

# Service Managed Gateway™

## How to Configure Event Filters on an SMG

Issue 1.1

Date 22 July 2010

<b>1</b>	<b>About this document .....</b>	<b>3</b>
<b>1.1</b>	<b>Scope .....</b>	<b>3</b>
<b>1.2</b>	<b>Readership .....</b>	<b>3</b>
<b>1.3</b>	<b>More information.....</b>	<b>3</b>
<b>1.4</b>	<b>Prerequisite configurations .....</b>	<b>3</b>
<b>2</b>	<b>Introduction .....</b>	<b>4</b>
<b>3</b>	<b>Configuring the SMG.....</b>	<b>5</b>
<b>3.1</b>	<b>Configuring event filtering on an SMG .....</b>	<b>5</b>
3.1.1	Configure the event filter system.....	6
3.1.2	Configure an event filter.....	8
3.1.3	Add a new event filter .....	9
3.1.4	Modify an existing event filter .....	11
3.1.5	Save the event filter .....	11
<b>4</b>	<b>Severity definitions .....</b>	<b>14</b>
<b>5</b>	<b>Event class definitions.....</b>	<b>15</b>

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

This document describes how to configure event filters on Service Managed Gateway settings.

## 1.1 Scope

This document explains:

- how to configure event filters on an SMG;
- how to utilise the diagnostic and trace analyzer tools in the SMG; and
- describes the event classes available, and their numbers.

## 1.2 Readership

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

## 1.3 More information

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

## 1.4 Prerequisite configurations

It is important that the intended event filter target has previously been configured and the system reloaded before you configure the event filter.

For **SNMP** configurations refer to the guide '[Configuring the SMG for SNMP](#)'.

For **email notification** configurations refer to the guide '[Configuring the SMG for Mail Notification](#)'.

For **syslog configurations** refer to the guide '[Configuring the SMG for Syslog](#)'.

For **Activator configurations** refer to the guide '[Configuring the SMG for Activator](#)'.

## 2 Introduction

Events on the SMG have:

- A specific event class
- A subclass
- An event description, and
- A severity

The following table shows the event severities, in order, from the highest severity to the lowest.

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

**Table 1: Event severities and their descriptions**

By default, all messages with an 'Informational' severity and higher are recorded in the SMG event log.

The event filtering feature is used to capture and report a specified event to a specified event target. Use the filtering criteria to select these events and, when the event matches the filtering criteria, selectively log the event to the event target.

Matching events can be sent to targets:

- via email to an email recipient;
- via an SNMP trap to an SNMP manager;
- via HTTP to Activator;
- to a syslog server; and
- to the SMG event log.

