

Service Managed Gateway™

Event Tracing



Issue	1.1
Date	22 July 2010

1	About this document	3
1.1	Scope	3
1.2	Readership	3
2	Event tracing	4
2.1	Event classes.....	4
2.2	Tracing events in real time.....	6
2.2.1	Tracing using the command line interface.....	8
2.2.2	Tracing IP packet data	9

Copyright 2010 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

1.1 Scope

This document describes:

- event classes, their codes and severity ratings;
- how to trace events using the trace analyzer; and
- how to trace events using the command line.

1.2 Readership

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

2 Event tracing

The SMG comprises a number of software modules, each of which has a complex event system. For diagnosing complex problems, you can trace internal events in real time.

Note: you can also send events, as they occur, to a syslog server or SNMP manager. For more information, read user guides '[Configuring Event Filters](#)', and [Configuring a Syslog Client](#)'.

2.1 Event classes

All events are grouped into unique event classes with every event having an event severity ranging from the most severe **Emergency** value '0' to the least severe **Debug** value '7'.

Severity	Value	Description
Emergency	0	A severe service-affecting condition has occurred. Requires immediate corrective action.
Alert	1	Service or status change has occurred.
Critical	2	A fault occurred, resulting in severe degradation in capability of system or service. Urgent.
Error	3	Malfunction or failure not critical to system operation. Take corrective action as soon as possible.
Warning	4	Potential or pending fault. Correct problem as soon as possible before it becomes a severe, service-affecting fault.
Notice	5	Service or system notice.
Informational	6	Service or system status information.
Debug-Level Messages	7	Troubleshooting and debug messages.

Table 1: Event classes, their severity levels and descriptions

To view the available event classes, from the SMG Start page, click **Advanced**.

In the top menu, click **Operations**.

In **Operations** menu, click **troubleshooting->events->event class codes**.

Serial Number: 1234567890

Event Class Codes

0. EMERGENCY	34. ISDN	69. GENERAL
1. ALERT	35. DHCP	70. SCHEDULER
2. CRITICAL	36. SPID	71. SPD
3. EVENT_ERROR	37. POTS	72. IPSEC
4. EVENT_WARNING	38. MLPPP	73. IKE
5. EVENT_NOTICE	39. IPCP_STATE	74. SAD
6. EVENT_INFO	40. PPP_STATE	75. MKMD
7. EVENT_DEBUGMSG	41. CALL_USAGE	76. ESP
8. CONFIGURATION	42. DNSP	77. AH
9. SECURITY	43. USER_PROFILE	78. IP_ROUTE
10. MEMORY	44. UPLOAD	79. CMGR
11. PERFORMANCE	45. CALL_HISTORY	80. PDD
12. IP	46. AUTHENTICATION	81. DIFFSERV
14. SPT	48. ISDN_L1	85. AALO
15. LAPD	49. SCRIPT	86. MODEM
16. LCP	50. BANDWIDTH_MGT	96. ACTIVATOR

Figure 1: The event class codes page

Command line: show event classes

```

super> sh event classes
0      EMERGENCY
1      ALERT
2      CRITICAL
3      EVENT_ERROR
4      EVENT_WARNING
5      EVENT_NOTICE
6      EVENT_INFO
7      EVENT_DEBUGMSG
8      CONFIGURATION
9      SECURITY
10     MEMORY
11     PERFORMANCE
12     IP
13     IPX
14     SPT
15     LAPD
16     LCP
17     IPCP
18     IPXCP
19     BCP
20     CCP
21     ETHERNET
22     X25
23     FRAME_RELAY
23     FRAME_PVC
24     SERIAL
25     CONSOLE

