



Service Managed Gateway™

How to Configure RIP on a SMG

Issue 1.0
Date 26 March 2009

1	About this document	3
1.1	Scope	3
1.2	Readership	3
1.3	More information.....	3
1.4	Terminology	3
2	Introduction	4
2.1	How does the SMG implement RIP?.....	4
3	Configuring the SMG.....	5
3.1	Configuring RIP on the SMG	5
3.1.1	Configure the RIP IP system	6
3.1.2	Configure RIP on an interface.....	9
3.1.3	Configure RIP version 2 on an interface.....	13
4	Diagnostics.....	15
4.1	Routing Table	15
4.2	Trace analyzer.....	15
4.3	Tracing using the command line.....	17
4.3.1	Command line syntax	17

Copyright 2009 Virtual Access (Irl) Ltd. This material is protected by copyright. No part of this material may be reproduced, distributed, or altered without the written consent of Virtual Access. All rights reserved. Third party trademarks are the property of the third parties.

1 About this document

This document describes how to configure the Service Managed Gateway (SMG) for Routing Information Protocol (RIP).

1.1 Scope

This document explains how to:

- Configure the SMG for RIP
- Utilise the diagnostic and trace analyzer tools in the SMG

1.2 Readership

This document is for engineers who have previous experience configuring and managing networks.

1.3 More information

For more information about managing the SMG, read the Service Managed Gateway documentation. The current documentation is available online at <http://virtualaccess.com/smgdocs/>

1.4 Terminology

SLA	Service Level Agreement
SMG	Service Managed Gateway
RIP	Routing Information Protocol
IGP	Interior Gateway Protocol
PC	Personal Computer
SNMP	Simple Network Management Protocol
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
Eth-0	SMG Ethernet Interface number 0
SYN	TCP synchronise sequence number flag
MMS	Maximum Segment Size
TTL	Time to Live

2 Introduction

The Routing Information Protocol (RIP) is a dynamic routing algorithm used on IP-based Internet networks. The Internet is a network of hosts interconnected via gateways. Generally, hosts and gateways are presented with IP datagrams addressed to a host.

In general, the term 'packet' applies to any message formatted as a packet, while the term datagram is generally reserved for packets of an 'unreliable' service. A 'reliable' service is one that notifies the user if delivery fails, while an 'unreliable' one does not notify the user if delivery fails.

Routing is the method by which the host or gateway decides where to send the datagram. A routing protocol supply's the information required to do the routing.

A distance-vector routing algorithm is used by RIP to assist in maintaining network convergence. It uses a metric or 'hop' count as the primary routing criteria. Each route is advertised with the number of hops a datagram would take to reach the destination network. The maximum metric for RIP is 15. This limits the size of the network that RIP can support. Smaller metrics are more efficient-based on the cost associated with each metric.

RIP protocol is most useful as an 'Interior Gateway Protocol' (IGP). An IGP refers to the routing protocol used within a single autonomous system. There may be a number of autonomous systems, using different routing protocols, combined together to form a large network.

2.1 How does the SMG implement RIP?

- The router supports RIP for dynamic management of IP routing tables.
- RIP eliminates the need to establish static IP routing tables.

RIP configuration composes of two parts:

1. System-wide configuration commands that apply to all interfaces where RIP is enabled.
2. Interface-specific commands to allow for different RIP behaviour for different interfaces.

3 Configuring the SMG

The Service Managed Gateway (SMG) contains an internal web server that is used to configure the SMG. Before you can access the internal web server and start the SMG configuration, you must ensure that your PC has the correct networking set up.

To enable and configure connections on your SMG, the gateway must be correctly installed, and a valid service must be configured on it.

When your Service Managed Gateway is correctly connected to your PC, type fast.start into the URL line of your browser to display the Start page.

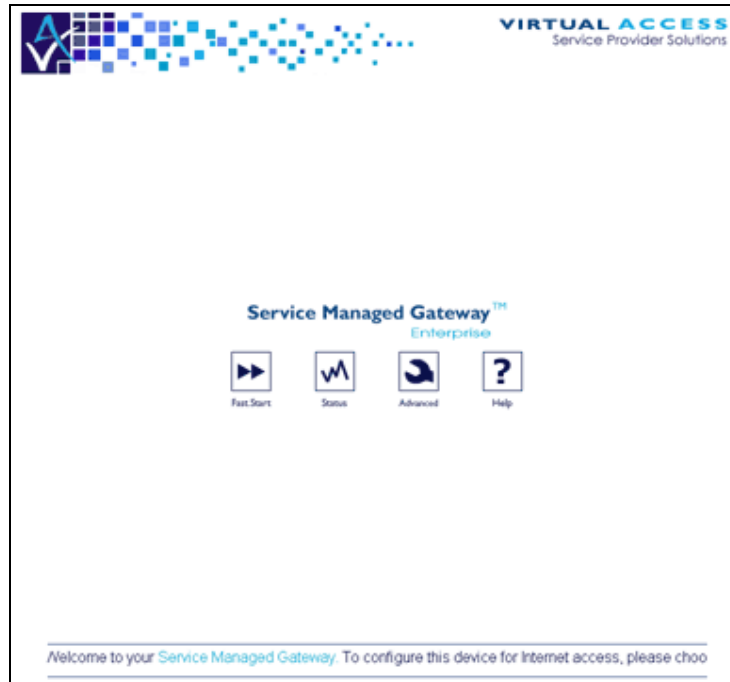


Figure 1: The SMG start page

If a login page appears type in the login password you received from your administrator.

