 4.1 Severity Level Logging Categories

The command parameters for the **config logging** command are shown in the following table. The command sets the logging level for a log category to one of a set of pre-defined severity levels.

Table 4.6: Config Logging Command Parameters

| Argument | Option | Format | Description |
|------------|---|---------|---|
| add | <syslog server> | address | Add a new Syslog server with given address or hostname. |
| clear | | | Clear the contents of the application log. |
| del | <syslog server> | address | Delete a Syslog server with given address or hostname. |
| delall | | | Delete all listed Syslog servers. |
| management | emergency alert rfid system | enum | Configures the level at and above which logs are retained and forwarded. Listed in decreasing order of severity. The default logging level in all cases is warning level. |
| | critical error warning notice info debug | | |

Note: You can add up to six syslog servers.

The logging categories are mapped to the following syslog facilities:

Table 4.7: Logging categories mapped to syslog facilities

| Category | syslog facility | Description |
|------------|-----------------|--|
| management | LOG_LOCAL0 | Reserved for local use |
| | LOG_AUTH | Security/authorization messages |
| | LOG_AUTHPRIV | Security/authorization messages (private) |
| system | LOG_LOCAL1 | Reserved for local use |
| | LOG_CRON | Clock daemon (cron and at) |
| | LOG_DAEMON | System daemons without separate facility value |
| | LOG_LPR | Line printer subsystem |
| | LOG_MAIL | Mail subsystem |
| | LOG_NEWS | USENET news subsystem |
| | LOG_SYSLOG | Messages generated internally by syslogd |
| | LOG_USER | Generic user-level messages (default) |
| | LOG_UUCP | UUCP subsystem |
| rfid | LOG_LOCAL2 | Reserved for local use (RFID related) |

These events can be viewed via the **show logging** command.

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

```
Usage: config logging <category> <level>
<category> is (management|rfid|system)
<level> is (emergency|alert|critical|error|warning|notice|info|debug)
```

Usage: config logging add <server name>

Usage: config logging clear

Usage: config logging del <server name>

Usage: config logging delall

An example of commands that clear the internal log file, configure RFID logging level to ‘warning’ (and above), and add a Syslog server located at 10.0.10.37 are shown below:

```
> config logging clear
Status='0,Success'
> config logging rfid warning
Status='0,Success'
> config logging add 10.0.10.37
Status='0,Success'
```

4.2.4 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 parameters are shown in the following table.

Table 4.8: Config Network Command Parameters

| Command | Description |
|--------------|---|
| hostname | Set the Reader’s network hostname. |
| mdns | Configures the mDNS service to either be enabled or disabled. |
| wlan | Submenu for WLAN specific configuration commands. |
| dns | Submenu of DNS-specific configuration commands. |
| interface | Submenu of network interface configuration commands. |
| ip | Submenu of IP address and configuration commands. |
| ntp | Submenu of NTP-specific configuration commands. |
| http | Submenu for HTTP specific commands |
| https | Submenu for HTTPS specific commands |
| ftp | Submenu for FTP-specific commands |
| ssh | Submenu for SSH-specific commands |
| portsecurity | Submenu for Port Security specific commands |
| sftp | Submenu for SFTP specific commands |
| lldp | Submenu of LLDP specific configuration commands. |

Config Network Hostname Command

The following table shows the **config network hostname** parameters.

Table 4.9: Config Network Hostname Command Parameters

| Command | Argument | Format | Description |
|----------|-------------|--------|---|
| hostname | <host name> | string | Set the Reader hostname. If using DHCP and a hostname is returned from the DHCP server, the hostname returned from DHCP will take precedence. |

The **config network hostname** command might only be available in Reader models prior to the Impinj R700 RAIN RFID Reader.

Example to change the hostname:

```
> config network hostname MySpeedwayRevolution
Status='0,Success'
```

Config Network Interface Command

Table 4.10: Config Network Interface Command Parameters

| Command | Argument | Format | Description |
|---------|------------|--------|--|
| primary | eth wlan | enum | Configure the primary interface type, i.e., the network interface that is active on bootup. Two types are supported: ethernet and wlan (WiFi). |
| active | eth wlan | enum | Switch the active interface to the specified type. |

Example to change the active interface:

```
> config network interface active eth
Status='0,Success'
```

Config Network mDNS Command

The **config network mdns** command might only be available in Reader models prior to the Impinj R700 RAIN RFID Reader. The following table shows the **config network mdns** parameters.

Table 4.11: Config Network mDNS Command Parameters

| Command | Argument | Format | Description |
|---------|------------------|--------|---|
| mdns | enable disable | enum | Configure the current state of the mDNS service. When enabled, mDNS is always active and can be used to both resolve addresses in the .local domain as well as provide resolution of the Reader within the .local domain. |

An example of the command to change the state of the mDNS service:

```
> config network mDNS enable
Status='14,Success-Reboot-Required'
```

Note : reader must be rebooted after this command.

```
> config network mDNS disable
Status='0,Success'
```

Config Network DNS Command

The **config network dns** command allows the user to statically configure DNS servers. These servers are in addition to any provisioned through DHCP. The command parameters are shown in the following table.

Table 4.12: Config Network DNS Command Parameters

| Command | Argument | Format | Description |
|---------|--------------|--------------|---|
| add | <dns server> | <ip address> | Add a statically configured server to the list of current DNS servers. Manually configured DNS servers will be utilized after searching DNS servers returned by DHCP. |
| del | <dns server> | <ip address> | Delete a statically configured server from the list of current DNS servers. Servers obtained through DHCP are not available for deletion. |
| delall | | | Delete all statically configured DNS servers from the current list. |

A sample command and response is shown below:

```
> config network dns add 1.2.3.4
```

```
Status='0,Success'
```

Config Network DNS Domain Command

The **config network dns domain** command allows the user to add statically configured DNS domains. These servers are in addition to any provisioned through DHCP. Command parameters are shown in the following table.

Table 4.13: Config Network DNS domain Command Parameters

| Command | Argument | Format | Description |
|---------|---------------|--------|---|
| add | <domain name> | string | Add a static domain name to the list of domain names. |
| del | <domain name> | string | Delete a static domain name from the list of domain names. |
| delall | | | Delete all static domain names from the list of domain names. |

A sample command and response is shown below:

```
> config network dns domain add mydomain.com  
Status='0,Success'
```

Config Network IP Command

The **config network ip** command allows the user to statically configure IP settings or configure the Reader to use DHCP.

The reader can be configured with either a static IPv4 or static IPv6 address. IPv6 does not support broadcast addresses. If you specify a broadcast address when specifying a static IPv6 address, the broadcast address will be ignored without returning an error.

Note: The static address is immediately available. The dynamic address will remain active until the next reboot.

The command parameters are shown in the following table.

Table 4.14: Config Network IP Command Parameters

| Command | Argument | Format | Description |
|---------|----------|--------|--|
| dynamic | | | Configure the Reader to use DHCP parameters. |

| Command | Argument | Format | Description |
|---------|---|--------|---|
| static | <ip_address> <netmask> <gateway> <broadcast> | | Configure the Reader to use statically configured IP address parameters. The following combinations of parameters are valid: <ip_address> or prefix length for IPv6 addresses (1-128) <ip_address> <gateway> <ip_address> <netmask> <gateway> <broadcast> For parameters not specified, the Reader will use default values derived from the values provided. |

Examples of the commands are shown below:

Set the IP mode to dynamic:

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

Show the current network IP settings:

```
> show network ip summary  
Status='0,Success'  
connectionStatus='Connected'  
ipAddressMode='Dynamic'  
ipAddress='10.10.10.41'  
ipMask='255.255.0.0'  
gatewayAddress='10.10.0.1'  
broadcastAddress='10.10.255.255'
```


Set a static IPv4 address:

```
> config network ip static 192.168.20.116  
Status='0,Success'  
> show network ip summary  
Status='0,Success'  
connectionStatus='Connected'  
ipAddressMode='Static'  
ipAddress='192.168.20.116'  
ipMask='255.255.0.0'  
gatewayAddress='192.168.0.1'  
broadcastAddress='192.168.255.255'
```

Set a static IPv4 address and gateway:

```
> 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 ip summary  
Status='0,Success'  
connectionStatus='Connected'  
ipAddressMode='Static'  
ipAddress='192.168.20.116'  
ipMask='255.255.255.0'  
gatewayAddress='192.168.20.1'  
broadcastAddress='192.168.20.255'
```

Set a static IPv6 address:

```
> config network ip static 2600:2104:5:3:2c88:2a32:5634:1234  
Status='0,Success'
```

Set a static IPv6 address and gateway:

```
> config network ip static 2600:2104:5:3:2c88:2a32:5634:1234 2600:2104:5:3:2c88:1111  
Status='0,Success'
```

Set a static IPv6 address, netmask, and gateway:

```
> config network ip static 2600:2104:5:3:2c88:2a32:5634:1234 64 2600:2104:5:3:2c88:1111  
Status='0,Success'
```

Show the current network IP settings (dynamic IPv6 example):

```
> show network ip summary  
Status='0,Success'  
connectionStatus='Connected'  
ipAddressMode='Static'  
ipAddress='2600:2104:5:3:2c88:2a32:5634:1234'  
ipMask='64'  
gatewayAddress='2600:2104:5:3:2c88:1111'  
MACAddress='00:16:25:11:55:aa'
```

Config Network LLDP Command

Readers that support transmit power of 36 dBm ERP (Effective Radiated Power) as covered in the ETSI EN 302 208 draft specification, must be powered by a DC power supply or a Power-over-Ethernet switch that supports PoE+.

For these readers, the Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol (CDP) is used to try to negotiate power with the PoE+-capable Ethernet switch, though not all PoE+ switches support software-based negotiation of LLDP/CDP.

LLDP/CDP is disabled by default on readers that require PoE+ power, but can be enabled with **config system power source auto** or disabled with **config system power source poe** or **config system power source poe+**.

Note: When the LLDP/CDP service is disabled and the Ethernet PoE+ switch cannot allocate sufficient electrical power, running an RO Spec on the reader may result in the reader rebooting.

| Command | Argument | Format | Description |
|---------|---------------------|--------|--|
| lldp | enable disable | enum | Enable and run or disable the LLDP service. When enabled, LLDP negotiates power with a PoE switch. |

The **lldp** command might only be available in Reader models prior to the Impinj R700 RAIN RFID Reader.

Reader products that do not require PoE+ do not use LLDP/CDP and the rshell command is unsupported:

```
> config network lldp enable
Status='7,Unsupported-Command'
```

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 (up to six available DHCP servers may be automatically included as dynamic servers in the list of current NTP servers). You may add up to six statically configured NTP servers. The NTP service determines which of the available servers to synchronize with and will only synchronize to one server at a time.

The NTP service runs by default but may be disabled by entering the following RShell command:

```
> config network ntp disable
```

Inclusion of dynamically configured NTP services (provisioned via DHCP) is enabled by default but may be disabled using the following command:

```
> config network ntp dynamicsservers disable
```

The command parameters are shown in the following table.