```

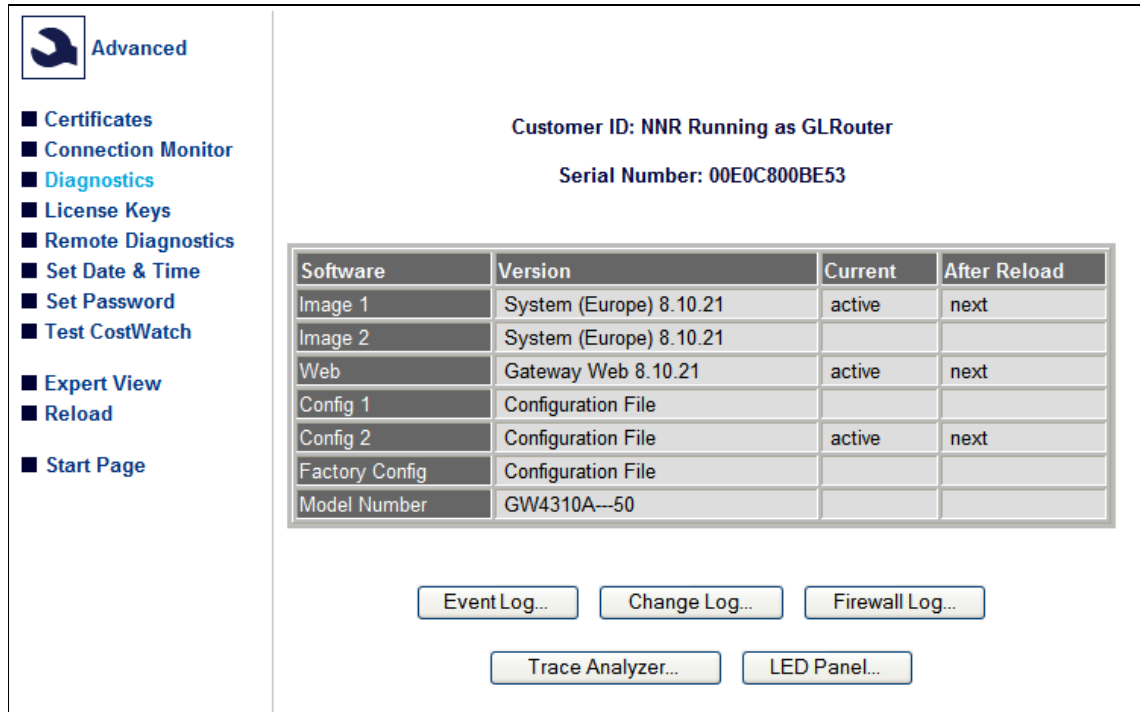
Figure 2: Output from the command line show event classes

2.2 Tracing events in real time

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

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

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



Software	Version	Current	After Reload
Image 1	System (Europe) 8.10.21	active	next
Image 2	System (Europe) 8.10.21		
Web	Gateway Web 8.10.21	active	next
Config 1	Configuration File		
Config 2	Configuration File	active	next
Factory Config	Configuration File		
Model Number	GW4310A---50		

Figure 3: The diagnostics page

On the Diagnostics page, click **Trace Analyzer**.