If you have not received a password, contact the Virtual Access Support team.

Access the Fast Start Wizard by clicking the Fast.Start icon on the Start page of the embedded web.

The Fast Start Wizard will guide you through a series of forms that you must complete to configure your SMG.

3.1 Configuring RIP on the SMG

To configure RIP, on the SMG Start page, click **Advanced**. The Advanced menu appears.

In the left-hand menu, click **Expert View**.

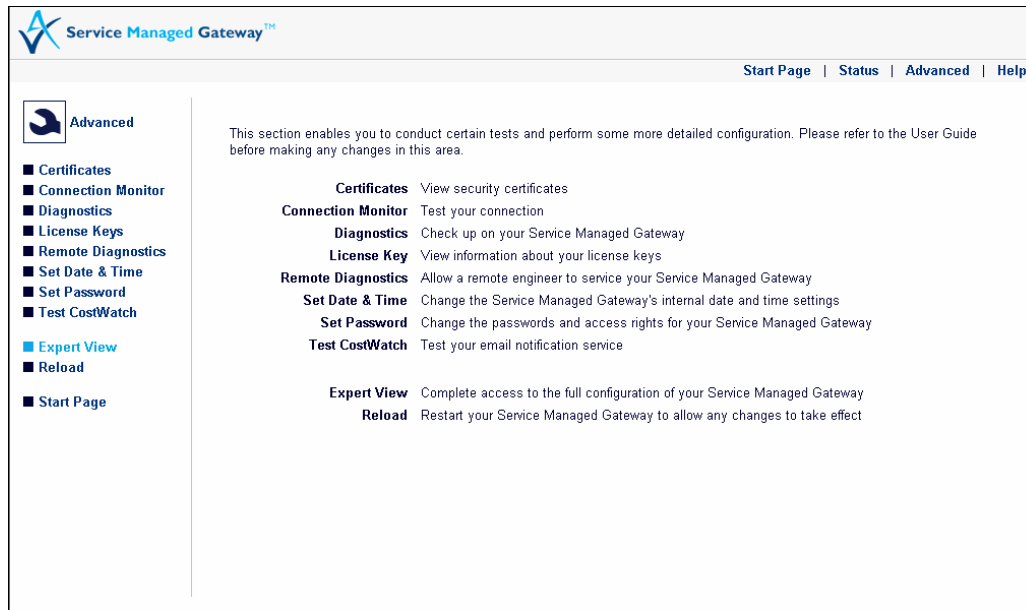


Figure 2: The Advanced menu showing Expert View

3.1.1 Configure the RIP IP system

The IP system RIP configuration pages allow configuration that applies to all interfaces that have RIP enabled.

In the Expert View menu, select **System -> IP -> system**. The System page appears. To view the advanced options, click **Advanced**. The advanced options are in red.

IP System

Default TTL

Reassembly Timeout secs

RIP Enabled

RIP Spoof Enabled

RIP TTL

RIP Response Interval secs

RIP Route Aging Timeout mins

RIP Next Hop Zero Enabled

TCP Adjust MSS

TCP SYN Retry Count

TCP Retransmission Timeout ms

TCP Keepalive Timeout secs

TCP Keepalive Interval secs

Management Address Enabled

Management IP Address

Figure 3: The advanced IP system page

Field	Description	Command Line				
Default TTL	Not available to RIP.					
Reassembly Timeout	Not available to RIP.					
RIP Enabled	<p>Enables or disables RIP. When enabled, RIP provides automatic routing by requesting each router's table and building routes based on the responses.</p> <p>Periodic updates are sent by RIP routers to ensure that neighbouring RIP routers are up to date.</p> <table border="1"> <tr> <td>yes</td> <td>Enables RIP.</td> </tr> <tr> <td>no</td> <td>Disables RIP.</td> </tr> </table>	yes	Enables RIP.	no	Disables RIP.	Set IP System RIP Enabled =
yes	Enables RIP.					
no	Disables RIP.					
RIP Spoof Enabled	<p>RIP spoofing periodically broadcasts network information even if routing or service tables are unchanged.</p> <p>Enables or disables RIP spoofing.</p> <table border="1"> <tr> <td>yes</td> <td>Enables RIP spoofing.</td> </tr> <tr> <td>no</td> <td>Disables RIP spoofing.</td> </tr> </table>	yes	Enables RIP spoofing.	no	Disables RIP spoofing.	Set IP System Rip Spoof Enabled =
yes	Enables RIP spoofing.					
no	Disables RIP spoofing.					
RIP TTL	When RIP Enabled is set to Yes , enter the upper bound on the TTL (Time to Live) of all RIP messages generated by the device. The TTL is reduced at the points along the route	Set IP System Rip TTL =				

