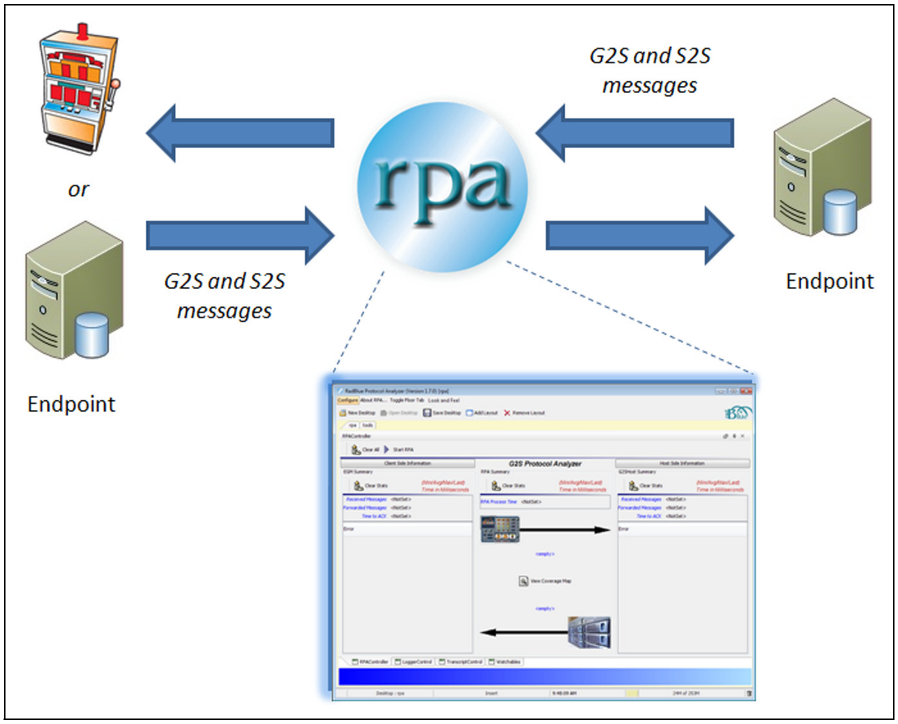
Protocol Analyzer

Radical Blue Gaming
Incredibly Innovative Gaming Solutions
85 Keystone Avenue Suite F Reno, Nevada 89503 775.329.0990 www.radblue.com

What Is the Protocol Analyzer?

The Protocol Analyzer verifies that G2S or S2S messages sent between two endpoints have been implemented according to GSA messaging standards.

These two endpoints consist of a system on one end, and an EGM, a kiosk or a system on the other end. The Protocol Analyzer sits between the two endpoints, receives messages from each side, verifies the messages, and forwards them on to their destination.



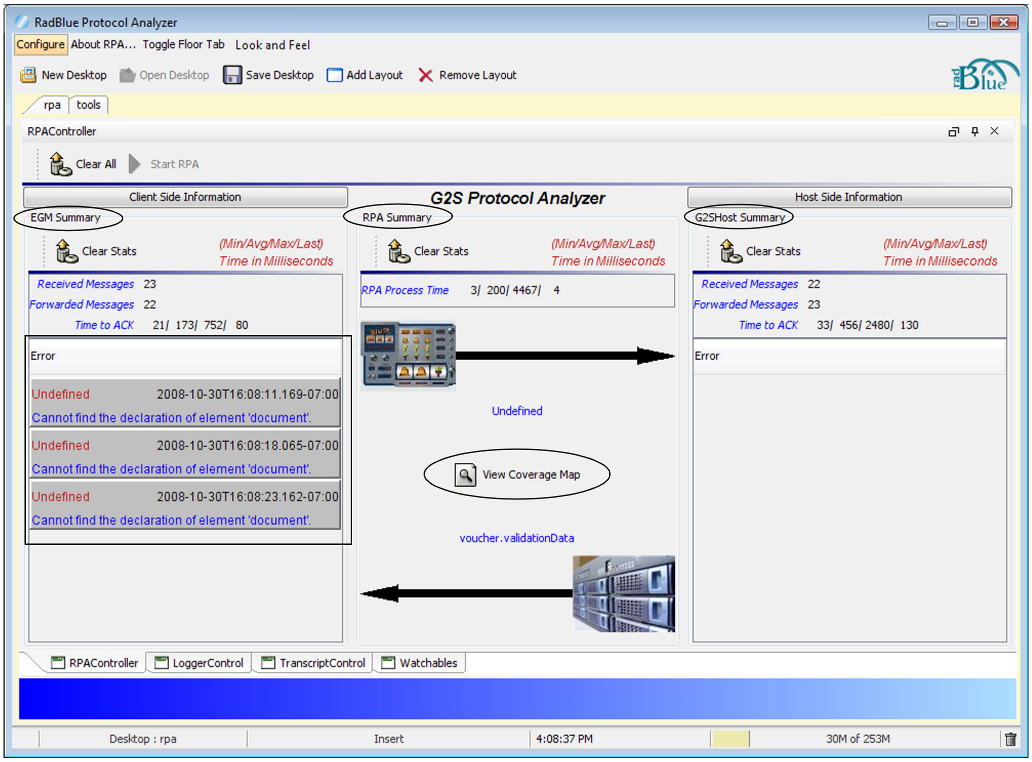
The Protocol Analyzer lets you view messages as they are passed between the two endpoints. You can:

- view all messages
- set up specific message types on a “watch” list
- easily identify any non-compliant messages
- view the **.xml** document behind any message
- use custom protocol schemas for validating messages
- generate a report of all communication errors

For more information, contact Russ Ristine at: 775.329.0990 or Russ@RadBlue.com

How Does the Protocol Analyzer Work?

