Configuring ISG Troubleshooting Enhancements

The Intelligent Services Gateway (ISG) debugging enhancements enable you to more easily isolate issues with ISG subscriber sessions in a production network, such as a session getting stuck in a dangling state (never reaches the established state). The troubleshooting enhancements described in this module allow you to diagnose these issues by introducing expanded statistics collection and event tracing.

Information About ISG Troubleshooting Enhancements

Event Tracing for Subscriber Sessions

When trying to reproduce or capture customer issues, collecting debug output is not always practical or even possible. Network administrators often do not detect an error until long after the event that caused the error has occurred. By the time a fault is detected, it is usually too late to enable debug commands because the session is already in an error state, or the session was terminated because of an error.

Event tracing allows you to capture traces for existing sessions on the router and to retain the history of any past sessions that were marked as interesting, such as a session that became stuck in a dangling state. This enables you to look at existing sessions, as well as past sessions, and review the data after the session gets into an unexpected state or never comes up.

If a session is marked as interesting, its event trace information is sent to a history log, if history logging is enabled. A session is considered interesting if it becomes stuck in a state, enters an error state, or terminates without transitioning into a target state, because of a programming error, end-user action, packet drop, or other reason. The decision whether to log an event trace is determined by the after-the-fact status of the object. Event traces for uninteresting sessions are removed to free up space in the history log buffer.

Previously, the event trace data for each subscriber session was attached to its session context. This data was purged when the session was terminated. These enhancements preserve the event trace data even after the sessions are gone.

Each session context that supports event trace creates a new event trace log to hold the event traces for that session context. The event trace logs can be displayed independently through **show** commands.

Dumping Event Traces

ISG event traces are enabled to capture the trace logs by default. All the event trace logs are stored in the device memory. When the device reloads due to crash, the trace logs are lost and it becomes difficult to debug issues that causes the crash.

To prevent losing the trace logs, event trace logs are saved in a pre-configured file. ISG event traces are collected and saved in a file that is pre-configured in the device. If the filename is not configured, event traces cannot be collected. So, it is recommended to configure the filename to collect and save event trace logs during a crash.

Note To collect the event traces, ensure to configure the file location as bootflash. You cannot collect the event traces in a hard disk.

This example shows how to collect the event traces in a text file.

```
Device #
Device # configure terminal
Device(config)# monitor event-trace subscriber dump-file bootflash:isg_dump_file.txt
```

How to Enable ISG Troubleshooting Enhancements

Enabling Event Tracing for ISG Sessions

Perform the following steps to enable event tracing for ISG subscriber sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor event-trace subscriber** *dump-file*
4. **monitor event-trace subscriber enable**
5. **exit**
6. **no monitor event-trace subscriber**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**monitor event-trace subscriber** *dump-file* **Example:** `Router(config)# monitor event-trace subscriber dump-file`	Sets the dump file name to be used to collect traces.

Step 4	**monitor event-trace subscriber enable**
	Example:
	`Router(config)# monitor event-trace subscriber enable`
	`Router(config)# monitor event-trace subscriber ?`
	`feature Feature manager traces`
	`gx GX traces`
	`ip-sip IP-SIP traces`
	`policy Policy manager trace`
	`ppp PPP traces`
	`service Service manager trace`
	`session Subscriber Subsystem trace`
	`vpdn VPDN Traces`
		Enables event tracing for all the subscriber sessions.
		Note You can enable event tracing for ISG componets, IP-SIP, policy, PPP, service, session, VPDN, and feature.

Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**no monitor event-trace subscriber** **Example:** `Router(config)# no monitor event-trace subscriber`	Disables traces for all components at all levels.

Displaying Event Traces for ISG Sessions

Use the following commands to display information about the event traces that are saved in text file.

SUMMARY STEPS

1. **show monitor event-trace subscriber**

DETAILED STEPS

show monitor event-trace subscriber

Use this command to display about the event traces that were saved in text file.

Example:

```
Router# show monitor event-trace subscriber
all-traces Show all the event traces
 feature Feature manager trace
 gx GX trace
 identifier Filter traces based on identity of session
 ip-sip IP-SIP trace
 policy SSS Policy manager trace
 ppp PPP trace
 service Service manager trace
 session SSS trace
 vpdn VPDN trace
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Debug commands	Cisco IOS Debug Command Reference .
DHCP Configuration	Part 3, “DHCP,” *IP Addressing Configuration Guide*.
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
ISG subscriber sessions	"Configuring ISG Access for IP Subscriber Sessions" module in this guide

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Troubleshooting Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for ISG Troubleshooting Enhancements

Feature Name	Releases	Feature Information
Dumping event-traces along with the crash	Cisco IOS XE Fuji 16.9.1	ISG event traces are enabled to track trace logs. The following command is introduced. **monitor event-trace subscriber** *dump-file bootflash:isg_dump_file.txt*