	<p>where it is processed. If the TTL reaches zero before the datagram reaches its destination, the datagram is discarded.</p> <table border="1"> <tr> <td>Minimum Value</td> <td>1</td> </tr> <tr> <td>Default Value</td> <td>64</td> </tr> <tr> <td>Maximum Value</td> <td>64</td> </tr> <tr> <td>Units</td> <td>Hops</td> </tr> </table>	Minimum Value	1	Default Value	64	Maximum Value	64	Units	Hops	
Minimum Value	1									
Default Value	64									
Maximum Value	64									
Units	Hops									
RIP Response Interval	<p>RIP response interval is the length of time in seconds between successive periodic RIP response message broadcasts. This option is used when sending RIP messages and is only supported when RIP Enabled is set to Yes.</p> <table border="1"> <tr> <td>Minimum Value</td> <td>15</td> </tr> <tr> <td>Default Value</td> <td>30</td> </tr> <tr> <td>Maximum Value</td> <td>65535</td> </tr> <tr> <td>Units</td> <td>Seconds</td> </tr> </table>	Minimum Value	15	Default Value	30	Maximum Value	65535	Units	Seconds	Set IP System RIP Response Interval =
Minimum Value	15									
Default Value	30									
Maximum Value	65535									
Units	Seconds									
RIP Route Aging Timeout	<p>The length of time, in minutes, the system allows for learning a route via RIP. When this value is exceeded the destination is marked as unreachable. The metric set to 16. This option is used when sending RIP messages.</p> <table border="1"> <tr> <td>Minimum Value</td> <td>1</td> </tr> <tr> <td>Default Value</td> <td>3</td> </tr> <tr> <td>Maximum Value</td> <td>1080</td> </tr> <tr> <td>Units</td> <td>Minutes</td> </tr> </table>	Minimum Value	1	Default Value	3	Maximum Value	1080	Units	Minutes	Set IP System RIP Route Aging Timeout =
Minimum Value	1									
Default Value	3									
Maximum Value	1080									
Units	Minutes									
RIP Next Hop Zero Enabled	<p>Defines whether to set the next hop field in all RIP routes be 0.0.0.0 or to the outbound interface address which the RIP broadcast is transmitted on. Some third party equipment require this field to be 0.0.0.0.</p> <table border="1"> <tr> <td>Yes</td> <td>Set the next hop field to 0.0.0.0 in all RIP routes</td> </tr> <tr> <td>No</td> <td>Set the next hop field in all RIP routes to the outbound port address (default)</td> </tr> </table>	Yes	Set the next hop field to 0.0.0.0 in all RIP routes	No	Set the next hop field in all RIP routes to the outbound port address (default)	Set IP System RIP Next Hop Zero Enabled =				
Yes	Set the next hop field to 0.0.0.0 in all RIP routes									
No	Set the next hop field in all RIP routes to the outbound port address (default)									
TCP Adjust MMS	Not available to RIP.									
TCP SYN Retry Count	Not available to RIP.									
TCP Retransmission Timeout	Not available to RIP.									
TCP Keepalive Timeout	Not available to RIP.									
TCP Keepalive Interval	Not available to RIP.									
Management Address Enabled	Not available to RIP. If Management Address is enabled it will be	Set IP System Management Address								

	sent in the RIP routes that are advertised even though it does not appear in the SMG routing table.	Enabled =
Management IP Address	Not available to RIP.	Set IP System Management Address =

Table 1: IP system fields and their descriptions

3.1.2 Configure RIP on an interface

To ensure specific interface configurations can take affect, you must have enabled RIP at the IP -> System level. For more information, read section 3.1.1.

Each IP interface can be configured to use RIP. To access the different interfaces on the SMG, select **Expert Menu -> interfaces**. The interfaces folder contains the various interfaces available for configuration.

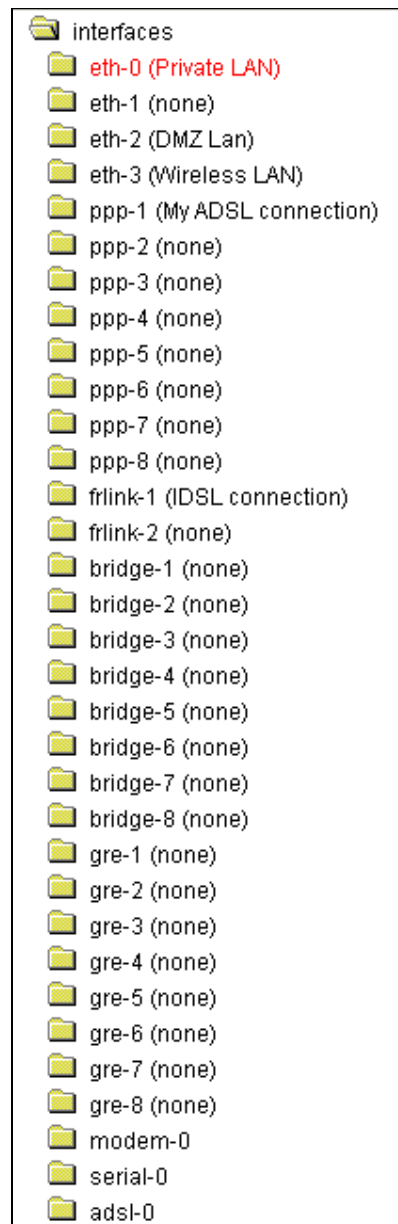


Figure 4: A list of interfaces in the interfaces folder

To access the RIP configuration page, select **<interface> -> ip -> rip**. The IP interface page appears. To view the advanced options, click **Advanced**.