Table 4.15: Config Network NTP Command Parameters

| Command | Argument | Format | Description |
|---------|-----------------|-----------|--|
| enable | | <address> | Enable and start the NTP service. |
| disable | | <address> | Disable and stop the NTP service. |
| add | <ntp server> | <address> | Add a static server (identified by either an IP address or hostname) to the list of current NTP servers. The NTP service must be disabled before adding a static server. |

| Command | Argument | Format | Description |
|---------------------------|-----------------|-----------|--|
| del | <ntp server> | <address> | Delete a statically configured server (identified by either an IP address or hostname) from the list of current NTP servers. The NTP service must be disabled before deleting a static server. |
| delall | | | Delete all the statically configured NTP servers from the current list. The NTP service must be disabled before entering this command. |
| dynamicservers enable | | | Enable automatic inclusion of NTP servers provisioned via DHCP. The NTP service must be disabled before entering this command. |
| dynamicservers disable | | | Disable automatic inclusion of NTP servers provisioned via DHCP. The NTP service must be disabled before entering this command. |

Note: Attempting to add an NTP server that has already been added will result in an error value of 3 (Invalid-Parameter-Value). Attempting to add more than six static NTP servers will result in an error value of 2 (Invalid-Command-Parameter). Attempting to change the system time (via “config system time”) while the NTP service is enabled will result in an error value of 8 (Permission-Denied). To manually change the system time you must first disable the NTP service (“config network ntp disable”). Attempting to change NTP settings (adding/deleting a static server or enabling/disabling dynamic servers) while the NTP service is enabled will result in a error value of 8 (Permission-Denied). Disable the NTP service before making any NTP settings changes and then re-enable the service.

An example of the command is:

```
> config network ntp add myntpserver.com
Status='0,Success'
```

Config Network Wlan Command

The **config network wlan** command allows the user to configure WiFi interface parameters. This command might only be available in Reader models prior to the Impinj R700 RAIN RFID Reader. Its configurable parameters are shown in the following table.

Table 4.16: Config Network Wlan Command Parameters

| Command | Argument | Format | Description |
|---------|---------------|--------|--|
| nettype | infra adhoc | enum | Set the network type to infrastructure or adhoc. |

| Command | Argument | Format | Description |
|---------|---------------------------------|--------|--|
| ssid | <ssid> | string | Set the WiFi SSID, up to 32 characters |
| keymgmt | wpa-psk wpa-none none | enum | Set the WiFi key management protocol. |
| encrypt | none wpa wpa2 | enum | Set the encryption type for WPA/WPA2 secured connection. |
| psk | <preshared- key> | string | Set the preashred key used for WPA/WPA2 secured connection. Must be between 8 and 32 characters inclusive. |
| update | NA | NA | Save the parameters entered into persistent storage, and then apply them. |
| commit | NA | NA | Save the parameters entered into persistent storage without applying them. |
| quit | NA | NA | Discard the paramters entered. |

The parameters entered are inter-dependent as shown in the following table for all supported use cases.

Table 4.17: WLAN Configuration Parameter Dependency

| Use case | nettype | keymgmt | encrypt | psk | Description |
|----------------------------------|---------|-------------|---------|----------------|---|
| Infrastructure, No security | infra | none | none | NA | No security, connect to other WiFi stations without any protection. |
| Infrastructure, WPA personal | infra | wpa- psk | wpa | <valid psk> | Connect to APs using WPA encryption and WPA2 encryption. |
| Infrastructure, WPA2 personal | infra | wpa- psk | wpa2 | <valid psk> | Connect to APs using WPA encryption and WPA2 encryption. |
| Adhoc, No security | adhoc | none | none | NA | No security, connect to other WiFi stations without any protection. |

| Use case | nettype | keymgmt | encrypt | psk | Description |
|----------------|---------|----------|---------|-------------|---|
| Adhoc, WPA | adhoc | wpa-none | wpa | <valid psk> | Connect to other WiFi stations using preshared key and WPA encryption. |
| Adhoc, WPA2 | adhoc | wpa-none | wpa2 | <valid psk> | Connect to other WiFi stations using preshared key and WPA2 encryption. |

Inconsistent parameters will result in the following error:

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

Here is an example of the command sequences for connecting to an infrastructure network with WPA2 security:

```
> config network wlan nettype infra
> config network wlan ssid "my network"
> config network wlan keymgmt wpa-psk
> config network wlan encrypt wpa2
> config network wlan psk <my-secret>
> config network wlan update
```

If you want to save the changes, but do not want to update your current connection, type:

```
> config network wlan commit
```

in which case the parameters are saved to flash memory and applied the next time the WiFi interface is activated.

Config Network HTTP Menu

The **config network http** menu allows the user to configure whether or not the http (web) server connection is enabled. There are only two configurable parameters, as shown in the following table. These settings will persist across reboots.

Table 4.18: Config Network HTTP Command Parameters

| Command | Description |
|---------|--|
| enable | Enables and starts the http server (default) |
| disable | Disables and stops the http server |

An example of the command is:

```
> config network http enable
Status='0,Success'
```

Config Network HTTPS Menu

The **config network https** menu allows the user to configure whether or not the secure https (web) server connection is enabled. There are only two configurable parameters, as shown in the following table. These settings will persist across reboots.

Table 4.19: Config Network HTTPS Command Parameters

| Command | Description |
|---------|---|
| enable | Enables and starts the https server (default) |
| disable | Disables and stops the https server |

An example of the command is:

```
> config network https enable
Status='0,Success'
```

Config Network FTP Command

The **config network ftp** command allows the user to configure whether or not the FTP server is enabled. There are only two configurable parameters as shown in the following table. These settings will persist across reboots.

Table 4.20: Config Network FTP Command Parameters

| Command | Description |
|---------|---|
| enable | Enables and starts the ftp server |
| disable | Disables and stops the ftp server (default) |

An example of the command is:

```
> config network ftp enable
Status='0,Success'
```

The ftp server is disabled by default. Disabling the ftp server will take effect immediately (a reboot is not required).

Note: Even when the ftp server is enabled, much of the file system is mounted read-only. As such, you may copy files from the reader but copying files to the reader will fail in most cases. For a full description of the default read/write state of file system partitions on the reader, please refer to the Impinj Reader and Gateway Embedded Developer's Guide.

Config Network SSH Command

The **config network ssh** command allows the user to configure whether or not the SSH server is enabled. There are only two configurable parameters as shown in the following table. These settings will persist across reboots.

Table 4.21: Config Network SSH Command Parameters

| Command | Description |
|---------|---|
| enable | Enables and starts the ssh server (default) |
| disable | Disables and stops the ssh server |

An example of the command is:

```
> config network ssh enable
Status='0,Success'
```

Config Network Port Security Command

The **config network portsecurity** command allows the user to configure whether or not 802.1x port-based authentication is enabled for the Ethernet port. There are also three configurable parameters as shown in the following table. These settings will persist across reboots.

Table 4.22: Config Network Port Security Command Parameters

| Command | Description |
|---------------|--|
| dot1x enable | Enables and starts the dot1x service |
| dot1x disable | Disables and stops the dot1x service (default) |

| Command | Description |
|----------------------------|--|
| method MD5 | Use MD5 authentication (default) |
| method PEAP | Use PEAP authentication |
| method MSCHAPv2 | Use MSCHAPv2 authentication |
| access username <username> | Set the username used for authentication |
| access password <password> | Set the password used for authentication |
| reset | Resets to defaults |

Notes: If the dot1x service is currently enabled, changes to the **method**, **username**, and/or **password** will not take effect until the device is rebooted or the service is manually disabled and reenabled.

The **username** and **password** are encrypted and stored locally on the device. The **username** and **password** are displayed as ‘...’ when requesting portsecurity configuration via the **show network portsecurity** command. The **username** and **password** are limited to 127 characters each.

Defaults: The default **method** is MD5. The default **username** is an empty string (“”). The default **password** is an empty string (“”).

An example of the command sequence is:

```
> config network portsecurity disable
Status='0,Success'
> config network portsecurity method PEAP
Status='0,Success'
> config network portsecurity access username user1
Status='0,Success'
> config network portsecurity access password pwd1
Status='0,Success'
> config network portsecurity dot1x enable
Status='0,Success'
```

Config Network SFTP Command

The **config network sftp** command allows the user to store the login credentials used to access an SFTP server. The commands are shown in the following table. This is presently used by the reader’s upgrade mechanism when an SFTP URI is used. The reader uses these login credentials to gain access to the SFTP server.

Table 4.23: Config Network Port Security Command Parameters

| Command | Description |
|----------------------------|---|
| access username <username> | Set the username used to access the SFTP server |
| access password <password> | Set the password used to access the SFTP server |
| reset | Resets to defaults |

Notes: The **username** and **password** are limited to 127 characters each. Once captured, they are encrypted and stored in the reader’s persistent partition.

If the **username** and/or **password** are properly specified as part of the URI, the reader will not use the stored credentials.

The **reset** sub-command will remove the stored credentials from the reader, as will a **config image default** command.

4.2.5 Config RFID Menu

The **config rfid** menu allows the user to set parameters of the Reader’s RFID control interface. The parameters are shown in the following table.

Table 4.24: Config RFID Command Parameters

| Command | Description |
|------------|--|
| resetstats | Reset the current RFID statistics. |
| llrp | Submenu of LLRP-specific configuration commands. |
| interface | Submenu of RFID interface configuration. |

Config RFID ResetStats Command

The **config rfid resetstats** command resets the RFID statistics maintained by the Reader.

An example of the command and response is shown below:

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

Config RFID LLRP Command

The **config rfid llrp** command allows the user to configure the LLRP implementation. The parameters are shown in the following table.

Table 4.25: Config RFID LLRP Commands

| Command | Description |
|------------|--|
| connclose | Initiate a manual close of the current LLRP connection. If no connection exists, a status code of '8-Permission-Denied' will be returned. |
| factory | Resets the LLRP configuration to its factory defaults. Deletes all configured RO Specs and Access Specs and restores the factory default LLRP configuration. This action resets only in-band configuration, not configuration items controlled by RShell. Note that this command will be rejected with a status code of '8-Permission-Denied' if a LLRP client connection exists |
| resetstats | Reset the current LLRP specific statistics maintained by the Reader. |

Config RFID LLRP Inbound Commands

The `config rfid llrp inbound` command provides a submenu of client-initiated connection configuration commands. Currently only the `tcp` subcommand is supported, which has its own series of subcommands, as described in the following table.

Table 4.26: Config RFID LLRP Inbound TCP Command Parameters

| Command | Argument | Format | Description |
|----------|----------------|---------|--|
| port | <port number> | integer | Configure the port on which TCP connections are accepted. Default is IANA-assigned port of 5084 for the standard LLRP connections (security set to none) and port 5085 for secure LLRP connections (security set to encrypt). |
| service | on off | enum | Turn on or off LLRP client-initiated TCP connections to the Reader. Disabling this service will cause 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. Current LLRP connections are not affected by this command. |
| security | none encrypt | enum | Selecting none will disable validation and encryption. Selecting encrypt will encrypt but not validate data over the LLRP connection. |

Note: Usage of port 5085 is not allowed for standard LLRP connections (security set to **none**) and usage of port 5084 is not allowed for usage of secure LLRP connections (security set to **encrypt**).