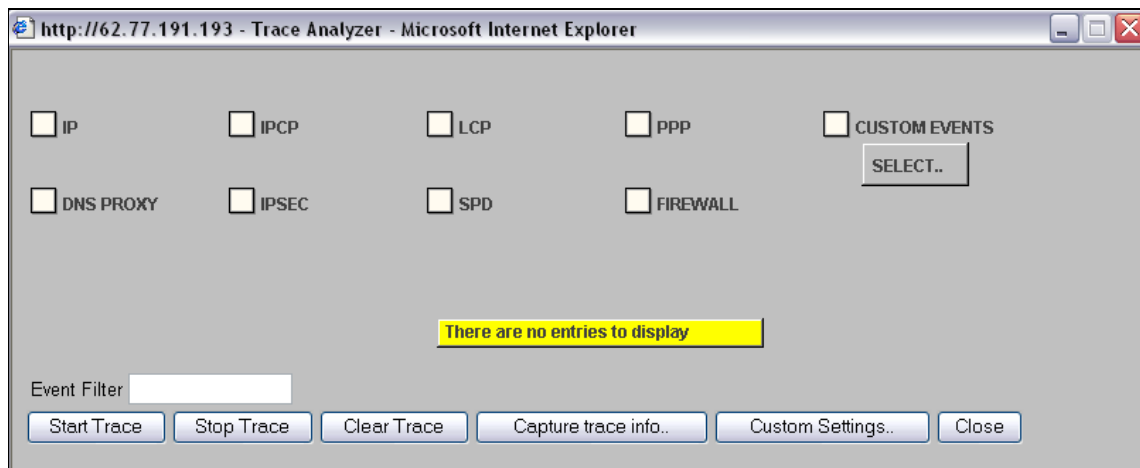


Figure 4: The trace analyzer pop up window

To display all severities within an event class, check the box beside an event class and click **Start Trace**.