The screenshot shows the configuration page for RIP on interface eth-0. The left sidebar shows a tree view of the configuration hierarchy, with 'eth-0 (Private LAN)' expanded to show 'ip' and 'rip' selected. The main panel is titled 'IP Interface RIP on eth-0' and contains the following settings:

- Send Requests: yes
- Periodic Updates Enabled: yes
- Triggered Updates Enabled: no
- Learn Host Routes: yes
- Learn Default Route: yes
- Learn Default Route Metric Override: 1
- Send Responses: yes
- Announce Host Routes: yes
- Announce Default Routes: yes
- Announce Static Routes: no
- Announce Route Metric Delta: 0
- Split Horizon: yes
- Poison Reverse: yes
- Route Hold-Down: no
- Summarize Routes: yes
- Advertise Interface List: (empty text box)

Buttons at the bottom: Update, Delete, Standard.

Figure 5: The IP interface RIP on eth-0 page, where <interface> is eth-0

Field	Description	Command Line				
Send Requests	Enable or disable sending RIP requests for routing tables on the selected interface. A request is used to ask for a response containing all or part of a router's routing table. Requests are sent as broadcasts (RIP1) or multicasts (RIPv2) by routers which have just become active. <table border="1"> <tr> <td>Yes</td> <td>Send RIP requests</td> </tr> <tr> <td>No</td> <td>Do not send RIP requests</td> </tr> </table>	Yes	Send RIP requests	No	Do not send RIP requests	Set IP Interface RIP Send Request Enabled =
Yes	Send RIP requests					
No	Do not send RIP requests					
Periodic Updates Enabled	Enable or disable RIP from performing a periodic routing table update for the selected interface. <table border="1"> <tr> <td>Yes</td> <td>Enable periodic updates</td> </tr> <tr> <td>No</td> <td>Disable periodic updates</td> </tr> </table>	Yes	Enable periodic updates	No	Disable periodic updates	Set IP Interface RIP Periodic Updates Enabled =
Yes	Enable periodic updates					
No	Disable periodic updates					
Triggered Updates Enabled	Enable or disable RIP updating the routing table when events occur. Events such as new routes advertised or metric changes would typically trigger RIP to update routes. <table border="1"> <tr> <td>Yes</td> <td>Enable triggered updates</td> </tr> <tr> <td>No</td> <td>Disable triggered updates</td> </tr> </table>	Yes	Enable triggered updates	No	Disable triggered updates	Set IP Interface RIP Triggered Updates Enabled =
Yes	Enable triggered updates					
No	Disable triggered updates					
Learn Host Routes	Enable or disable learning IP host routes on the selected interface. Routes that have been learned are stored in the routing table.	Set IP Interface RIP Learn Host Route Enabled =				