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

Usage: `config rfid llrp inbound tcp service <on|off>`

Usage: `config rfid llrp inbound tcp security <none|encrypt>`

Config RFID LLRP Outbound Commands

The `config rfid llrp outbound` command leads to a submenu of Reader-initiated connection configuration commands, as shown in the following table.

Table 4.27: 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. A maximum of 5 servers can be added. The Reader will attempt to establish a connection to each of the servers in a round-robin manner. After a connection is established, the procedure will stop. If the connection is lost, the procedure will restart with the first configured server. |

| Command | Argument | Format | Description |
|---------|--------------------|----------------------|---|
| 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 be preconfigured for the command to succeed. |
| delall | | | Delete all remote hosts to which Reader attempts Reader-initiated LLRP connections. |
| open | <hostname> [:port] | string [:integer] | Attempt to open an LLRP connection to the specified remote host. and the host and port combination is not preserved. This command can only be used as a debugging aid. For normal scenarios using Reader-initiated connections, use the “add” command parameter. This command will always return the status ‘10,Command-Being-Processed’. The disposition of the connection after the command is immediately available. To determine if the connection was successful, use the summary command. |
| retry | <retry timeout> | integer | Configure the period in seconds between Reader-initiated connection attempts. The first number represents the minimum period between failed connection attempt and the second number represents the attempt by the Reader. The Reader will attempt a geometric progression back-off time between attempts if the retry timeout argument is provided. The Reader will attempt to connect to the remote host for 10 seconds, 10 seconds, 20 seconds, 40 seconds, etc. After a successful connection is established, the timeout is reset to the minimum value and the Reader will attempt a connection fails. |

| Command | Argument | Format | Description |
|----------|----------------------------------|---------|---|
| service | on off | enum | Turn on/off LLRP Reader-initiated connections. Disabling this service will prevent future connection attempts to be made. Enabling this service will cause the reader to resume connection attempts to any connected readers. Current LLRP connections are not affected by this command. |
| timeout | <timeout> | integer | Configure the timeout (in seconds) for Reader-initiated connections before the reader retries. If the TCP handshake has not completed within this timeout period, the next connection attempt is subject to the geometric back-off algorithm. On a high-latency WAN, one could tune this timeout higher so that the Reader waits longer for the handshake to complete before dropping the connection attempt. A failed handshake will invoke the retry timer. For more information, see the retry command entry. |
| security | none encrypt encryptvalidate | enum | Set security options for reader-initiated connections (TLS 1.2). You can disable the security for reader-initiated connections (none), enable encryption (encrypt), or enable encryption and peer validation (encryptvalidate). |

Note: The **security encryptvalidate** option supports only preinstalled certificates from well-known CAs.

Config RFID Interface Command

The **config rfid interface** command sets the RFID interface of the reader to either LLRP or REST. This command is only available on the R700 reader.

The **config rfid interface** command parameters are shown in the following table.

Table 4.28: Config RFID Interface Command Parameters

| Command | Description |
|---------|----------------------------------|
| llrp | Enable Impinj LLRP Interface. |
| rest | Enable Impinj RESTful Interface. |

You can configure the reader interface through the reader webpage as well. Select either **Impinj LLRP Interface** or **Impinj RESTful Interface** from the **Available Interfaces** menu in the **READER INTERFACE** section of the page and then click the **Update** button (figure 4.2). The page will update the setting information in the **Reader Interface** section on the left side.



Figure 4.2 Reader interface menu

4.2.6 Config SNMP Command

The **config snmp** menu allows the user to configure the SNMP settings for the Reader. The **config snmp** command parameters are shown in the following table.

Table 4.29: Config SNMP Command Parameters

| Command | Description |
|-------------|--|
| service | Enable/Disable the SNMP service. |
| trapservice | Enable/Disable SNMP trap service. |
| reset | Reset SNMP settings to default values. |
| access | Submenu of access specific commands. |
| write | Submenu of write specific commands. |
| epcg | Submenu of EPCglobal RM MIB specific commands. |
| trap | Submenu of trap specific commands. |
| version | Submenu of version specific commands. |
| v3 | Submenu of SNMP V3 specific commands. |

Config SNMP Service Command

The following table shows the **config snmp service** parameters.

Table 4.30: Config SNMP Service Command Parameters

| Command | Argument | Format | Description |
|---------|------------------|--------|--|
| service | enable disable | enum | Globally enable/disable the SNMP service. When the service is enabled, it is started, and when it is disabled, it is stopped. If the service is enabled when the system boots, the SNMP service will be started. |

Example to enable the service:

```
> config snmp service enable
Status='0,Success'
```

Config SNMP TrapService Command

The following table shows the **config snmp trapservice** parameters.

Table 4.31: Config SNMP TrapService Command Parameters

| Command | Argument | Format | Description |
|-------------|------------------|--------|---|
| trapservice | enable disable | enum | Globally enable/disable the SNMP trap service. When the service is enabled, it is started, and when it is disabled, it is stopped. If the service is enabled when the system boots, the SNMP service will be started. |

When the trapservice is enabled, the following standard traps are sent:

> **coldStart (.1.3.6.1.6.3.1.1.5.1)**

This trap is sent when the SNMP service is restarted. The SNMP service is restarted when SNMP parameters are changed.

> **nsNotifyShutdown (.1.3.6.1.4.1.8072.4.0.2)**

This trap is sent when a normal shutdown is requested (e.g. an rshell reboot request).

> **nsNotifyRestart (.1.3.6.1.4.1.8072.4.0.3)**

This trap is sent when the SNMP service is reconfigured. The SNMP service is reconfigured when certain systems settings are changed (e.g. when the hostname changes).

> **authenticationFailure (.1.3.6.1.6.3.1.1.5.5)**

This trap is an unknown community name is used in a V2c request or an unknown passphrase is used in a V3 request.

When the trapservice is enabled, the following custom (Impinj-defined) traps may be explicitly enabled:

> **impUnexpectedRestart (.1.3.6.1.4.1.25882.4.1)**

This trap is sent when the reader experiences an unexpected shutdown.

Note: The exact circumstances under which these traps may be sent is subject to change in future releases of the Octane and R700 firmware.

Example to enable the trapservice:

```
> config snmp trapservice enable
Status='0,Success'
```

Config SNMP Reset Command

This command resets the SNMP settings to the default values. There are no parameters required for this command.

Example to reset SNMP settings to default values:

```
> config snmp reset
Status='0,Success'
```

Config SNMP Access Command

The **config snmp access** command allows the user to configure the SNMP read and write access settings for the Reader. The **config snmp access** command parameters are shown in the following table.

Table 4.32: Config SNMP Access Command Parameters

| Command | Argument | Format | Description |
|---------------|---------------------|--------|--|
| rocommunity | <read-only string> | string | Sets the read-only community string for read access to SNMP attributes. |
| rwcommunity | <read-write string> | string | Sets the read-write community string for read-write access to SNMP attributes. If SNMP writes are disabled this string may still be used to read via SNMP. |
| trapcommunity | <trap string> | string | Sets the trap community string for allowing receipt of SNMP notifications from the reader. |

Note: The rocommunity and rwcommunity may not be set to the same string. Attempting to set both rocommunity and rwcommunity to the same string will result in the error: Status='3,Invalid-Parameter-Value'.

Example to set the rocommunity string to “my-read-only-password”:

```
> config snmp access rocommunity my-read-only-password
Status='0,Success'
```

Config SNMP Write Command

The **config snmp write** command allows the user to configure whether SNMP writes are allowed (enabled) or not (disabled). If writes are disabled, then SNMP writes are allowed (for any agents), even if the rwcommunity is set properly. If the SNMP service is enabled, writes are enabled, and the rwcommunity is set properly, then writable SNMP values can be modified. Note that no reader specific settings are currently writable via SNMP. Refer to the Octane SNMP document for more information. The **config snmp write** command parameters are shown in the following table.

Table 4.33: Config SNMP Write Command Parameters

| Command | Argument | Format | Description |
|---------|----------|--------|---|
| enable | all | string | Enable SNMP writes on all writeable objects. |
| disable | all | string | Disable SNMP writes on all writeable objects. |

Example to enable SNMP writes:

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

Config SNMP EPCG Command

The **config snmp epcg** menu provides control of the EPCglobal RM MIB. There are no direct subcommands and only one submenu, device, for this command.

Config SNMP EPCG Device Command

The **config snmp epcg device** command is used to configure epcg device settings. Currently, the device **role** is the only settings that can be configured. The **config snmp epcg device** command parameters are shown in the following table.

Table 4.34 Config SNMP EPCG Device Command Parameters

| Command | Argument | Format | Description |
|---------|----------|--------|---|
| role | <role> | string | The string that should be reported for device role. |

Example to configure the epcg device role to “my-reader-role”:

```
> config snmp epcg device role my-reader-role
Status='0,Success'
```

Config SNMP Trap Command

The **config snmp trap** command allows the user to configure whether sending SNMP traps from the reader are allowed (enabled) or not (disabled). The **config snmp trap** command parameters are shown in the following table.

Table 4.35: Config SNMP Trap Command Parameters

| Command | Argument | Format | Description |
|---------|----------|--------|--|
| enable | <trap> | string | Enable sending standard traps and the specified custom SNMP trap. Supported custom traps: unexpectedrestart |
| disable | <trap> | string | Disable sending standard traps and the specified custom SNMP trap. Supported custom traps: unexpectedrestart |
| sink | <host> | string | Hostname or IP address to receive SNMP notifications. |
| sink2 | <host> | string | Additional hostname or IP address to receive SNMP notifications. |
| sink3 | <host> | string | Additional hostname or IP address to receive SNMP notifications. |
| sink4 | <host> | string | Additional hostname or IP address to receive SNMP notifications. |
| delall | | | Clear all SNMP trap (notification) sinks. |
| port | <port> | string | UDP port to send SNMP traps to (default is 162). |

Note: The trap port setting applies to all SNMP trap sinks.

Note: The unexpected restart trap (.1.3.6.1.4.1.25882.4.1) is sent when the reader restarts due to an unexpected software or hardware error. Refer to the IMPINJ-ROOT-REG-MIB.mib file for more details.

Example to enable the unexpected restart trap:

```
> config snmp trap enable unexpectedrestart
Status='0,Success'
```

Config SNMP Version Command

The **config snmp version** command allows the user to configure whether SNMP version 2c and version 3 security models are enabled or disabled. Each model can be enabled or disabled separately. When version 2c is enabled, version 1 requests are also allowed (with the appropriate community string). The **config snmp version** command parameters are shown in the following table.

Table 4.36: Config SNMP Version Command Parameters

| Command | Argument | Format | Description |
|---------|------------------|--------|---|
| 2c | enable disable | enum | Enable the SNMP version 1 and 2c security model. When enabled, SNMP client applications can communicate with the reader using using the v1 or v2c protocol. |
| 3 | enable disable | enum | Enable the SNMP version 3 security model. When enabled, SNMP client applications can communicate with the reader using the v3 protocol. |

Note: Refer to the Octane SNMP documentation and the IMPINJ-ROOT-REG-MIB.mib file for more details on Octane SNMP support.