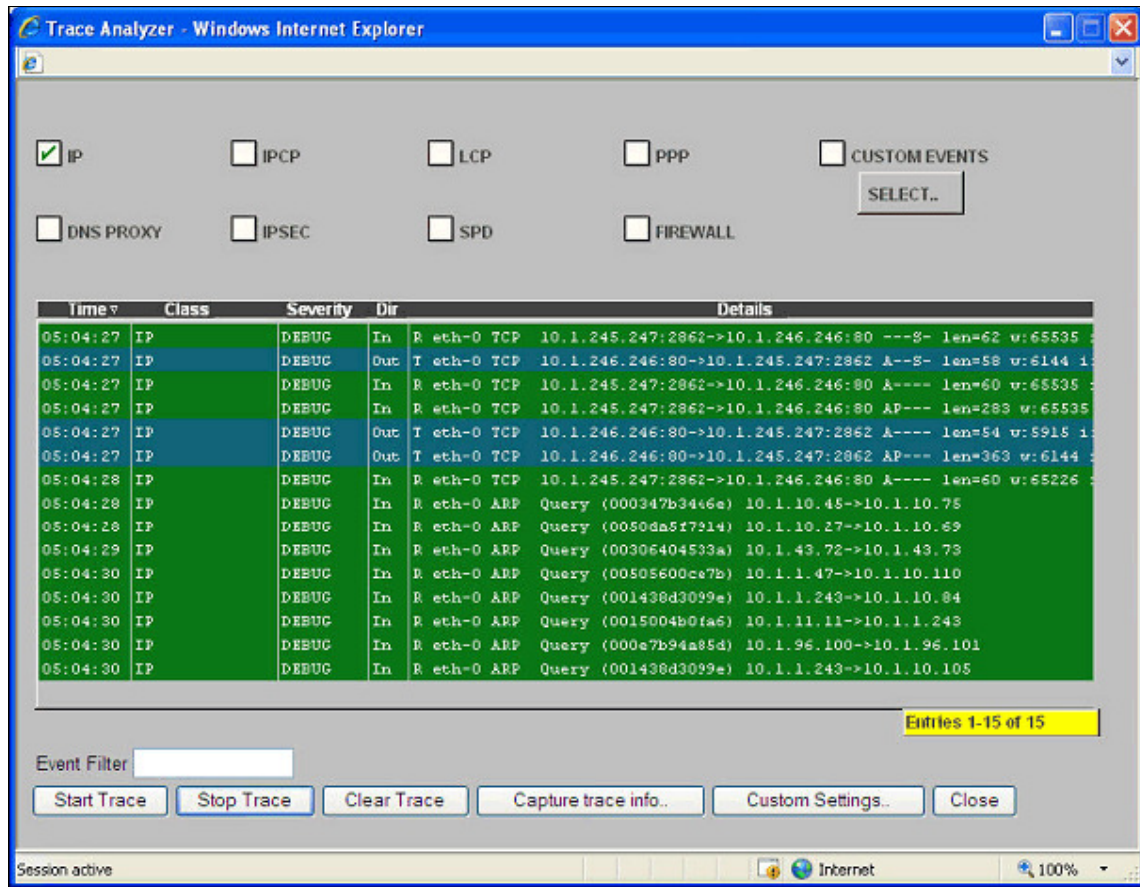


Figure 5: The trace analyzer pop-up window

To save traces to your local machine for analysis, click **Capture Trace info.**

Note: the trace analyzer log is of finite size and so if you trace large amounts of events, the trace analyser will 'wrap around' overwriting older events. To avoid this happening, trace using the command line interface. See section 2.2.2 'Tracing using the command line interface'.

Events can be filtered by string matching so that unwanted events are not displayed. In this instance enter an event filter. Event filters are not case sensitive. Tables 2 and 3 show examples of event filters.

Event filter	Description
Tracing IP events with Event Filter ICMP	Displays IP events with ICMP in the event string.

Table 2: Event filter example1

Use the comparators **& (AND)**, **| (OR)**, **!(NOT)**. to build up complex filters.

Use an underscore **_** to represent a space.

Event filter	Description
Tracing IP events with Event Filter: 1.2.3.4&:1998	Displays IP events with :1998 and IP address 1.2.3.4 in the event

Table 3: Event filter example 2

Use the example in table 3 to see IP events using port number 1998 and IP address 1.2.3.4

2.2.1 Tracing using the command line interface

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.

Some modules support raw packet dumping. Examples of these are the serial relay module and the IP module. You can only dump raw packets through the command line.

2.2.1.1 Command line tracing syntax

Enter **++** followed by the event class to trace, optionally followed by the desired event severity.

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.

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.

Table 4 shows the command line tracing syntax and their descriptions.

Syntax	Description
++all 6	Traces all informational events and greater.
++ip	Traces all IP events.
++ip 5	Traces all IP events of notice severity and greater.

Table 4: Command line tracing syntax and their descriptions

2.2.1.2 Command line event filters

To avoid displaying unwanted events, command line events can be filtered by string matching, in the same way as filtering by the web interface. Event filters are not case sensitive. The syntax is:

```
++<event class>:<string to match>
```

Syntax	Description
++ip:1.2.3.4	Traces all IP events with 1.2.3.4 in the event string

Table 5: Example 1 of command line event filtering

Use the comparators **& (AND)**, **| (OR)**, **!(NOT)**. to build up complex filters.

Use an underscore **_** to represent a space.

Syntax	Description
++ip:1.2.3.4&:1998	Traces all IP events with 1.2.3.4 AND :1998 in the event string

Table 6: Example 2 of command line event filtering

Use the example in table 7 for filtering when you are looking for a particular port and IP address combination.

Syntax	Description
++ip:1998&ppp-1 tcp 6	Traces all IP information events and greater with 1998 AND ppp-1 OR tcp in the event string.

Table 7: Example 3 of command line event filtering

2.2.2 Tracing IP packet data

The IP module supports dumping hex raw packet information in real time.

Syntax	Description
<code>++ipdump:<string to match> [mode] [length]</code>	Starts tracing IP packets displaying normal IP event followed by hex packet data

Table 8: Example of syntax for dumping hex raw packet information in real time

Both mode and length are optional. Table 9 shows valid modes for an IP dump event.

Mode	Description
RAW	Dumps whole packet, including MAC header. This mode also dumps non-IP packets. All other modes ignore non-IP packets.
IP (default)	Dumps from the IP header.
DATA	Dumps from the IP data portion onwards (skipping the 20 byte IP header)
TEXT	Dumps the TCP data portion (skipping IP and TCP headers) and also prints as text – up to 72 chars per line. Non-printable characters are shown as (dot). <code>\r</code> or <code>\r\n</code> causes a natural line break to improve readability.