	<table border="1"> <tr> <td>Yes</td> <td>Learn host routes</td> </tr> <tr> <td>No</td> <td>Disable learning host routes</td> </tr> </table>	Yes	Learn host routes	No	Disable learning host routes					
Yes	Learn host routes									
No	Disable learning host routes									
Learn Default Route	<p>Allow the SMG to learn a default route from RIP responses.</p> <table border="1"> <tr> <td>Yes</td> <td>Learn default route</td> </tr> <tr> <td>No</td> <td>Disable learning default route</td> </tr> </table>	Yes	Learn default route	No	Disable learning default route	Set IP Interface RIP Learn Default Route Enable =				
Yes	Learn default route									
No	Disable learning default route									
Learn Default Route Metric Override	<p>Enter the number of hops (metric) from 1 to 15. When a RIP message is routed out the default route, the number of hops entered in this field overrides the number of hops in the original RIP message.</p> <table border="1"> <tr> <td>Minimum Value</td> <td>1</td> </tr> <tr> <td>Default Value</td> <td>1</td> </tr> <tr> <td>Maximum Value</td> <td>15</td> </tr> <tr> <td>Units</td> <td>Hops</td> </tr> </table>	Minimum Value	1	Default Value	1	Maximum Value	15	Units	Hops	Set IP Interface RIP Default Route Metric Override =
Minimum Value	1									
Default Value	1									
Maximum Value	15									
Units	Hops									
Send Responses	<p>Enable or disable sending RIP responses to RIP requests for routing tables on the selected interface. The router uses responses to send regular updates (unsolicited response) and also triggered updates caused by a route change.</p> <table border="1"> <tr> <td>Yes</td> <td>Allow interface to send responses.</td> </tr> <tr> <td>No</td> <td>Set the next hop field in all RIP routes to the outbound port address (default)</td> </tr> </table>	Yes	Allow interface to send responses.	No	Set the next hop field in all RIP routes to the outbound port address (default)	Set IP Interface RIP Send Response Enabled =				
Yes	Allow interface to send responses.									
No	Set the next hop field in all RIP routes to the outbound port address (default)									
Announce Host Routes	<p>Allows any host routes stored in the routing table to be propagated within RIP responses. Host routes are routes to a specific internetwork address i.e. network address and host address.</p> <table border="1"> <tr> <td>Yes</td> <td>Allow host routes in RIP responses</td> </tr> <tr> <td>No</td> <td>Do not include host routes in RIP responses</td> </tr> </table>	Yes	Allow host routes in RIP responses	No	Do not include host routes in RIP responses	Set IP Interface RIP Announce Host Route Enabled =				
Yes	Allow host routes in RIP responses									
No	Do not include host routes in RIP responses									
Announce Default Routes	<p>Enables or disables including the RIP Default Route in RIP announcements.</p> <table border="1"> <tr> <td>Yes</td> <td>Include default route in announcements</td> </tr> <tr> <td>No</td> <td>Do not include default route in announcements</td> </tr> </table>	Yes	Include default route in announcements	No	Do not include default route in announcements	Set IP Interface RIP Announce Default Route Enabled =				
Yes	Include default route in announcements									
No	Do not include default route in announcements									
Announce Static Routes	<p>Enables or disables announcing static routes, including the static IP routes in RIP announcements.</p> <table border="1"> <tr> <td>Yes</td> <td>Enable static route announcing for this interface</td> </tr> <tr> <td>No</td> <td>Disable static route announcing for this interface (default)</td> </tr> </table>	Yes	Enable static route announcing for this interface	No	Disable static route announcing for this interface (default)	Set IP Interface RIP Announce Static Route Enabled =				
Yes	Enable static route announcing for this interface									
No	Disable static route announcing for this interface (default)									
Announce Route Metric Delta	<p>Defines a value which will be added to the metric of each routing entry sent in a RIP response on an interface. This feature can be used to increase the metric of each route and therefore make the route less attractive to neighbouring routers.</p> <table border="1"> <tr> <td>Minimum Value</td> <td>0</td> </tr> <tr> <td>Default Value</td> <td>0</td> </tr> <tr> <td>Maximum Value</td> <td>14</td> </tr> </table>	Minimum Value	0	Default Value	0	Maximum Value	14	Set IP Interface RIP Transmit Metric Override =		
Minimum Value	0									
Default Value	0									
Maximum Value	14									

	Units	Hops	
Split Horizon	Split Horizon is a scheme for avoiding problems caused by including routes in updates sent to the gateway from which they were learned. The 'simple split horizon' scheme omits routes learned from one neighbour in updates sent to that neighbour.		Set IP Interface RIP Split Horizon Enabled =
	Yes	Enables the split horizon algorithm on the selected interface.	
	No	Disables the split horizon algorithm on the selected interface.	
Poison Reverse	'Split horizon with poisoned reverse' includes the routes in updates, but sets their metrics to infinity (16). The router sends updates with unreachable hop counts back to the sender for every route received to help prevent routing loops.		Set IP Interface RIP Poison Reverse Enabled =
	Yes	Enables the split horizon with poisoned reverse algorithm on the selected interface.	
	No	Disables the split horizon with poisoned reverse algorithm on the selected interface.	
Route Hold-down	When enabled is set to 'yes', an aged route cannot be 'refreshed' to a non-aged status but instead must be deleted and relearned, thus enhancing the stability of the RIP topology in the presence of transients.		Set IP Interface RIP Route Holddown Enabled =
	Yes	Enables locking aged routes learned from RIP messages on the selected interface.	
	No	Disables locking aged routes learned from RIP messages on the selected interface.	
Summarize Routes	Route Summarization consists of announcing only the parent network address of IP subnetworks to other IP networks.		Set IP Interface RIP Summarize Route Enabled =
	Yes	Enables control for generating route summaries in RIP responses sent out the selected interface	
	No	Disables control for generating route summaries in RIP responses sent out the selected interface	
Advertise Interface List	Defines a list of interfaces that will be advertised in the RIP responses. No list entry means all enabled interfaces will be included. Specifying entries in the list limits the routes in the SMG RIP announcements to the interfaces in the list. Separate interface list entries with a comma. For example, to advertise 'eth-0 and ppp-1' set IP interface RIP advertise list entries eth-0, ppp-1.		Set IP Interface RIP Advertise List Entries =
	Minimum Value	0	
	Default Value	Unspecified	
	Maximum Value	199	
	Units	String	

Table 2: IP Interface RIP system fields and their descriptions

3.1.3 Configure RIP version 2 on an interface

To ensure specific interface configurations can take affect, you must have enabled RIP at the IP -> System level. For more information, read section 3.1.1.

RIP version 2 shares the same basic algorithms as RIP version 1 but it supports a further three features:

- Subnet masks
- Authentication
- Next hop field

RIP version 2 also supports the sending of periodic and triggered updates.

To access the RIP version 2 configuration page, from the Expert View menu select **interfaces -> <interface> -> ip -> ripv2**.