Example to enable version 2c security model support:

```
> config snmp version 2c enable
Status='0,Success'
```

Config SNMP V3 Command

The **config snmp v3** command allows the user to configure V3 security model specific parameters. Octane currently supports only one read-only user and no read-write users. The **config snmp v3** command parameters are shown in the following table.

Table 4.37: Config SNMP V3 Command Parameters

| Command | Argument | Format | Description |
|-----------------------|-----------------|--------|--|
| ro auth rouser | <username> | string | Specify the read-only username. |
| ro securitylevel | <noauth auth> | enum | Specify authentication and/or encryption of read-only user requests. |
| ro auth passphrase | <passphrase> | string | Specify read-only authentication passphrase. |

| Command | Argument | Format | Description |
|-------------------|-----------------|---------------|--|
| ro auth method | <MD5> | enum | Specify read-only authentication method. |

Note: Refer to the Octane SNMP documentation and the IMPINJ-ROOT-REG-MIB.mib file for more details on Octane SNMP support.

Example to set the authentication method for the read-only user:

```
> config snmp v3 ro auth method MD5
Status='0,Success'
```

Config Version Compatibility

Support for version 2c and version 3 get requests can be enabled or disabled independently.

Only version 2c traps are supported.

Version 2c traps are sent if both the SNMP service and trapservice are enabled (and appropriate sink, port and trapcommunity values are set).

Version 2c read (get, getnext, and walk) requests are supported if the SNMP service is enabled and version 2c is enabled (and the appropriate rocommunity is set).

Version 3 read (get, getnext, walk) requests are supported if the SNMP service is enabled and version 3 is enabled (and the appropriate v3 values are set).

4.2.7 Config System Menu

This menu allows configuration of the system operating region, time and identification parameters. See the following table for a description of the configuration system command parameters.

Warning: By changing the Reader’s operating region, you are changing the Reader’s RF settings. The RF settings must match the country or region of operation to comply with local laws and regulations. You, the user, are responsible to ensure operation with the correct RF settings and are solely responsible for any fines and other damages due to incorrect or non-compliant country/region settings on your Reader.

Table 4.38: Config System Command Parameters

| Command | Argument | Format | Description |
|-------------|----------------------|---------|--|
| contact | <contact string> | string | Configure the system contact. ASCII characters are allowed, except for single and double quotes. Double and single quotes can only be used if the leading and trailing characters of the string has white space. |
| description | <description string> | string | Configure the system description. ASCII characters are allowed, except for single and double quotes. Double and single quotes can only be used if the leading and trailing characters of the string has white space. |
| location | <location string> | string | ASCII characters are allowed, except for single and double quotes. Double and single quotes can only be used if the leading and trailing characters of the string has white space. |
| name | <name string> | string | ASCII characters are allowed, except for single and double quotes. Double and single quotes can only be used if the leading and trailing characters of the string has white space. |
| region | <region number> | Integer | Certain Reader models permit the user to select an alternate operating region. Each operating region is encoded as an integer. Alternate regions (if available) can be found by issuing a show system region command. |

| Command | Argument | Format | Description |
|---------|--------------|--|--|
| time | <time value> | MMDDhhmmCCYY MM.DD-hh:mm:ss CCYY.MM.DD- hh:mm:ss CCYY.MM.DD- hh:mm hh:mm:ss hh:mm | Configure the system time. Time must be entered in one of the approved formats. If the year is set explicitly when setting the time, the year must be at least 2000. Also, the date may not be greater than January 2038. See Note below. |
| power | | | Submenu of power specific configuration commands. |

Note: To use this command to set the system time, you must disable the NTP service (“config network ntp disable”). Failure to do so will result in a “Permission-Denied” error.

A sample command that sets the system location to “my-reader-location” is shown below:

```
> config system location my-reader-location
Status='0,Success'
```

A sample command that sets the system time is shown below: (Time is set to April, 27th 1:11:00 p.m. 2012.)

```
> config system time 042713112012
Status='0,Success'
```

Config System Power Command

Readers that support transmit power of 36 dBm ERP (Effective Radiated Power) as covered in the ETSI EN 302 208 draft specification, must be powered by a DC power supply or a Power-over-Ethernet switch that supports PoE+.

For these readers, the Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol (CDP) is used to try to negotiate power with the PoE+-capable Ethernet switch, though not all PoE+ switches support software-based negotiation of LLDP/CDP.

LLDP/CDP is enabled by default on readers that require PoE+ power, but can be disabled with **config system power source auto**, or reenabled with **config system power source poe** or **config system power source poe+**.

The **config system power** command might only be available in the Impinj R700 RAIN RFID Reader and later models.

Note: When the LLDP/CDP service is disabled and the Ethernet PoE+ switch cannot allocate sufficient electrical power, running an RO Spec on the reader may result in the reader rebooting or browning out.

| Command | Argument | Format | Description |
|---------|----------------------|---------|---|
| source | PoE PoE+ Auto | enum | The power source (PoE or Power over Ethernet, PoE plus, or automatic negotiation). |
| timeout | <milliseconds> | integer | The maximum time to negotiate the power source with a PoE switch. Only used if source is set to auto . Can delay startup if the PoE switch is slow to send LLDP power information. |

Reader products that do not require PoE+ do not use LLDP/CDP and the rshell commands are unsupported:

```
> config system power source poe+
Status='7,Unsupported-Command'
> config system power timeout 20000
Status='7,Unsupported-Command'
```

Config System Region Command

Use this command to set the operating region. Regions can be found by issuing a **show system region** command as shown below:

```
> show system region
```

Regions are set using **config**:

```
> config system region [region]
Status='0, Success'
```

| Status | Description |
|--------|--|
| 0 | Success - set to the current region |
| 3 | Invalid-Parameter-Value |
| 8 | Permission-Denied - region unavailable |
| 14 | Success - set to different region. Requires reboot |

Changes to the Reader’s operating region do not take effect until the next reboot. Attempts to execute RFID operations on the Reader after you change the region but before you reboot the Reader will cause unexpected behavior.

4.2.8 Config Feature Menu

The **config feature** menu allows the user to activate, enable and disable features in the Reader. The command parameters are shown in the following table.

Table 4.39: Config Features Command Parameters

| Command | Description |
|----------|--------------------------------|
| activate | Activates a specified feature. |
| enable | Enables an active feature. |
| disable | Disables an active feature. |

Config Feature Activate Command

The following table shows the **config feature activate** parameters.

Table 4.40: Config Feature Activate Command Parameters

| Argument | Format | Description |
|----------------|---------|--|
| <feature name> | enum | Activates the specified <feature name>, with a valid <key>. |
| <key> | integer | |
| [<type>] | enum | Optionally, a feature might need an additional <type> parameter. |

Config Feature Enable and Disable Commands

The **config feature enable** command allows the user to enable a feature. The **config feature disable** command allows the user to disable a feature. The parameter for each command is shown in the following tables.

Table 4.41: Config Feature Enable and Disable Command Parameters

| Command | Argument | Format | Description |
|---------|----------------|--------|---|
| enable | <feature name> | enum | Enable <feature name>. See the following table for the list of supported features. |
| disable | <feature name> | enum | Disable <feature name>. See the following table for the list of supported features. |

Table 4.42: Supported Enable/Disable Features

| Feature | Description |
|---------|---|
| anthub | The Impinj Antenna Hub (available on R120 and R420) |

For example, to enable the Antenna Hub feature:

```
> config feature enable anthub
Status='0,Success'
```

And to disable the Antenna Hub feature:

```
> config feature disable anthub
Status='0,Success'
```

4.3 Show Command

The **show** command has several submenus, as shown in the following table, and described in the following sections.

Table 4.43: Show Command Parameters

| Command | Description |
|--------------------|---------------------------------------|
| 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. |
| feature | Submenu of feature status commands. |
| version 7.4 anthub | Submenu of anthub status commands. 51 |

4.3.1 Show Image Menu

The **show image** menu contains commands that are shown in the following table.

Table 4.44: Show Image Command Parameters

| Command | Description |
|----------|--|
| metafile | Displays information about the current upgrade metafile. If no metafile has ever been successfully downloaded, only a subset of the available fields are shown. See the following table for command responses. |
| summary | Displays the Reader's image information. See the following table. |
| version | Displays all version information for a partition on the current image. |

The upgrade command, **UpgradeStatus** can take any of the arguments values shown in the following table. For each abnormal status, a reason parameter is given to indicate the reason for the status. The reason values are also given in the following table.

Table 4.45: Show Image Metafile Response Parameters

| Argument | Format | Description |
|-----------------|--------------------------------------|--|
| MetafileUri | string | The current upgrade metafile URI. |
| RetrieveMode | Manual Auto | The current retrieve mode. |
| RetrievePeriod | integer | The current retrieve period, present only mode is auto . This period is specified in |
| UpgradeMode | auto forced | The upgrade mode in use if the metafile is currently available |
| CommitMode | immediate scheduled wait-4-cmd | The commit mode if metafile is currently available |
| CommitTime | string | The scheduled commit time, which is present only if the commit mode is set to scheduled . The format is <timezone-yyyy-mm-dd-hh-mm-ss>. Current time zone GMT is supported. |
| EarlyActOk | yes no | Indicates whether an early activation of the upgrade image is allowed if the commit mode is scheduled . Present only if the metafile has the early-act-ok field. |
| DownloadRetries | integer | Number of times to retry a failed download |

| Argument | Format | Description |
|---------------------|--|---|
| DownloadRetryPeriod | integer | Number of seconds between retry attempts. |
| ReaderModelName | string | The model name of the Reader. This indicates the model section of the metafile was used to create the Reader. |
| ImageType | integer | Firmware image upgrade file type (present in the metafile). |
| DownloadMode | immediate fixed-delay <delay> random-delay <delay> | Indicates the current download mode. For fixed or random delay, the DownloadDelay field indicates the corresponding the delay value. |
| DownloadDelay | integer | For fixed delay, this is a constant offset. For random delay, this is the maximum value for a random delay offset. |
| ImageFileUri | uri | URI from which the file image is retrieved. |

Examples of possible **show image summary** command responses are shown in the following two tables, along with the corresponding field formats. A code example follows these two tables.