## 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 event filtering on an SMG

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

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

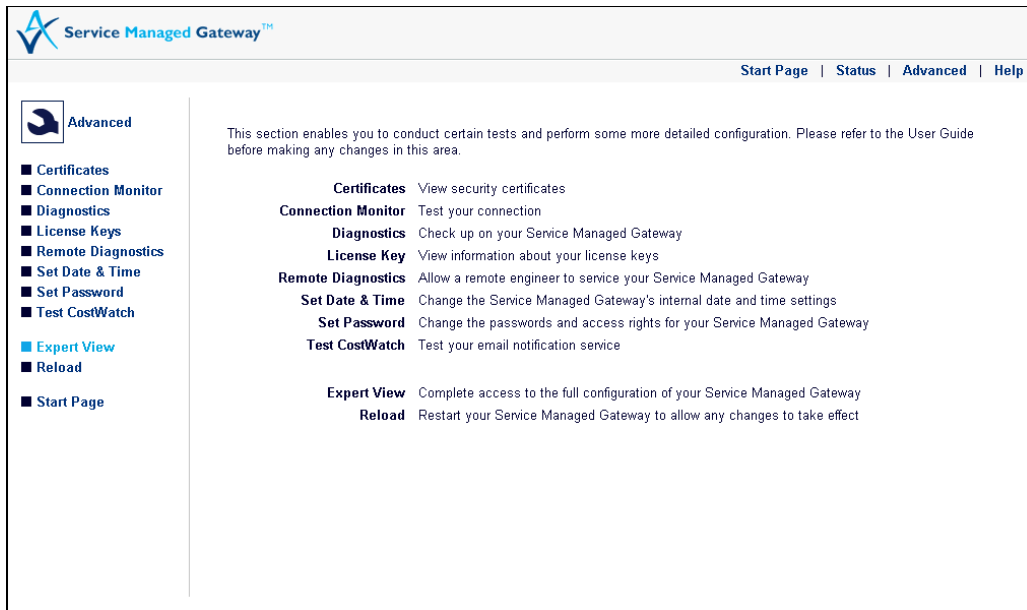


Figure 2: The advanced menu showing expert view

### 3.1.1 Configure the event filter system

You use the Event Filtering System page to enable or disable the event filtering system. You can also use it to configure event logging.

You must enable the event filtering system to log events to the SMG event log.

To send events to other destinations, you must configure specific event filters and set the Discriminator Enabled field to **yes**.

To configure the event filter system, in the Expert View menu, select **system -> events -> event system**. The Event Filtering System page appears.

**Event Filtering System**

Enabled

Discriminator Enabled

Discriminator Default Action

Discriminator Default Severity

Log Size

Log Activator Events

Log IP Diffserv Info

Figure 3: The event filtering system page

Field	Description	Command Line				
<b>Enabled</b>	<p>Enables or disables the event filtering system. This option must be enabled to allow specific filters to operate.</p> <p>If enabled, all events with a severity of Informational and higher are captured via the SMG event log. Select <b>Yes</b>.</p> <table border="1"> <tr> <td><b>Yes</b></td> <td>Enables filtering.</td> </tr> <tr> <td><b>No</b></td> <td>Disables filtering.</td> </tr> </table>	<b>Yes</b>	Enables filtering.	<b>No</b>	Disables filtering.	<pre>Set Event Forwarding Enabled =</pre>
<b>Yes</b>	Enables filtering.					
<b>No</b>	Disables filtering.					
<b>Discriminator Enabled</b>	<p>Enables or disables the filtering discriminator as configured in the Event Filtering form.</p> <p>If enabled, the event filters list is checked. If the event matches an event filter, the filter defines the action. If no event filter matches, then the discriminator default action and severity fields are used to determine the action.</p> <p>Select <b>Yes</b>.</p> <table border="1"> <tr> <td><b>Yes</b></td> <td>Enables filtering discriminator.</td> </tr> <tr> <td><b>No</b></td> <td>Disables filtering discriminator.</td> </tr> </table>	<b>Yes</b>	Enables filtering discriminator.	<b>No</b>	Disables filtering discriminator.	<pre>Set Event Forwarding Discriminator Enabled =</pre>
<b>Yes</b>	Enables filtering discriminator.					
<b>No</b>	Disables filtering discriminator.					
<b>Discriminator Default Action</b>	<p>Enables or disables storing system events to the internal event log of the router.</p> <table border="1"> <tr> <td><b>Log</b></td> <td>Logs the event to the event log if an action has not been specified (default).</td> </tr> <tr> <td><b>Do Not Log</b></td> <td>Does not log events to the event log.</td> </tr> </table>	<b>Log</b>	Logs the event to the event log if an action has not been specified (default).	<b>Do Not Log</b>	Does not log events to the event log.	<pre>Set Event Forwarding Default Action =</pre>
<b>Log</b>	Logs the event to the event log if an action has not been specified (default).					
<b>Do Not Log</b>	Does not log events to the event log.					
<b>Discriminator Default Severity</b>	<p>Selects the severity level to use as the default filtering criteria. Severity levels are listed in order. Emergency is the highest severity and Debug-Level Messages is the lowest operating severity. For a list of</p>	<pre>Set Event Forwarding Default Severity =</pre>				