Table 9: Valid modes for IP dump event

The length field defaults to 64 bytes. To see more data, specify a longer length.

The IPDUMP generates the normal IP event associated with the packet and then the hex data follows on the next line.

The filter string is also optional, but is recommended with IPDUMP. It uses the same syntax as normal event filters.

Note: the string match matches against the IP event generated as part of the IPDUMP information and not against the dumped hex packet data.

The following examples show dump syntax and their descriptions.

Syntax	Description
<code>++ipdump</code>	Dumps up to 64 bytes of data from all IP packets transmitted or received starting from the IP header.

Table 10: Example 1 of IP packet tracing syntax

```
super> ++ipdump
Warning: enabling IPDUMP with no filter will produce a LOT of output!
Added event class to monitor list

super> |21:10:43 R ppp-1 TCP 217.67.129.153:1483->217.40.99.49:23 A---- len=54
000000 45 00 00 28 61 37 40 00 6B 06 17 62 D9 43 81 99 E..(a7@.k..b.C..
000010 D9 28 63 31 05 CB 00 17 6F 20 75 9E 4F C9 F8 66 .(c1....o u.O..f
000020 50 10 FE 16 E7 B5 00 00 P.....
```

Figure 6: Output from IP packet tracing syntax example 1 in table 23

Syntax	Description
<code>++ipdump::80 raw 1500</code>	Dumps up to 1500 bytes of transmitted or received packets with :80 in the IP event text, from the MAC header. Also prints non IP packets.

Table 11: Example 2 of IP packet tracing syntax

```

super> ++ipdump::80 raw 1500
Added event class to monitor list
|00:01:14 R eth-0 TCP 10.1.245.247:1516->10.1.1.32:80 AP--- len=335 w:65535 i:
000000 12 34 56 78 90 12 00 80 C7 20 A4 9D 08 00 45 00 .4Vx..... .E.
000010 01 41 74 DF 40 00 80 06 79 BE 0A 01 F5 F7 0A 01 .At.θ...y.....
000020 01 20 05 EC 00 50 30 AE 04 1E D2 3F 40 43 50 18 . ...PO....?@CP.
000030 FF FF F1 E5 00 00 47 45 54 20 2F 6F 65 6D 2F 71 .....GET /oem/q
000040 61 2D 74 6F 70 6C 6F 67 6F 2E 67 69 66 20 48 54 a-toplogo.gif HT
000050 54 50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20 TP/1.1..Accept:
000060 2A 2F 2A 0D 0A 52 65 66 65 72 65 72 3A 20 68 74 */*..Referer: ht
000070 74 70 3A 2F 2F 31 30 2E 31 2E 31 2E 33 32 2F 71 tp://10.1.1.32/q
000080 61 2D 68 6F 6D 65 2E 61 72 70 0D 0A 41 63 63 65 a-home.arp..Acce
000090 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20 67 61 2D pt-Language: ga-
0000a0 69 65 0D 0A 55 41 2D 43 50 55 3A 20 78 38 36 0D ie..UA-CPU: x86.
0000b0 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 .Accept-Encoding
0000c0 3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D : gzip, deflate.
0000d0 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A .User-Agent: Moz
0000e0 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 61 74 illa/4.0 (compat
0000f0 69 62 6C 65 3B 20 4D 53 49 45 20 37 2E 30 3B 20 ible; MSIE 7.0;
000100 57 69 6E 64 6F 77 73 20 4E 54 20 35 2E 31 3B 20 Windows NT 5.1;
000110 2E 4E 45 54 20 43 4C 52 20 31 2E 31 2E 34 33 32 .NET CLR 1.1.432
000120 32 29 0D 0A 48 6F 73 74 3A 20 31 30 2E 31 2E 31 2) ..Host: 10.1.1
000130 2E 33 32 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A .32..Connection:
000140 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 0D 0A Keep-Alive....

```

Figure 7: Output from IP packet tracing syntax example 2 in table 11