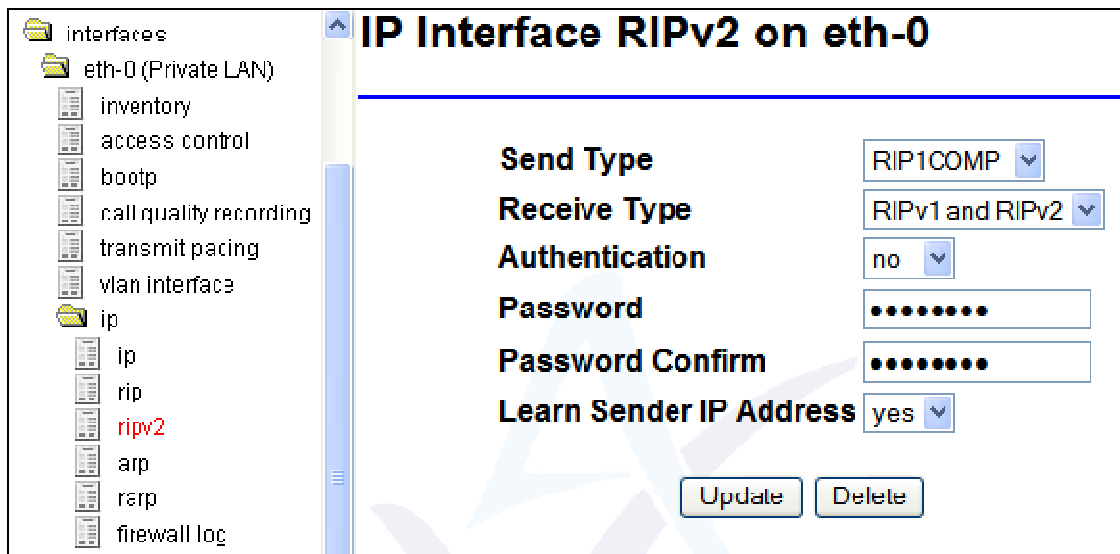


Figure 6: IP Interface RIPv2 on eth-0 page, where <interface> is eth-0

Field	Description	Command Line
Send Type	Allows you to choose the send mode for the elected interface. This configures which version of RIP will be set in the SMG RIP responses. RIPv1 is sent as a broadcast address 255.255.255.255 . RIPv2 is sent as a multicast address 224.0.0.9 .	Set IP Interface RIPv2 Send Type =
	do not send Disables sending all RIP messages.	
	RIPv1 Sends only RIP version 1 messages.	
	RIPv1COMP Sends RIP version 1 and RIP version 2 messages.	
	RIPv2 Sends only RIP version 2 messages.	
Receive Type	Allows you to choose the receive mode for	Set IP Interface RIPv2 Receive Type =

	<p>the elected interface. This will set which version of RIP the SMG will accept.</p> <table border="1"> <tr> <td>RIPv1</td> <td>Receives RIP version 1 only.</td> </tr> <tr> <td>RIPv2</td> <td>Receives RIP version 2 only.</td> </tr> <tr> <td>RIPv1 and RIPv2</td> <td>Receives RIP version 1 and RIP version 2.</td> </tr> <tr> <td>No RIP</td> <td>Disables receiving RIP messages for an interface.</td> </tr> </table>	RIPv1	Receives RIP version 1 only.	RIPv2	Receives RIP version 2 only.	RIPv1 and RIPv2	Receives RIP version 1 and RIP version 2.	No RIP	Disables receiving RIP messages for an interface.	
RIPv1	Receives RIP version 1 only.									
RIPv2	Receives RIP version 2 only.									
RIPv1 and RIPv2	Receives RIP version 1 and RIP version 2.									
No RIP	Disables receiving RIP messages for an interface.									
Authentication	<p>Allows you to select the type of authentication required for the selected interface.</p> <table border="1"> <tr> <td>Yes</td> <td>Indicates that a password is needed to access the RIP configuration on this interface. If you select this option, you must enter the password in the password field.</td> </tr> <tr> <td>No</td> <td>Indicates that no password is needed.</td> </tr> </table>	Yes	Indicates that a password is needed to access the RIP configuration on this interface. If you select this option, you must enter the password in the password field.	No	Indicates that no password is needed.	Set IP Interface RIPv2 Authentication Type =				
Yes	Indicates that a password is needed to access the RIP configuration on this interface. If you select this option, you must enter the password in the password field.									
No	Indicates that no password is needed.									
Password	<p>Specifies the password when authentication has been enabled.</p> <table border="1"> <tr> <td>Minimum Value</td> <td>0</td> </tr> <tr> <td>Default Value</td> <td>Unspecified</td> </tr> <tr> <td>Maximum Value</td> <td>199</td> </tr> <tr> <td>Units</td> <td>String</td> </tr> </table>	Minimum Value	0	Default Value	Unspecified	Maximum Value	199	Units	String	Set IP Interface RIPv2 Plain Text Password =
Minimum Value	0									
Default Value	Unspecified									
Maximum Value	199									
Units	String									
Password Confirm	<p>Confirms the string in the password field when authentication has been enabled.</p> <table border="1"> <tr> <td>Minimum Value</td> <td>0</td> </tr> <tr> <td>Default Value</td> <td>Unspecified</td> </tr> <tr> <td>Maximum Value</td> <td>199</td> </tr> <tr> <td>Units</td> <td>String</td> </tr> </table>	Minimum Value	0	Default Value	Unspecified	Maximum Value	199	Units	String	N/A (only relevant on web form)
Minimum Value	0									
Default Value	Unspecified									
Maximum Value	199									
Units	String									
Learn Sender IP Address	<p>Allows the router to learn the IP address of the sender of the RIP packets received.</p> <table border="1"> <tr> <td>Yes</td> <td>Learns the router IP address</td> </tr> <tr> <td>No</td> <td>Does not learn the router IP address</td> </tr> </table>	Yes	Learns the router IP address	No	Does not learn the router IP address	Set IP Interface RIPv2 Learn Sender IP Address When Next Hop Is Invalid =				
Yes	Learns the router IP address									
No	Does not learn the router IP address									