	severities and their definitions, see section 4, 'Severity definitions'.		
<b>Log Size</b>	Specifies the size of the event log. Set this field to a number within the following range:	Set Event Log Size =	
	<b>Minimum value</b>		10
	<b>Default value</b>		50
	<b>Maximum value</b>		750
	<b>Units</b>	unspecified	
<b>Log Activator Events</b>	Allows Activator events to be logged. SMG Log Activator events by selecting <b>Yes</b> .	Set Event Activator Logging =	
	<b>Yes</b>		Log Activator events.
	<b>No</b>	Does not log Activator events.	
<b>Log IP Diffserv Info</b>	Allows for IP details to be logged when a diffserv queue has been defined.	Set Event IP Diffserv Logging =	
	<b>Yes</b>		Log IP diffserv information
	<b>No</b>	Do not log IP DiffServ information	

Table 2: Event filtering system fields and their descriptions

Set your configurations and click **Update**.

### 3.1.2 Configure an event filter

**Note:** The event filtering list will be checked for a match only if the event system event forwarding discriminator is enabled.

In the Expert View menu, select **system -> events -> event filters**. The Event Filtering List page appears.

Index	Event Class	Event Subclass	Target	Operation
1	Script	9999	Manager 1	<a href="#">modify/delete</a>
2	unconfigured	-	-	<a href="#">add</a>
3	unconfigured	-	-	<a href="#">add</a>
4	unconfigured	-	-	<a href="#">add</a>
5	unconfigured	-	-	<a href="#">add</a>
6	unconfigured	-	-	<a href="#">add</a>
7	unconfigured	-	-	<a href="#">add</a>
8	unconfigured	-	-	<a href="#">add</a>
9	unconfigured	-	-	<a href="#">add</a>
10	unconfigured	-	-	<a href="#">add</a>
11	unconfigured	-	-	<a href="#">add</a>

Figure 4: The event filtering list

### 3.1.3 Add a new event filter

To add a new event filter, in the Event Filtering List Operation column, select **add**. The Event Filtering Entry page appears.

Figure 5: The event filtering entry page

To view advanced options, click **Advanced**. The Event Subclass field is added to the filtering options.

Figure 6: The advanced event filtering options

Field	Description	Command Line
<b>Event Class</b>	Select the type of event or service to filter from the drop-down menu. For definitions of the event classes, read section 5, 'Event class definitions'.	Set Event Forwarding Discriminator Entry Class 1,26
<b>Event Subclass</b>	Forwards the event only if its subclass matches the event subclass configured here. If you want to filter all events in the event class are to be filtered, set to 0. The field may be set to a number with:	Set Event Forwarding Discriminator Entry Subclass 1,0