Table 4.46: Show Image Summary Response Parameters

| Argument | Format | Description |
|---------------|--|---|
| UpgradeStatus | Ready WaitingForMetafileTransfer WaitingForMetafileRetry ProcessingMetafile DeterminingNeedForImageFile WaitingForImageFileTransfer WaitingForImageFileRetry ProcessingImageFile WaitingForCommitImage SchedulingActivation | The upgrade status of the last executed upgrade. The following enumerations are possible values for the UpgradeStatus field. Application is ready for additional commands. Metafile is being transferred from server. Metafile transfer timed out, waiting for subsequent transfer. Metafile was received and is being validated. Version information is being examined to determine if the image file needs to be retrieved. Image file is being transferred from server. Image file transfer timed out, waiting for subsequent transfer. Image file is being validated. Image file is being committed to flash memory. Image activation is being scheduled. |

| Argument | Format | Description |
|---------------------|----------------------------|--|
| | WaitingToActivateImmediate | Image is being activated, and will be followed by immediate reboot. |
| | WaitingToActivateScheduled | Image is being activated, and reboot is scheduled based on user specified commit time. |
| | WaitingRandomRebootDelay | System is in the random delay window (provided as part of commit time specification) prior to system reboot. |
| | WaitingForFallback | A config image fallback command is being processed and preparing to reboot the system. |
| | WaitingForCDR | A config image default command is being processed and preparing to reboot the system. |
| LastOperation | WaitingForRequestedReboot | Reader is about to be rebooted. This supplements the UpgradeStatus field to give a reason for the status. This is only displayed or provided in conjunction with the next line (LastOperationStatus). Typically status reasons are provided only when additional information is required, such as under error scenarios or when a system reboot has been scheduled. This generally reports the condition leading up to the current status. |
| | Unknown Host | Download failed because of an unknown host. |
| | Unsupported Scheme | Download failed because of unsupported URI scheme (only FTP, HTTP, TFTP and SFTP 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, such as for a bad password. |
| LastOperationStatus | Not Matching Metafile | Upgrade image did not match the version specified in the metafile. |
| | Bad File Format | Bad upgrade image file format. |
| | Bad CRC | Bad image CRC. |

| Argument | Format | Description |
|-----------------|-------------------------------------|---|
| | No Matching Hardware Version | Image file does not contain a hardware version that matches the Reader hardware version. |
| | 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. |
| | Missing SOP | Metafile does not contain SOP partition while an SPP 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. |

| Argument | Format | Description |
|-----------------|----------------------------|--|
| UpgradeStatus | | The upgrade status of the last executed upgrade. The following enumerations are possible values for the UpgradeStatus field. |
| | Ready | Application is ready for additional commands. |
| | WaitingForMetafileTransfer | Metafile is being transferred from server. |
| | WaitingForMetafileRetry | Metafile transfer timed out, waiting for subsequent transfer. |

| Argument | Format | Description |
|-----------------|------------------------------------|--|
| | ProcessingMetafile | Metafile was received and is being validated. |
| | DeterminingNeedForImageFileVersion | Information is being examined to determine if the image file needs to be retrieved. |
| | WaitingForImageFileTransfer | Image file is being transferred from server. |
| | WaitingForImageFileRetry | Image file transfer timed out, waiting for subsequent transfer. |
| | ProcessingImageFile | Image file is being validated. |
| | WaitingForCommitImage | Image file is being committed to flash memory. |
| | SchedulingActivation | Image activation is being scheduled. |
| | WaitingToActivateImmediate | Image is being activated, and will be followed by immediate reboot. |
| | WaitingToActivateScheduled | Image is being activated, and reboot is scheduled based on user specified commit time. |
| | WaitingRandomRebootDelay | System is in the random delay window (provided as part of commit time specification) prior to system reboot. |
| | WaitingForFallback | A config image fallback command is being processed and preparing to reboot the system. |
| | WaitingForCDR | A config image default command is being processed and preparing to reboot the system. |
| | WaitingForRequestedReboot | Reader is about to be rebooted. |
| LastOperation | | This supplements the UpgradeStatus field to give a reason for the status. This is only displayed or provided in conjunction with next line (LastOperationStatus). Typically status reasons are provided only when additional information is required, such as under error scenarios or when a system reboot has been scheduled. This generally reports the condition leading up to the current status. |

| Argument | Format | Description |
|---------------------|-------------------------------------|---|
| | Unknown Host | Download failed because of an unknown host. |
| | Unsupported Scheme | Download failed because of unsupported URI scheme (only FTP, HTTP, TFTP and SFTP 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. |
| LastOperationStatus | Not Matching Metafile | Upgrade image did not match the version specified in the metafile. |
| | Bad File Format | Bad upgrade image file format. |
| | Bad CRC | Bad image CRC. |
| | No Matching Hardware Version | Image file does not contain a hardware version matching the Reader hardware version. |
| | 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. |
| | Missing SOP | Metafile does not contain SOP partition while an SPP 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. |

| Argument | Format | Description |
|-----------------|---------------|--|
| | Generic Error | Download error other than those specified above. |

Table 4.47: Show Image Summary Response Parameters (continued)

| Argument | Format | Description |
|---------------------------------|---------------|--|
| PrimaryImageType | integer | The image type number for the primary image (10). |
| PrimaryImageState | enum | The current state of the primary image (this should always be Active). Refer to the Show Image Summary Response Parameters Table for details of image state values. |
| PrimaryImageSystem-Version | string | The version of the primary image’s system OS partition. |
| PrimaryImageConfig-Version | string | The current version of the primary image’s persistent partition. ‘255.255.255.255’ is the default SPP version. |
| PrimaryImage-CustomApp-Version | string | The version of the primary image’s custom application partition. This displays only if CAP is present. |
| SecondaryImageType | integer | The image type number for the secondary image (10). If the secondary image is not valid this argument is not shown. |
| SecondaryImageState | enum | The current state of the secondary image would typically have one of the values from the Show Image Summary Response Parameters table. If the secondary image is not valid this argument is not shown. |
| SecondaryImageSystem-Version | string | The version of the secondary image’s system OS partition. If the secondary image is not valid this argument is not shown. |
| SecondaryImageConfig-Version | string | The current version of the secondary image’s persistent partition. ‘255.255.255.255’ is the default SPP version. If the secondary image is not valid this argument is not shown. |
| SecondaryImageCustom-AppVersion | string | The version of the primary image’s custom application partition. This displays only if CAP is present. If the secondary image is not valid this argument is not shown. |

An example:

```
> show image summary
Status='0,Success'
UpgradeStatus='Ready'
PrimaryImageType='10'
PrimaryImageState='Active'
PrimaryImageSystemVersion='5.2.0.240'
PrimaryImageConfigVersion='255.255.255.255'
PrimaryImageCustomAppVersion='1.0.0.0'
SecondaryImageType='10'
SecondaryImageState='Active'
SecondaryImageSystemVersion='4.12.0.240'
SecondaryImageConfigVersion='255.255.255.255'
SecondaryImageCustomAppVersion='1.0.0.0'
```

Image State

An image state has four possible values, active, pre-active, pending, and obsolete, which are described in the following table.

Table 4.48: Image State Values

| State Value | Meaning |
|-------------|---|
| Active | Image has been previously run and is eligible to fallback to. |
| Pre-Active | Image has been activated and is ready to become the Primary image on next reboot. |
| Pending | Image has been committed to flash memory, waiting for commit time to move it to the Pre-Active state. |
| Obsolete | Image has been invalidated, typically due to a fallback operation |

4.3.2 Show Logging Menu

The **show logging** menu displays the logging configuration for the system and for displaying the actual logged information in text form. The commands are described in the following table. Log entries are shown in chronological order, with the most recent entry displayed last.

Response parameters for the **show logging** events and the **show logging summary** command (which displays the summary of response parameters along with security levels) are shown in the

following tables.

Table 4.49: Show Logging Command Parameters

| Command | Arguments | Format | Description |
|---------|------------------------------|------------------|---|
| events | (err app) <event count> | enum, integer | Uses the event count number to determine how many of the last internal log entries to display. |
| summary | | | Displays the current user logging configuration. The “Show Logging Summary Response Parameters” table displays the summary of response parameters along with severity levels. |

Table 4.50: Show Logging Events Response Parameters

| Argument | Format | Description |
|----------|--------|---|
| Event1 | string | The string responses from the log events. |
| Event2 | string | |
| ... | ... | ... |
| Event<n> | string | |

The following table displays the summary of response parameters along with severity levels.

Table 4.51: Show Logging Summary Response Parameters

| Argument | Format | Description |
|-----------------|---|-----------------------------------|
| Managementlevel | Emergency Alert Critical Error Warning Notice Info Debug | Log severity level for Management |
| RFIDLevel | | Log severity level for RFID |
| SystemLevel | | Log severity level for System |

Samples of the commands are shown below:

```
> show logging summary
Status='0,Success'
ManagementLevel='Error'
SystemLevel='Error'
RFIDLevel='Error'
```

> **show logging events app 3**

Status='0,Success'

Event1='Dec 4 00:22:46 (none) sshd[20090]: lastlog_openseek: Couldn't stat /var/log/lastlog: No such file or directory'

Event2='Dec 4 00:22:53 (none) Rshell: User entered "show logging summary" '

Event3='Dec 4 00:22:53 (none) Rshell: ICTL target syslogconf returned status 0 '

4.3.3 Show Network Menu

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 the following table, while the response parameters are shown in the tables that follow this table.

Table 4.52: Show Network Menu Commands

| Command | Description |
|-----------------|------------------------------------|
| dns | Summary of DNS settings |
| icmp | ICMP statistics |
| dnssd | Summary of DNSSD settings |
| mdns | Display current status of mDNS |
| ntp | Summary of NTP settings |
| summary | Summary of network settings |
| tcp | TCP statistics |
| udp | UDP statistics |
| http | Http server status |
| https | Https server status |
| ftp | FTP server status |
| ssh | SSH server status |
| portsecurity | Port Security Settings |
| sftp | SFTP settings |
| lldp | Display LLDP status |
| wlan (sub-menu) | WiFi adapter configuration submenu |
| ip (sub-menu) | IP statistics submenu |

The **lldp** and **wlan** commands might only be available in Reader models prior to the Impinj R700 RAIN RFID Reader.