From the main screen, you can configure both endpoints, start and stop the Protocol Analyzer, and view processing statistics and messaging errors.



Received Messages 23
Forwarded Messages 22
Time to ACK 21/ 173/ 752/ 80

RPA Process Time 3/ 200/ 4467/ 4

Received Messages 22
Forwarded Messages 23
Time to ACK 33/ 456/ 2480/ 130

Error

Undefined 2008-10-30T16:08:11.169-07:00
Cannot find the declaration of element 'document'.

Undefined 2008-10-30T16:08:18.065-07:00
Cannot find the declaration of element 'document'.

Undefined 2008-10-30T16:08:23.162-07:00
Cannot find the declaration of element 'document'.

Undefined

voucher.validationData

Error

- The **Summary** section provides statistics about the messages received from each endpoint.
- The **Coverage Map** is a quick lookup for commands that have been sent to Protocol Analyzer. It displays the command and the number of times the command has been sent.
- The **Error** section displays any messages with errors received from either the host or client endpoint.

A **Transcript Control** screen allows you to view all received messages, to mark records as needed for troubleshooting or testing, to perform searches of all received messages, and to view the XML content of any received messages.

What Do I Need to Get Started?

The minimum requirements for computers running the Protocol Analyzer are:

- Operating System: Windows XP, Windows Vista, or Linux
- Memory: 2 GB
- Hard Drive: 120 GB
- Disk Space: 250 MB
- Processor: Intel 2.8 Ghz or comparable
- Evaluation License from RadBlue to try out the tool

For more information, contact Russ Ristine at: 775.329.0990 or Russ@RadBlue.com

What Are Disruptive Filters?

Disruptive filters provide additional (optional) RPA functionality that lets you manipulate selected commands received by RPA to test system and EGM functionality. All supported commands and events are available for filtering.

There are two types of disruptive filters: automatic and interactive. Automatic filters *do not* require any additional user input once they are configured. Interactive filters, once configured, require manual handling of the specified command(s).

For automatic filters, you configure the parameters for each active filter. If an individual filter is active in the current automatic filter set, configuration changes to that filter are applied immediately (no restart required). The automatic filter set randomly chooses a filter to apply from the active filters in the set.The following list briefly describes each filter and its effect when applied to an encountered G2S message:

Filter	Description
Add Valid Attribute Filter	You specify the location within the message (g2sBody, g2sMessage, Class, Command and Sub-Element), and RPA adds a new attribute in a valid third-party namespace.
Add Valid Element Filter	You specify the location within the message (g2sBody, g2sMessage, Class, Command and Sub-Element), and RPA adds a new element in a valid third-party namespace.
Application-Level Error Filter	This filter acts on responses *only*. If the specified command is a request, it is not affected. You select an application-level or command class error from a list. The error is added to the response and RPA forwards it to the intended recipient. The response may originate from an EGM or a host.
Change Host ID/EGM ID Filter	This filter lets you modify the host ID and/or EGM ID within a message, which tests whether the target entity validates these attributes for each received message. This filter can affect the g2sBody attributes and/or the SOAP elements.
Duplicate Message Filter	This filter duplicates a message from one to 10 times. For the automatic filter, you define the minimum and maximum number of times the message should be duplicated.Duplicate copies of the message are resent as soon as the `g2sAck` response is received. A `g2sAck` command response is sent to the originator after all duplicate messages have been sent.
Event Data Filter	This filter removes associated data from selected events. You can remove class meters, device meters, all meters, transaction data, status information, or have RPA randomly choose for you.

Filter	Description
Message Delay Filter	Interactive filter messages are delayed while waiting for user input. Messages that are not acted upon within a user-specified amount of time are automatically forwarded to the target entity. For automatic filter messages, the filter configuration includes a delay range (X to Y seconds), after which the message is forwarded to the recipient.
Message-Level Error Filter	Select a message-level error from list. The error replaces the `g2sAck` to the originator, and the original message is *not* forwarded to the recipient.
Resend Filter	The resend filter drops the specified message without sending a `g2sAck` to the originator (so the originator realizes the message was lost).
Retry Filter	The retry filter drops the specified message, but sends a `g2sAck` to the originator (so the originator thinks the message was sent successfully).
Toggle Session Type Filter	This filter changes the *sessionType* attribute for the specified message. You can replace the session type with valid data (for example, change “request” to “notification”) or replace the session type with invalid data (changed to “RBG_junk”).