	<table border="1"> <tr> <td><b>Minimum value</b></td> <td>0 (default)</td> </tr> <tr> <td><b>Maximum value</b></td> <td>9999</td> </tr> <tr> <td><b>Units</b></td> <td>unspecified</td> </tr> </table>	<b>Minimum value</b>	0 (default)	<b>Maximum value</b>	9999	<b>Units</b>	unspecified																													
<b>Minimum value</b>	0 (default)																																			
<b>Maximum value</b>	9999																																			
<b>Units</b>	unspecified																																			
<b>Target</b>	<p>If the event meets the filtering criteria, select the destination of the event from the drop-down menu.</p> <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>Event Log</b></td> <td>Logs the event to the internal event log of the router.</td> </tr> <tr> <td><b>Manager 1</b></td> <td>Issues an SNMP trap to manager 1.</td> </tr> <tr> <td><b>Manager 2</b></td> <td>Issues an SNMP trap to manager2.</td> </tr> <tr> <td><b>Manager 3</b></td> <td>Issues an SNMP trap to manager 3.</td> </tr> <tr> <td><b>Manager 4</b></td> <td>Issues an SNMP trap to manager 4.</td> </tr> <tr> <td><b>Manager 5</b></td> <td>Issues an SNMP trap to manager 5.</td> </tr> <tr> <td><b>Manager 6</b></td> <td>Issues an SNMP trap to manager 6.</td> </tr> <tr> <td><b>Manager 7</b></td> <td>Issues an SNMP trap to manager 7.</td> </tr> <tr> <td><b>Manager 8</b></td> <td>Issues an SNMP trap to manager 8.</td> </tr> <tr> <td><b>Manager 9</b></td> <td>Issues an SNMP trap to manager 9.</td> </tr> <tr> <td><b>Manager 10</b></td> <td>Issues an SNMP trap to manager 10.</td> </tr> <tr> <td><b>All SNMP Managers</b></td> <td>Forwards the event to all configured SNMP managers.</td> </tr> <tr> <td><b>Email</b></td> <td>Forwards the event as an email to the specified email address.</td> </tr> <tr> <td><b>Activator</b></td> <td>Forwards the event to Activator.</td> </tr> <tr> <td><b>Syslog</b></td> <td>Forwards the event to the specified syslog server.</td> </tr> <tr> <td><b>All Targets</b></td> <td>Forwards the event to all configured targets</td> </tr> </tbody> </table>	Option	Description	<b>Event Log</b>	Logs the event to the internal event log of the router.	<b>Manager 1</b>	Issues an SNMP trap to manager 1.	<b>Manager 2</b>	Issues an SNMP trap to manager2.	<b>Manager 3</b>	Issues an SNMP trap to manager 3.	<b>Manager 4</b>	Issues an SNMP trap to manager 4.	<b>Manager 5</b>	Issues an SNMP trap to manager 5.	<b>Manager 6</b>	Issues an SNMP trap to manager 6.	<b>Manager 7</b>	Issues an SNMP trap to manager 7.	<b>Manager 8</b>	Issues an SNMP trap to manager 8.	<b>Manager 9</b>	Issues an SNMP trap to manager 9.	<b>Manager 10</b>	Issues an SNMP trap to manager 10.	<b>All SNMP Managers</b>	Forwards the event to all configured SNMP managers.	<b>Email</b>	Forwards the event as an email to the specified email address.	<b>Activator</b>	Forwards the event to Activator.	<b>Syslog</b>	Forwards the event to the specified syslog server.	<b>All Targets</b>	Forwards the event to all configured targets	Set Event Forwarding Discriminator Entry Target 1,1
Option	Description																																			
<b>Event Log</b>	Logs the event to the internal event log of the router.																																			
<b>Manager 1</b>	Issues an SNMP trap to manager 1.																																			
<b>Manager 2</b>	Issues an SNMP trap to manager2.																																			
<b>Manager 3</b>	Issues an SNMP trap to manager 3.																																			
<b>Manager 4</b>	Issues an SNMP trap to manager 4.																																			
<b>Manager 5</b>	Issues an SNMP trap to manager 5.																																			
<b>Manager 6</b>	Issues an SNMP trap to manager 6.																																			
<b>Manager 7</b>	Issues an SNMP trap to manager 7.																																			
<b>Manager 8</b>	Issues an SNMP trap to manager 8.																																			
<b>Manager 9</b>	Issues an SNMP trap to manager 9.																																			
<b>Manager 10</b>	Issues an SNMP trap to manager 10.																																			
<b>All SNMP Managers</b>	Forwards the event to all configured SNMP managers.																																			
<b>Email</b>	Forwards the event as an email to the specified email address.																																			
<b>Activator</b>	Forwards the event to Activator.																																			
<b>Syslog</b>	Forwards the event to the specified syslog server.																																			
<b>All Targets</b>	Forwards the event to all configured targets																																			
<b>Severity Criterion</b>	<p>Select the severity criterion from the drop-down menu.</p> <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>Greater Than</b></td> <td>Logs all events that have a severity level greater than the level indicated in the Severity field.</td> </tr> <tr> <td><b>Greater Than or Equal To</b></td> <td>Logs all events that have a severity level higher than, or the same as, the level indicated in the Severity field.</td> </tr> <tr> <td><b>Same As</b></td> <td>Logs all events that have a severity level higher than, or the same as, the level indicated in the Severity field.</td> </tr> </tbody> </table>	Option	Description	<b>Greater Than</b>	Logs all events that have a severity level greater than the level indicated in the Severity field.	<b>Greater Than or Equal To</b>	Logs all events that have a severity level higher than, or the same as, the level indicated in the Severity field.	<b>Same As</b>	Logs all events that have a severity level higher than, or the same as, the level indicated in the Severity field.	Set Event Forwarding Discriminator Entry Criteria 1,2																										
Option	Description																																			
<b>Greater Than</b>	Logs all events that have a severity level greater than the level indicated in the Severity field.																																			
<b>Greater Than or Equal To</b>	Logs all events that have a severity level higher than, or the same as, the level indicated in the Severity field.																																			
<b>Same As</b>	Logs all events that have a severity level higher than, or the same as, the level indicated in the Severity field.																																			