Table 4.53: Show Network DNS Response Parameters

| Argument | Format | Description |
|------------------|------------|--|
| Domain<n>Static | string | Statically configured domain (if configured) |
| Domain<n>Dynamic | string | DNS domain obtained from DHCP (if available) |
| Server<n>Static | ip address | Address of the Nth static DNS server |
| Server<n>Dynamic | ip address | Address of the Nth dynamic DNS server |

Table 4.54: Show Network ICMP Response Parameters

| Argument | Format | Description |
|----------------------|---------|--------------------|
| icmpInMsgs | integer | See MIB-2 RFC 1213 |
| icmpInErrors | integer | |
| icmpInDestUnreachs | integer | |
| icmpInTimeExcds | integer | |
| icmpInParmProbs | integer | |
| icmpInSrcQuenchs | integer | |
| icmpInRedirects | integer | |
| icmpInEchos | integer | |
| icmpInEchoReps | integer | |
| icmpInTimestamps | integer | |
| icmpInTimestampReps | integer | |
| icmpInAddrMasks | integer | |
| icmpInAddrMaskReps | integer | |
| icmpOutMsgs | integer | |
| icmpOutErrors | integer | |
| icmpOutDestUnreachs | integer | |
| icmpOutTimeExcds | integer | |
| icmpOutParmProbs | integer | |
| icmpOutSrcQuenchs | integer | |
| icmpOutRedirects | integer | |
| icmpOutEchos | integer | |
| icmpOutEchoReps | integer | |
| icmpOutTimestamps | integer | |
| icmpOutTimestampReps | integer | |
| icmpOutAddrMasks | integer | |
| icmpOutAddrMaskReps | integer | |

Table 4.55: Show Network mDNS Response Parameters

| Argument | Format | Description |
|------------|---|--|
| mDNSStatus | enabled disabled NotAvailableOnCurrentInterface | Indicates the current state of the mDNS service. When the active interface is cellular and the status is enabled , it shows as NotAvailableOnCurrentInterface. |

Table 4.56: Show Network HTTP Response Parameters

| Argument | Format | Description |
|----------------|--------------|--|
| ServiceEnabled | True False | Indicates whether or not the service will be started at boot time. |

Table 4.57: Show Network HTTPS Response Parameters

| Argument | Format | Description |
|----------------|--------------|--|
| ServiceEnabled | True False | Indicates whether or not the service will be started at boot time. |

Table 4.58: Show Network SSH Response Parameters

| Argument | Format | Description |
|----------------|--------------|--|
| ServiceEnabled | True False | Indicates whether or not the service will be started at boot time. |

Table 4.59: Show Network FTP Response Parameters

| Argument | Format | Description |
|----------------|--------------|--|
| ServiceEnabled | True False | Indicates whether or not the service will be started at boot time. |

Table 4.60: Show Network NTP Response Parameters

| Argument | Format | Description |
|---|--|--|
| ServiceEnabled | True False | Indicates whether or not the NTP service will be started at boot time. |
| DynamicServersEnabled | True False | Indicates whether or not NTP servers discovered via DHCP will be included in the list of NTP servers. |
| Synchronized | True False | Indicates whether or not the NTP service has successfully synchronized with an NTP server. |
| SynchronizedServer | string IP Address | If the NTP service has successfully synchronized with an NTP server, that server IP address or hostname is specified here. |
| NtpServerDynamic<n>-Address NtpServerStatic<n>-Address | string IP Address | Hostname or IP address of the Nth static or dynamic NTP server |
| NtpServerDynamic<n>-State NtpServerStatic<n>-State | 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 successfully communicated with the server eight times. During this process, the <i>NtpServerDynamic/Static<n>Reach</i> parameter will generally transition through 3, 7, 17, 37, 77, 177, and 377. When the Reader has selected a server and locked on to it, the state parameter will become Synchronized . |
| NtpServerDynamic<n>-Stratum NtpServerStatic<n>-Stratum | integer | The current stratum number of the NTP server. |

| Argument | Format | Description |
|----------------------------|---------|--|
| NtpServerDynamic<n>- Reach | integer | The reachability register of the NTP server. |
| NtpServerStatic<n>- Reach | | |

Note: If a pooled NTP server, such as pool.ntp.org, is specified as a dynamic or static NTP server, rshell may not be able to correctly display the NTP server status in the NtpServerDyanamic<n>-Xxx or NtpServerStatic<n>-Xxx response parameters. The Synchronized and SynchronizedServer response parameters will, however, display the correct state.

Note: The “show network ntp” command will display any avialable dynamic NTP servers and any previously configured static NTP servers, whether or not the NTP service is enabled. If the NTP service is disabled, only the server names are displayed. If the NTP service is enabled, the name and status for each NTP server will be displayed.

Table 4.61: Show Network Summary Response Parameters

| Argument | Format | Description |
|------------------|--------|---|
| PrimaryInterface | string | The primary network device enabled at start (e.g. ‘eth:eth0’ for Ethernet). |
| ActiveInterface | string | The currently active network device, such as ‘eth:eth0’ for Ethernet. |
| Hostname | string | The current hostname of the Reader. |

| Argument | Format | Description |
|------------------|--|--|
| connectionStatus | AdminUp Connected Disconnected | The connection status of the current active interface. The value is one of the following: <ul style="list-style-type: none">• AdminUp: Interface is started but not yet connected. This state is temporary.• Connected: Interface is up and running.• Disconnected: Interface is down. |
| ipAddressMode | Dynamic Static | Indicates the current configuration of the network interface. Dynamic (using DHCP for IP configuration) or Status (using manual IP configuration). |
| ipAddress | IP address | Reports the current IP address assigned to the Reader. This value will not be reported if it is not currently assigned or the network is disconnected. |
| ipMask | IP address | Reports the current IP address mask assigned to the Reader. If not currently assigned or network disconnected, this value will not be reported. |
| gatewayAddress | IP address | Reports the current network gateway assigned to the Reader. This value will not be reported if it is not currently assigned or the network is disconnected. |

| Argument | Format | Description |
|------------------|------------|--|
| broadcastAddress | IP address | Reports the current IP broadcast address assigned to the Reader. This value will not be reported if it is not currently assigned or the network is disconnected. |

Table 4.62: Show Network IP Stat Response Parameters

| Argument | Format | Description |
|-------------------|---------|--------------------|
| ipForwarding | integer | See MIB-2 RFC 1213 |
| ipDefaultTTL | integer | |
| ipInReceives | integer | |
| IpInHdrErrors | integer | |
| ipInAddrErrors | integer | |
| ipForwDatagrams | integer | |
| ipInUnknownProtos | integer | |
| ipInDiscards | integer | |
| ipInDelivers | integer | |
| ipOutRequests | integer | |
| ipOutDiscards | integer | |
| ipOutNoRoutes | integer | |
| ipReasmTimeout | Integer | |
| ipReasmReqds | integer | |
| IpReasmOKs | integer | |
| IpReasmFails | integer | |
| ipFragOKs | integer | |
| ipFragFails | integer | See MIB-2 RFC 1213 |
| ipFragCreates | integer | |
| IpRoutingDiscards | integer | |

Table 4.63: Show Network IP Summary Response Parameters

| Argument | Format | Description |
|------------------|---|---|
| connectionStatus | AdminUp Connected Disconnected MismatchedModem Unauthorized | Current state of the network interface. |

| Argument | Format | Description |
|------------------|------------------|---|
| ipAddressMode | Dynamic Static | If configuration is currently dynamic, the dynamic values returned by DHCP are given. If a value is not currently set (such as the gateway address when LLA is in use,) the argument does not appear. |
| ipAddress | IP address | |
| IpMask | IP address | |
| gatewayAddress | IP address | |
| broadcastAddress | IP address | |

Table: Show Network LLDP Response Parameters

| Argument | Format | Description |
|------------------------|---|---|
| ServiceEnabled | True False | Indicates whether or not the service will be started at boot time. |
| PoePlusRequired | True False | Indicates whether or not the reader requires PoE+ to ramp full power. |
| NegotiationState | Unknown PowerRequested PowerAllocated Error | The state of the reader/switch LLDP/CDP negotiation. When a PoE power injector or a switch that does not support LLDP is used, the state will remain Unknown. When an LLDP/CDP switch is used, after the switch responds, the state is PowerAllocated. See RequiredPowerAvailable to tell if power requirements can be met. |
| RequiredPowerAvailable | True False | After LLDP/CDP negotiation, this is True if the PoE+ switch can supply enough electrical power to the reader. |
| RequestedPower | integer | Power in milliwatts that the reader has requested from the Poe+ switch. |
| AllocatedPower | integer | Power in milliwatts that the switch has allocated to the PoE port. |

The **show network lldp** command might only be available in Reader models prior to the Impinj R700 RAIN RFID Reader.

An example of successful LLDP/CDP negotiation with a PoE+ switch that can meet the reader's

power requirements:

```
> show network lldp
Status='0,Success'
ServiceEnabled='True'
PoePlusRequired='True'
RequestedPower='20000'
AllocatedPower='25500'
NegotiationState='PowerAllocated'
RequiredPowerAvailable='True'
```

An example of the LLDP/CDP state for a PoE+ switch that has not replied to a power negotiation request or a power injector that does not support LLDP/CDP. In this state, the reader assumes that there is sufficient electrical power and will allow RFID operation.

```
> show network lldp
Status='0,Success'
ServiceEnabled='True'
PoePlusRequired='True'
RequestedPower='0'
AllocatedPower='0'
NegotiationState='Unknown'
RequiredPowerAvailable='AssumedTrue'
```

Example of LLDP/CDP status after a successful negotiation, but full power requirements cannot be met. In this state, an LLRP ROSpec will not be run and an LLRP error will result since the reader may reset as it increases RF power past the switch's capacity to supply power.

```
> show network lldp
Status='0,Success'
ServiceEnabled='True'
PoePlusRequired='True'
NegotiationState='PowerAllocated'
RequiredPowerAvailable='False'
RequestedPower='20000'
AllocatedPower='13000'
```

Reader products that do not require PoE+ do not use LLDP/CDP and the rshell command is unsupported:

```
> show network lldp
Status='7,Unsupported-Command'
```

The description for all arguments displayed in the following two tables are described in MIB-2 RFC 1213.

Table 4.64: Show Network TCP Response Parameters

| Argument | Format | Description |
|-----------------|---------|--------------------|
| tcpRtoAlgorithm | integer | See MIB-2 RFC 1213 |
| tcpRtoMin | integer | |
| tcpRtoMax | integer | |
| tcpMaxConn | integer | |
| tcpActiveOpens | integer | |
| tcpPassiveOpens | integer | |
| tcpAttemptFails | integer | |
| tcpEstabResets | integer | |
| tcpCurrEstab | integer | |
| tcpInSegs | integer | |
| tcpOutSegs | integer | |
| tcpRetransSegs | integer | |
| tcpInErrs | integer | |
| tcpOutRsts | integer | |

Table 4.65: Show Network UDP Response Parameters

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

Table 4.66: Show Network Wlan Summary Response Parameters

The **show network wlan command** might only be available in Reader models prior to the Impinj R700 RAIN RFID Reader.

| Argument | Format | Description |
|------------------|---|---|
| NetType | adhoc infra | The WiFi network type. |
| FeatureStatus | Disabled NotSupportedByHW NotSupportedOnPoE | Present if WLAN is not supported, in which case all other fields are absent. Disabled: Feature is explicitly disabled for whatever reason. Currently not supported. NotSupportedByHw: The hardware does not support WiFi feature. NotSupportedOnPoE: WiFi feature not supported when Reader is powered over Ethernet. |
| ConnectionStatus | AdminDown Searching Disconnected Connected | See the Show Network Summary Response Parameters table. |
| DeviceStatus | Absent Loading Loaded | Present only when connectionStatus is not Connected or Searching . Indicates the WiFi device status. Absent: The USB WiFi module is not plugged in. Loading: The WiFi driver is loading. Loaded: The WiFi driver is loaded. |
| SSID | String | The SSID of the currently connected network. |
| BSSID | MAC Address | The BSSID of the currently connected AP for infrastructure network. Or the (random) BSSID of the adhoc network initiator. |
| SignalLevel | <integer>dBm | The signal level of the currently connected AP. |
| MyMacAddress | MAC Address | The Mac address of the Reader's WiFi card. |
| PeerMacAddress | MAC Address | Present on in adhoc network. The MAC address of the i'th station that is connected on the ahoc network. |

The **show network wlan config active/persistent** command shows the configuration that is currently active, or that is in persistent storage.