Table 3: The interface RIPv2 fields and their descriptions

4 Diagnostics

The Service Managed Gateway supports extensive remote diagnostics, status and SLA monitoring capabilities.

The status and diagnostics tools are provided as a series of Java applets.

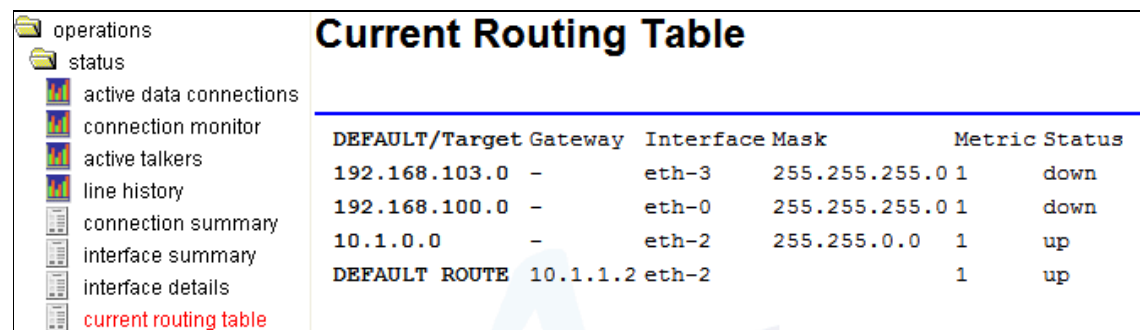
4.1 Routing table

To view the routing table, from the SMG Start page, click **Advanced**.

In the Advanced menu, click **Expert View**.

In the top menu click **Operations**.

In the Operation menu, click **Status -> current routing table**.



DEFAULT/Target Gateway	Interface	Mask	Metric	Status
192.168.103.0	eth-3	255.255.255.0	1	down
192.168.100.0	eth-0	255.255.255.0	1	down
10.1.0.0	eth-2	255.255.0.0	1	up
DEFAULT ROUTE 10.1.1.2	eth-2		1	up

Figure 7: The current routing table page

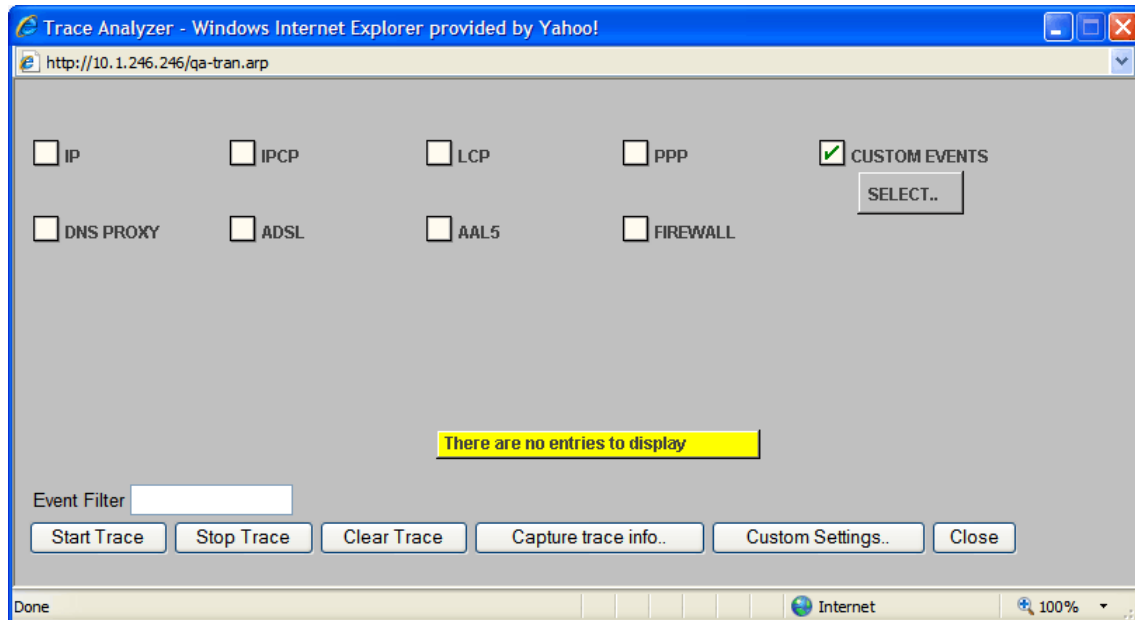
4.2 Trace analyzer

The Trace Analyzer provides a web interface to event tracing allowing you to quickly locate and analyze problems.