	<b>Less Than</b>	Logs all events that have a severity level lower than the level indicated in the Severity field.
	<b>Less Than or Equal To</b>	Logs all events that have a severity level lower than or the same as the level indicated in the Severity field.
	<b>Not The Same As</b>	Logs all events that have a severity level other than the level indicated in the Severity field.
	<b>Forward all Severities</b>	Ignores the event severity when filtering the event list.
<b>Severity</b>	Selects the severity to use as the filtering criteria. Severity levels are list in order. Emergency is the highest severity and Debug-Level Messages is the lowest severity.  For a list of severities and their definitions, see section 4, 'Severity definitions'.	

### 3.1.4 Modify an existing event filter

To modify or delete an existing event filter, on the Event Filtering Entry page, in the Operation column, select **Modify/Delete**. The Event Filtering List page appears. To add or modify an event click **Update**.

To delete an existing entry, click **Delete**.

For details on how to permanently save your changes to the configuration file, read section 3.1.5, Save the event filter.

### 3.1.5 Save the event filter

To ensure the event filter modifications and additions are permanent you must save them to a configuration file.

In the top-right corner of the Event Filter List page, click **Unsaved changes**.

Event Filtering List		<a href="#">(Unsaved changes)</a>		
Index	Event Class	Event Subclass	Target	Operation
1	Script	9999	Manager 1	<a href="#">modify/delete</a>
2	Security	0	Event Log	<a href="#">modify/delete</a>
3	unconfigured	-	-	<a href="#">add</a>
4	unconfigured	-	-	<a href="#">add</a>
5	unconfigured	-	-	<a href="#">add</a>

Figure 7: Click unsaved changes to save your configuration

When you click **Unsaved changes**, the Save Configuration to Flash page appears.

## Save Configuration to Flash

---

The last flash configuration loaded was **config1**.  
When the system is next rebooted, **config1** will be loaded.

Some of your [recent changes](#) have not yet been saved to flash.

Save Committed Changes To Config 1

Figure 8: The save configuration to flash page

Click **Save** to save your committed changes. The Configuration Saved page appears. Go to Figure 10.

If you have not previously committed all of your changes, click **recent changes** to view and commit the changes. The Recent configuration changes page appears with a list of recent changes.

## Recent configuration changes

---

[Save configuration](#) Display all unsaved changes   [Download changes](#)

```

--- 10.1.10.143 on 30-Mar-2004 ---
23:16:12      Set event forwarding discriminator entry target 2,2

```

Figure 9: The recent changes page

Click **Save configuration**. The Save Configuration to Flash re-appears. Now you have committed your changes, so click **Save**. The Configuration Saved page appears.