Table 4.67: Show Network Wlan Config Active/Persistent

| Argument | Format | Description |
|----------|------------------------------|--|
| NetType | adhoc infra | The active/persistent network type. |
| SSID | String | The active/persistent SSID. |
| Keymgmt | wpa-psk wpa-none none | The active/persistent Key management protocol. |
| Encrypt | wpa2 wpa none | The active/persistent encryption type. |

| Argument | Format | Description |
|----------|--------|---|
| PSK | String | The active/persistent preshared key shown as ***** if set, otherwise empty. |

Table 4.68: Show Network Wlan Scanlist Response Parameters

| Argument | Format | Description |
|----------------|---------------|---|
| NetType<i> | adhoc infra | The i'th BSSID's network type |
| BSSID<i> | MAC address | The BSSID of the i'th AP |
| SSID<i> | String | The SSID of the i'th AP. |
| Security<i> | String | The i'th AP's security settings, e.g. 'WPA2PSK/AES' |
| Frequency<i> | <integer>Mhz | The i'th AP's channel as represented by the MHz |
| SignalLevel<i> | <integer>dBm | The i'th AP's signal level. |

Table 4.69: Show Network SFTP Response Parameters

| Argument | Format | Description |
|----------|--------|---|
| Username | string | Shows '...' if the username is stored, otherwise empty ("") |
| Password | string | Shows '...' if the password is stored, otherwise empty ("") |

4.3.4 Show RFID Menu

The **show rfid** menu contains commands to display RFID parameters and statistics. Submenu commands are shown in the following table.

Table 4.70: Show RFID Command Parameters

| Command | Description |
|-----------|---|
| Stat | Display RFID statistics for the Reader. |
| Interface | Show enabled RFID Interface. |
| Llrp | Leads to submenu of LLRP status statistics. |

Show RFID Stat

The **show rfid stat** command displays the RFID statistics for that Reader. See the following table for the complete stat response parameters.

Table 4.71: Show RFID Stat Response Parameters

| Argument | Format | Description |
|------------------------------------|--------------------|--|
| LastStatisticReset | integer | The elapsed time [in seconds] since the RFID statistics were last reset. |
| ReaderOperational- Status | enabled disabled | Indicates whether RFID applications are running on the Reader. |
| ReaderAdministrative- Status | enabled | Desired status by administration is always enabled. |
| Antenna<n>- Administrative- Status | enabled | Desired status of antenna by administration - always enabled. |

| 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 LLRP checks of antenna status have been performed, the Reader will report unknown for this statistic. Once an RFID operation has occurred, or an in-band check is performed, the Reader will update this value. Enabled=connected antenna Disabled=disconnected from antenna. Note that accurate reports are only available on in-use antennas. Antennas currently not in use are not checked. |
| Antenna<n>Last- PowerLevel | integer | 100 times the dBm setting of Antenna <n>. |
| Antenna<n>Last- NoiseLevel | integer | Always 0. |
| Antenna<n>- Energized- Time | integer | Time Antenna <n> has been powered, in milliseconds. |
| Antenna<n>Unique- InventoryCount | integer | Number of unique tags seen at Antenna <n>. |

| Argument | Format | Description |
|---------------------------------|---------------|---|
| Antenna<n>Total-InventoryCount | integer | Total Inventory Count for Antenna <n>. |
| Antenna<n>Failed-InventoryCount | integer | Always 0. |
| Antenna<n>Read-Count | integer | Number of tags read at Antenna <n> that matched the configured filters. |
| Antenna<n>Failed-ReadCount | integer | Number of tags where a read was attempted at Antenna <n> because the tag matched the configured filters, but the read failed. |
| Antenna<n>-WriteCount | integer | Number of tags written at Antenna <n> that matched the configured filters. |
| Antenna<n>Failed-WriteCount | integer | Number of tags where a write was attempted at Antenna <n> because the tag matched the configured filters, but the write failed. |
| Antenna<n>-LockCount | integer | Number of tags locked at Antenna <n> that matched the configured filters. |
| Antenna<n>Failed-LockCount | integer | Number of tags where a lock was attempted at Antenna <n> because the tag matched the configured filters, but the lock failed. |

| Argument | Format | Description |
|------------------------------|---------|---|
| Antenna<n>Kill- Count | integer | Number of tags killed at Antenna <n> that matched the configured filters. |
| Antenna<n>Failed- KillCount | integer | Number of tags where a kill was attempted at Antenna <n> because the tag matched the configured filters, but the kill failed. |
| Antenna<n>- EraseCount | integer | Number of tags erased at Antenna <n> that matched the configured filters. |
| Antenna<n>Failed- EraseCount | integer | Number of tags where a erase was attempted at Antenna <n> because the tag matched the configured filters, but the erase failed. |

Show RFID Interface Command

The **show rfid interface** command displays the enabled RFID interface. Here is an example of successfully showing the RFID interface, changing it, and then showing the new interface.

```
> show rfid interface
Status='0,Success'
interface='Impinj LLRP Interface'
> config rfid interface rest
Status='0,Success'
> show rfid interface
Status='0,Success'
interface='Impinj RESTful Interface'
```

This command is only available on the R700 reader.

Show RFID LLRP Commands

The **show rfid llrp** command provides statistics on the LLRP interface and includes the subcommands listed in the following table.

Table 4.72: Show RFID LLRP Command Parameters

| Command | Argument | Format | Description |
|--------------|----------|---------|---|
| accessspec | id | integer | Displays the XML text of a specified AccessSpec. |
| capabilities | | | Displays the XML text of the LLRP capabilities advertised by this Reader. Note: For readers that support more than one region, the capabilities may not be accurate if no region is selected. |
| config | | | Displays the XML text of the LLRP configuration. |
| inbound | | | Displays information about LLRP client-initiated connections. |
| outbound | | | Displays information about LLRP Reader-initiated connections. |
| region | | | Displays the LLRP region and Impinj sub-region at which the Reader is currently operating. Also will display sub-regulatory region information when configured by LLRP extensions. |
| rospec | id | integer | Displays the XML text of a specified ROSpec. |
| stat | | | Reports LLRP statistics. |
| summary | | | Displays a summary of the LLRP configuration and status. |

Show RFID LLRP Outbound Command

This command displays information about LLRP Reader-initiated connections. Here is an example of successfully showing this information.

```
> show rfid llrp outbound
Status='0,Success'
LLRPOutboundTCPEnabled='True'
LLRPOutboundRetrySec='5'
LLRPOutboundTimeoutSec='2'
LLRPOutboundSecurity='None'
LLRPOutboundTCPServer1=""
LLRPOutboundTCPServer2=""
```

```

LLRPOutboundTCPServer3="
LLRPOutboundTCPServer4="
LLRPOutboundTCPServer5="
>

```

4.3.5 Show SNMP Menu

The **show snmp** menu displays information about the SNMP configuration. The following table provides a list of the available **show snmp** subcommands.

Table 4.73: Show SNMP Command Parameters

| Command | Description |
|---------|--|
| all | Displays all of the the SNMP settings. |
| summary | Displays summary of generic SNMP settings. |
| epcg | Displays EPCG RM MIB specific settings. |

The response parameters for **show snmp summary** and for **show snmp epcg** are shown in the following two tables. The response parameters for **show snmp all** is a concatenation of the summary and **epcg** response parameters.

Table 4.74: Show SNMP Summary Response Parameters

| Argument | Format | Description |
|---------------|--------------------|--|
| SnmService | Enabled Disabled | The status of the SNMP service. |
| ROCommunity | string | The value of the read-only community string. |
| RWCommunity | string | The value of the read-write community string. |
| TrapCommunity | string | The value of the trap community string. |
| WriteEnabled | True False | Indicates whether SNMP writes are enabled or disabled. |
| TrapService | Enabled Disabled | The status of the SNMP trap service. |
| Sink | string | The hostname or IP address that will receive SNMP traps. |
| Sink2 | string | Additional hostname or IP address to receive SNMP traps. |
| Sink3 | string | Additional hostname or IP address to receive SNMP traps. |
| Sink4 | string | Additional hostname or IP address to receive SNMP traps. |

| Argument | Format | Description |
|----------|--------|---|
| Port | string | The UDP port that SNMP traps will be sent to. |

Table 4.75: Show SNMP EPCG Response Parameters

| Argument | Format | Description |
|-------------------------------------|--------|--|
| EpcgRmMib-Revision | string | The Epcglobal Reader management MIB revision, example. 200703080000Z. |
| EpcgRdrDev-Description | string | Reader description: The same value that is reported for SNMP system description. |
| EpcgRdrDevRole | string | The value of the configured device role. |
| EpcgNotifChan-Name1 | string | The name of notification channel 1. Always the LLRP Client. |
| EpcgNotifChan-Name2 | string | The name of notification channel 2. Always the LLRP Reader. |
| EpcgRdrDevOper-StateEnable | string | Indicates whether Reader operation state change notifications are enabled. Always False . |
| EpcgRdrDevOperNotif-StateLevel | string | The severity level for Reader operation state change notifications. Always Error . |
| EpcgReadPointOper-StateNotifyEnable | string | Indicates whether read point operation state notifications are enabled. Always False . |
| EpcgReadPointOper-NotifyStateLevel | string | The severity level for read point operation state change notifications. Always Error . |
| EpcgSrcOper-StatusNotifEnable | string | Indicates whether source state change notifications are enabled. Always False . |
| EpcgSrcOper-StatusNotifyLevel | string | The severity level for source state change notifications. Always Error . |
| EpcgNotifChan-OperNotifEnable | string | Indicates whether notification channel operation state change notifications are enabled. Always False . |
| EpcgNotifChan-OperNotifLevel | string | The severity level for notification channel operation state change notifications. Always Error . |

4.3.6 Show System Menu

The **show system** menu displays information about the state of the Reader. The following table provides a list of the available **show system** subcommands. The next four tables after that summarize the respective response parameters.