To view the Trace Analyzer, from the SMG Start page, click **Advanced**.

In the **Advanced** menu, click **Diagnostics**.

On the Diagnostics page, click **Trace Analyzer**. The Trace Analyzer pop-up window appears.



To view the RIP traces check **Custom Events** and then click **Select**. The Select Events to Trace pop-up window appears.

In the Events Available window, scroll to the bottom of the list and select **RIP** and click **ADD**. RIP appears in the Selected Events window.

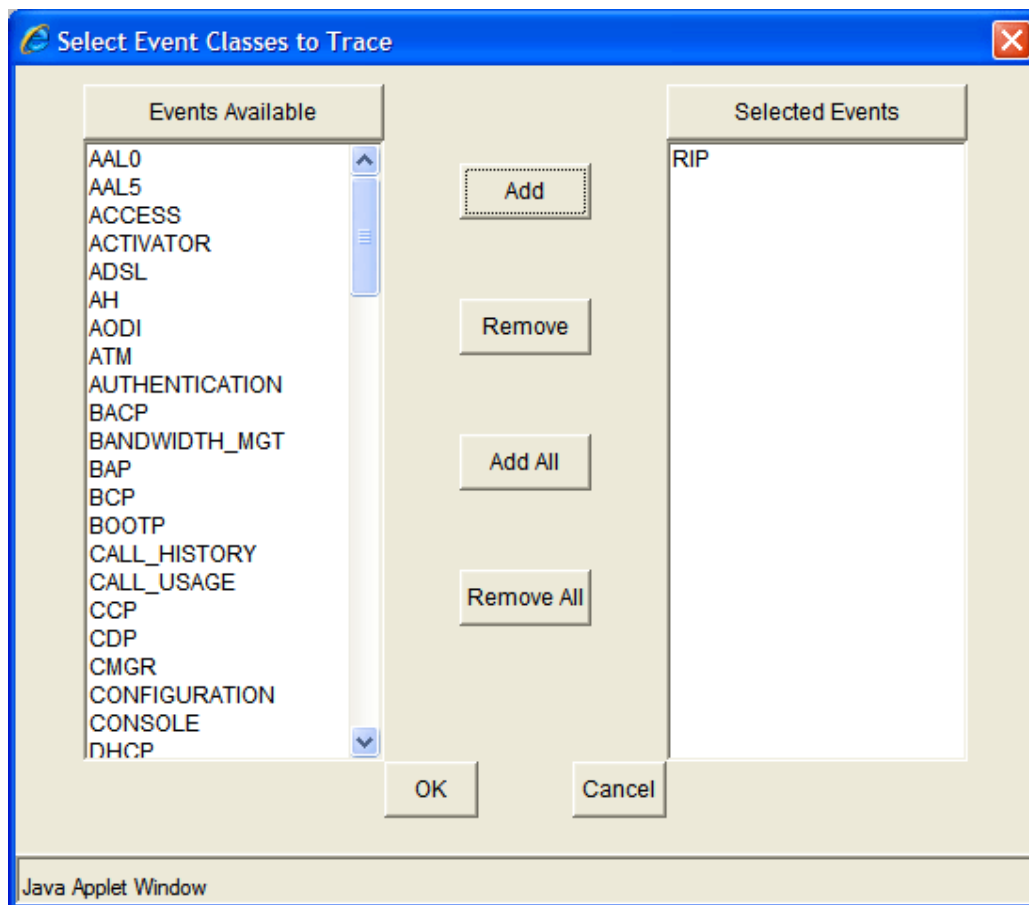


Figure 8: The select event classes to trace pop-up window

Click **OK**. The pop-up window automatically closes.

When you have added the event, the Trace Analyzer will capture RIP events. In the Trace Analyzer window, click **Start Trace**.

4.3 Tracing using the command line

For information on logging on to the command line interface, read the quick guide 'Using the CLI to Manage an SMG'

Tracing via the command line is more flexible than using the trace analyser as you can specify the event severity and use the all class event to trace all event classes.

Command line tracing also allows you to trace to a log file for examining events over a protracted period of time.

If you enter no event severity, all event severities are displayed.

If you chose an event severity, all events of the chosen severity and greater are displayed.

4.3.1 Command line syntax

To stop tracing, entering – (minus) followed by the event class will stop tracing for this event class. Entering – (minus) on its own will stop all tracing.

Syntax	Description
++rip	Starts tracing RIP events
-rip	Stops RIP tracing
++ip:520	Starts tracing RIP IP packets
-ip:520	Stops tracing RIP IP packets

Table 4: The command line tracing syntax and their descriptions