## Configuration Saved

---

Your configuration has been successfully saved.

The system's software image is **image1** and will restart using **image1**  
The system's flash configuration file is **config1** and will restart using **config1**

Some of your recent changes require a reload to take effect. To reload your Service Managed Gateway n below. You should only reload after you have completed all your configuration changes.

Figure 10: The configuration saved page

Click **Reload Router**.

The Reload Router button shows a progress timer and then the page returns to the Fast.Start page.

You can leave saving your configuration until you have made all the configuration changes you need to.

## 4 Severity definitions

The following table shows severity options and their descriptions.

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

## 5 Event class definitions

<b>Class Number</b>	<b>Option</b>	<b>Description</b>
85	<b>AAL0</b>	AAL0 events
65	<b>AAL5</b>	AAL5 events
125	<b>AC</b>	AC events
116	<b>Access</b>	8021x authentication events
87	<b>Activator</b>	Activator events
66	<b>ADSL</b>	ADSL events
77	<b>AH</b>	AH events
130	<b>All Classes</b>	All event classes
33	<b>AODI</b>	AODI events
111	<b>AOT/XOT</b>	Asynchronous Over TCP and X25 Over TCT events
64	<b>ATM</b>	ATM events
46	<b>Authentication</b>	PPP Authentication events
54	<b>BACP</b>	Bandwidth Allocation Control Protocol events
50	<b>Bandwidth Management</b>	Bandwidth Management events
47	<b>BAP</b>	Bandwidth Allocation Protocol events
19	<b>BCP</b>	BCP events
61	<b>BOOTP</b>	BOOTP events
103	<b>BRI</b>	BRI events
14	<b>Bridging</b>	Bridging events
31	<b>Call Control</b>	Call Control events
45	<b>Call History</b>	Call History events
41	<b>Call Usage</b>	Call Usage events
20	<b>CCP</b>	CCP events
79	<b>CMGR</b>	CMGR events
8	<b>Configuration</b>	Configuration Events
25	<b>Console</b>	Console events
35	<b>DHCP</b>	DHCP events
105	<b>DHCP Client</b>	DHCP client events
81	<b>DiffServ</b>	Diffserv events
42	<b>DNS Proxy Server</b>	DNS Proxy Server events
60	<b>DST</b>	DST events
76	<b>ESP</b>	ESP events
21	<b>Ethernet</b>	Ethernet events
51	<b>Feature Key</b>	License Key events
84	<b>Firewall</b>	Firewall events
23	<b>Frame Relay</b>	Frame Relay events
121	<b>FRAMEBR</b>	Frame Bridge events
59	<b>FTP</b>	File Transfer Protocol events
69	<b>General</b>	General system events
109	<b>GRE</b>	GRE events
98	<b>GSHDSL</b>	GSHDSL events
108	<b>HTTP Proxy</b>	HTTP Proxy events
88	<b>HTTPC</b>	HTTPC events