Table 4.76: Show System Command Parameters

| Command | Description |
|----------|---|
| cpu | Displays statistics regarding platform memory usage and available application space |
| platform | Displays generic platform statistics |
| summary | Displays a summary of system info |
| region | Displays alternative regions options (if any) |
| power | Display powersource info (LLDP status) |

Table 4.77: Show System CPU Response Parameters

| Argument | Format | Description |
|---------------------------------|---------|---|
| TotalMemory | integer | Total available RAM in bytes |
| FreeMemory | integer | Total free RAM in bytes |
| CpuUtilization | integer | CPU utilization in percent |
| TotalConfiguration-StorageSpace | integer | Total configuration/persistent partition space in bytes |
| FreeConfiguration-StorageSpace | integer | Free configuration/persistent partition space in bytes |
| TotalApplication-StorageSpace | integer | Total application partition space in bytes |
| FreeApplication-StorageSpace | integer | Free application partition space in bytes |

Table 4.78: Show System Platform Response Parameters

| Argument | Format | Description |
|----------------------|---------|---|
| BootEnv- Version | integer | Internal 'Boot Environment' data version |
| Hardware- Version | string | Returns the hardware version information for the Reader and internal hardware. |
| IntHardware- Version | | |
| SerialNumber | string | Returns the Reader's hardware serial number for thr Reader and internal hardware. |
| IntSerialNumber | | |
| MACAddress | string | MAC address of the unit's Ethernet port. |
| HLAVersion | string | Returns the High Level Assembly (HLA) information for the Reader. |

| Argument | Format | Description |
|-------------------|--|---|
| RegionsValid | integer[,integer,...] | Indicates the numerical values of the regions supported on this hardware. |
| FeaturesValid | integer[,integer,...] | Indicates features enabled on this hardware. |
| BIOSVersion | string | Returns the version information for the Reader BIOS. |
| PTN | integer.integer | Product Type Number This is used to differentiate Reader models. |
| UptimeSeconds | integer | Time since last reboot in seconds. |
| BootStatus | integer | Bootloader status. This indicates various boot errors detected by the boot loader. |
| BootReason | Cold Processor Reboot External Watchdog External Watchdog Fallback | The reason for the last reboot. A Cold reboot occurs when power is first applied to the Reader. Processor / Reboot occurs when software causes a reboot. External Watchdogs are the result of the Reader being reset by the embedded watchdog feature. An External Watchdog Fallback occurs after repeated watchdog resets and an automatic rollback of the image (if available). |
| PowerFailTime | integer | Linux time of last power fail expressed in seconds. Only defined for the first boot following a power failure. |
| ActivePowerSource | PoE jack | Indicates power source as either Power over Ethernet (PoE) or power jack. |

Table 4.79: Show System Summary Response Parameters

| Argument | Format | Description |
|-------------|--------|---|
| SysDesc | string | The system description. Defaults to model name of the Reader. |
| SysContact | string | The system contact information. Defaults to 'unknown'. |
| SysName | string | The system name. Defaults to hostname of the Reader. |
| SysLocation | string | The system location. Defaults to 'unknown'. |
| SysTime | string | The current time on the Reader in UTC. |

Table 4.80: Show System Region Response Parameters

| Argument | Format | Description |
|-----------------------|-----------------------|---|
| Operating- Region | integer | Current operating region number. |
| Selectable- Regions | integer[,integer,...] | Available operating region numbers. |
| Selectable- Region<n> | integer,string | List of the available operating region numbers along with a short descriptive string. <n> starts at zero. |

Table 4.81: Show System Power Response Parameters

| Argument | Format | Description |
|------------------------|---|---|
| ServiceEnabled | True False | Indicates whether or not the service will be started at boot time. |
| NegotiationTimeout | integer | The maximum time to negotiate the power source, in milliseconds. |
| PoePlusRequired | True False | Indicates whether or not the reader requires PoE+ to ramp full power. |
| NegotiationState | Unknown PowerRequested PowerAllocated Error | The state of the reader/switch LLDP/CDP negotiation. When a PoE power injector or a switch that does not support LLDP is used, the state will remain Unknown. When an LLDP/CDP switch is used, after the switch responds, the state is PowerAllocated. See RequiredPowerAvailable to tell if power requirements can be met. |
| RequiredPowerAvailable | True False | After LLDP/CDP negotiation, True if the PoE+ switch can supply enough electrical power to the reader. |
| RequestedPower | integer | Power in milliwatts that the reader has requested from the PoE+ switch. |
| AllocatedPower | integer | Power in milliwatts that the switch has allocated to the PoE port. |

| Argument | Format | Description |
|-------------|-------------------|--|
| PowerSource | PoE PoE+ Auto | The power source (PoE or Power over Ethernet, PoE plus, or automatic negotiation). |

The **show system power** command might only be available in the Impinj R700 RAIN RFID Reader and later models.

An example of successful LLDP/CDP negotiation with a PoE+ switch that can meet the reader's power requirements:

```
> show system power
Status='0,Success'
ServiceEnabled='True'
NegotiationTimeout='20000'
PoePlusRequired='True'
RequestedPower='20000'
AllocatedPower='25500'
NegotiationState='PowerAllocated'
RequiredPowerAvailable='True'
PowerSource='auto (PoE+)'
```

An example of the LLDP/CDP state for a PoE+ switch that has not replied to a power negotiation request or a power injector that does not support LLDP/CDP. In this state, the reader assumes that there is sufficient electrical power and will allow RFID operation.

```
> show system power
Status='0,Success'
ServiceEnabled='True'
NegotiationTimeout='20000'
PoePlusRequired='True'
RequestedPower='0'
AllocatedPower='0'
NegotiationState='Unknown'
RequiredPowerAvailable='AssumedTrue'
PowerSource='auto (PoE)'
```

Example of LLDP/CDP status after a successful negotiation, but full power requirements cannot be met. In this state, an LLRP ROSpec will not be run and an LLRP error will result since the reader may reset as it increases RF power past the switch's capacity to supply power.

```
> show system power
Status='0,Success'
ServiceEnabled='True'
NegotiationTimeout='20000'
PoePlusRequired='True'
NegotiationState='PowerAllocated'
RequiredPowerAvailable='False'
RequestedPower='20000'
AllocatedPower='13000'
PowerSource='auto (PoE)'
```

Reader products that do not require PoE+ do not use LLDP/CDP and the rshell command is unsupported:

```
> show system power
Status='7,Unsupported-Command'
```

4.3.7 Show Feature Menu

The **show feature** menu displays information regarding features enabled on the Reader. The following table provides a list of the available parameters. The table after that summarizes the respective response parameters for the Antenna Hub feature. The **show feature all** command includes all the feature response parameters defined in this section.

Table 4.82: Show Feature Command Parameters

| Command | Description |
|---------|--|
| all | Display information for all defined features. |
| stp2 | Display information for the STP2 feature group. |
| anthub | Display information for the Antenna Hub feature. |

Table 4.83: Show Feature Anthub Response Parameters

| Argument | Format | Description |
|------------------|-------------------------|---|
| anthubKey-Status | Activated Deactivated | R120 and R420 always display Activated, All others display Deactivated. |
| anthubStatus | Enabled Disabled | Operational status of the Antenna Hub feature. |

4.3.8 Show Anthub Command

The **show anthub** command has a parameter as shown in the following table.

Table 4.84: Show Anthub Command Parameters

| Command | Description |
|---------|-----------------------------------|
| summary | Display a summary of Anthub info. |

The **show anthub summary** command has a response as shown in the following table.

Table 4.85: Show Anthub Summary Response

| Argument | Format | Description |
|--------------------------------|---|---|
| FeatureStatus | Enabled Disabled | Displays whether anthub mode is configured as enabled or disabled. |
| AntennaHub[n] ConnectionStatus | Unknown Disconnected Connected | Indicates if an Antenna Hub was detected at boot up. ‘Unknown’ indicates that the feature was disabled at boot up. Note that this field is not dynamically updated. |
| AntennaHub[n] Fault | None RF power RF power seen on Hub n Not initialized Serial | |
| AntennaHub[n] FWVersion | string | Displays the version of firmware that is running on the Antenna Hub microcontroller. |
| AntennaHub[n] PCBVersion | string | Displays the Antenna Hub’s hardware version. |
| AntennaHub[n] SerialNumber | string | Displays the Antenna Hub’s serial number. |

5 Revision History

| Date | Revision | Comments |
|------------|----------|--|
| 04/02/2009 | 1.0 | Initial release |
| 04/20/2009 | 1.1 | Updated for first release |
| 08/27/2009 | 4.2 | Added SNMP support Added mDNS and LLA support Updated Upgrade error message for a non-matching hardware version between the image file and the Reader. Clarified LLRP connection management Added comment for “show image summary” that secondary parameters/values are only shown if the secondary image is valid. Corrected strings to match RShell counterparts. |
| 02/24/2010 | 4.4 | Finalized for release Added DNS-SD support Updated status code table with new values |
| 03/05/2010 | 4.4 | Added cellular and GPS support. |
| 03/31/2010 | 4.4 | Added “show network dnssd” to show http status |
| 10/27/2010 | 4.6 | Updates for Octane 4.6 release |

| Date | Revision | Comments |
|-------------|-----------------|--|
| 4/25/2011 | 4.8 | Updates for Octane 4.8 release Added: Config System Region Command Added: Config Image RemoveCAP Command Added: Config Feature Command Added: Show System Region Command Added: Show Feature Command Added: Warning regarding changing region Added: Configuration for wlan Other minor clarifications |
| 5/20/2012 | 4.10 | Updates for Octane 4.10 release Added: Antenna Hub feature |
| 12/16/2014 | 5.2 | Updates for Octane 5.2 release |
| 5/29/2015 | 5.4 | Updates for Octane 5.4 release Added: portsecurity feature for wire 802.1x configuration support Added: SFTP as a supported protocol and related commands to set credentials |
| 9/2/2015 | 5.6 | Updates for Octane 5.6 release Added: SNMP trap and V3 support |
| 12/21/2015 | 5.6.2 | Updates for Octane 5.6.2 release |
| 10/10/2016 | 5.8 | Updates for Octane 5.8 release, including |
| 11/29/2016 | 5.10 | Updates for Octane 5.10 release Modified: zeroconf related RShell Commands Modified: config network ip command requires a reboot |
| 2/21/2017 | 5.12 | Updates for Octane 5.12 release Modified: allowed syslog servers. Modified: Document the NTP service before changing NTP set |

| Date | Revision | Comments |
|-------------|-----------------|---|
| 5/15/2017 | 5.12 | Updated for R120 support. Removed spec of antennas with or without Antenna Hub command. |
| 1/30/2020 | 7.00 | Updated for Octane 7.00 release and R70. Supplemented lldp commands with power |
| 5/15/2020 | 7.1 | Updated for Octane 7.1 release. Included and show/config rfid interface. |

6 Notices

Copyright © 2020, Impinj, Inc. All rights reserved.

Impinj gives no representation or warranty, express or implied, for accuracy or reliability of information in this document. Impinj reserves the right to change its products and services and this information at any time without notice.

EXCEPT AS PROVIDED IN IMPINJ'S TERMS AND CONDITIONS OF SALE (OR AS OTHERWISE AGREED IN A VALID WRITTEN INDIVIDUAL AGREEMENT WITH IMPINJ), IMPINJ ASSUMES NO LIABILITY WHATSOEVER AND IMPINJ DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATED TO SALE AND/OR USE OF IMPINJ PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT.

NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY PATENT, COPYRIGHT, MASK WORK RIGHT, OR OTHER INTELLECTUAL PROPERTY RIGHT IS GRANTED BY THIS DOCUMENT.

Impinj assumes no liability for applications assistance or customer product design. Customers should provide adequate design and operating safeguards to minimize risks.

Impinj products are not designed, warranted or authorized for use in any product or application where a malfunction may reasonably be expected to cause personal injury or death or property or environmental damage ("hazardous uses") or for use in automotive environments. Customers must indemnify Impinj against any damages arising out of the use of Impinj products in any hazardous or automotive uses.

Impinj, GrandPrix™, Indy®, Monza®, Octane™, QT®, Speedway®, STP™, True3D™, xArray®, and xSpan® are trademarks or registered trademarks of Impinj, Inc. All other product or service names are trademarks of their respective companies.

These products may be covered by one or more U.S. patents. See <http://www.impinj.com/patents> for details.

For more information, contact support@impinj.com