<b>104</b>	<b>IGMP</b>	IGMP events
<b>73</b>	<b>IKE</b>	IKE events
<b>12</b>	<b>IP</b>	IP events
<b>78</b>	<b>IP Route</b>	IP Routing events
<b>107</b>	<b>IPAT</b>	IPAT events
<b>17</b>	<b>IPCP</b>	IPCP events
<b>39</b>	<b>IPCP State</b>	IPCP state change events
<b>72</b>	<b>IPSEC</b>	IPSec events
<b>13</b>	<b>IPX</b>	IP Exchange events
<b>18</b>	<b>IPXCP</b>	IP Exchange Control Protocol events
<b>15</b>	<b>ISDN LAPD</b>	ISDN events at the Linked Access Protocol channel D layer events
<b>48</b>	<b>ISDN Physical</b>	ISDN layer 1 events
<b>34</b>	<b>ISDN Q931</b>	ISDN Q931 specific events
<b>36</b>	<b>ISDN SPID</b>	ISDN SPID events
<b>129</b>	<b>ISDNBR</b>	ISDN Bridging events
<b>118</b>	<b>ISDNTCP</b>	ISDN TCP events
<b>100</b>	<b>ITH</b>	ISDN Test Harness events
<b>16</b>	<b>LCP</b>	LCP events
<b>123</b>	<b>MUAL</b>	Maul events
<b>10</b>	<b>Memory</b>	Memory Events
<b>110</b>	<b>MGCP</b>	MGCP events
<b>75</b>	<b>MKMD</b>	MKMD events
<b>86</b>	<b>Modem</b>	Modem events
<b>112</b>	<b>MOT</b>	Memocam events
<b>38</b>	<b>Multilink PPP</b>	Multilink PPP events
<b>106</b>	<b>NetBios</b>	Netbios events
<b>29</b>	<b>NTP</b>	NTP events
<b>120</b>	<b>PAD</b>	XOT events
<b>80</b>	<b>PDD</b>	POTS PDD events
<b>11</b>	<b>Performance</b>	Performance Events
<b>67</b>	<b>POE</b>	Point to Point Protocol over Ethernet events
<b>58</b>	<b>POP3</b>	POP3 events
<b>37</b>	<b>POTS</b>	POTS events
<b>53</b>	<b>Power Status</b>	Power Status events
<b>32</b>	<b>PPP</b>	General Point to Point Protocol events
<b>55</b>	<b>PPP LCP</b>	Point to Point Protocol Link Control Protocol events
<b>40</b>	<b>PPP State</b>	Point to Point Protocol state change events
<b>99</b>	<b>PRI</b>	PRI events
<b>102</b>	<b>PRITH</b>	PRI Test Harness events
<b>128</b>	<b>PROSLIC</b>	Prosllic events
<b>57</b>	<b>ProxyLib</b>	General proxy events
<b>68</b>	<b>PTL Detect</b>	Automatic Protocol Detection events
<b>115</b>	<b>Radius</b>	Radius events
<b>62</b>	<b>RIP</b>	RIP events
<b>74</b>	<b>SAD</b>	Security Authentication D events
<b>70</b>	<b>Scheduler</b>	Scheduler events
<b>49</b>	<b>Script</b>	Script events

<b>124</b>	<b>SCTP</b>	Stream Control Transmission Protocol events
<b>9</b>	<b>Security</b>	Security Events
<b>24</b>	<b>Serial</b>	Serial events
<b>114</b>	<b>SGW</b>	Secure Gateway events
<b>113</b>	<b>SIP</b>	SIP events
<b>117</b>	<b>Skinny</b>	Skinny events
<b>63</b>	<b>SMTP</b>	SMTP events
<b>27</b>	<b>SNMP</b>	SNMP events
<b>71</b>	<b>SPD</b>	SPD events
<b>52</b>	<b>Syslog</b>	Syslog events
<b>101</b>	<b>T1E1</b>	T1E1 events
<b>26</b>	<b>Telnet</b>	Telnet events
<b>119</b>	<b>TERMSERV</b>	Terminal server events
<b>30</b>	<b>TFTP</b>	Trivial File Transfer Protocol events
<b>44</b>	<b>Upload</b>	Upload events
<b>122</b>	<b>USB</b>	USB events
<b>43</b>	<b>User Profile</b>	User profile events
<b>82</b>	<b>VDSL</b>	VDSL events
<b>83</b>	<b>VOIP</b>	Voice over Internet Protocol events
<b>127</b>	<b>VQMON</b>	Detects packet loss and jitter buffer discard events
<b>126</b>	<b>VRRP</b>	VRRP events
<b>56</b>	<b>WAN</b>	WAN events
<b>28</b>	<b>Web</b>	Web events
<b>22</b>	<b>X25</b>	X25 events