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.

- Restrictions for ISG Troubleshooting Enhancements, page 1
- Information About ISG Troubleshooting Enhancements, page 1
- How to Enable ISG Troubleshooting Enhancements, page 2
- Configuration Examples for ISG Troubleshooting Enhancements, page 7
- Additional References, page 7
- Feature Information for ISG Troubleshooting Enhancements, page 9

Restrictions for ISG Troubleshooting Enhancements

Enabling the **subscribertracehistory** command does not mean that all event traces for subscriber sessions are stored in the history buffer. Event traces for the DPM and PM are written to their respective history buffers only if a session has an issue (such as a session that becomes a dangling session).

Information About ISG Troubleshooting Enhancements

DPM Statistics

The DHCP policy module (DPM) has many complex interactions with other components such as the policy manager (PM) module, which can make it difficult to troubleshoot issues and find the root cause. For example, dangling IP sessions are often caused by an error in the interactions between DHCP, the DPM, and the PM, resulting in DPM sessions getting stuck in a startup state.

The DPM enhancements enable more efficient debugging of issues with DPM and its interactions in customer networks. This includes improved statistics collection at both the system and session level to show failure data, more comprehensive error messages, and event tracing.

DPM contexts could previously be displayed only by selecting the MAC address. These enhancements add the ability to search and display all DPM contexts on the router, DPM contexts for a particular client IP address, or DPM contexts in a particular state. All debug output is now prefixed with the DPM context identifier and MAC address so that in a large-scale scenario you can identify debugs for a particular transaction.

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.

Event tracing is supported by the DPM and PM modules. Each module logs event traces for each of its session contexts independently. The event trace data for each subscriber session is attached to its session context. Previously, 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 new event log is created at session startup or teardown, and is destroyed after the session reaches the established or destroyed state. The event trace logs can be displayed independently through **show** commands.

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. **subscriber trace event** {**dpm** | **pm**} [**retain**]
4. **subscriber trace history** {**dpm** | **pm**} [**size***max-records*]
5. **exit**

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:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**subscriber trace event** {**dpm** | **pm**} [**retain**] **Example:** `Router(config)# subscriber trace event dpm retain`	Enables event tracing for ISG subscriber sessions. • This command, without the **retain** keyword, is enabled by default for the DPM and PM.
Step 4	**subscriber trace history** {**dpm** | **pm**} [**size***max-records*] **Example:** `Router(config)# subscriber trace history dpm size 200`	Enables saving the event traces for ISG subscriber sessions to a history log. • This command, without the **size**keyword, is enabled by default for the DPM and PM. Default log size is 100 records.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Displaying Event Traces for ISG Sessions

Use the following commands to display information about the event traces that are saved to the history log for the specified module. You can use these commands in any order.

SUMMARY STEPS

1. **show subscriber trace statistics**
2. **show subscriber trace history** {**all** | **dpm** | **pm**} [**all** | **client-ip-address***ip-address* | **mac-address***mac-address* | **reason***number* | **uid***session-id*]
3. **clear subscriber trace history** {**dpm** | **pm**}

DETAILED STEPS

Step 1 **show subscriber trace statistics**

Use this command to display statistics about the event traces that were saved to the history log.

Example:

```
Router# show subscriber trace statistics
Event Trace History Statistics: DPM
Logging enabled
All time max records: 5
Max records: 5
Current records: 5
Current log size: 200
Proposed log size 200
Oldest, newest index: 0 : 4
Event Trace History Statistics: Policy Manager
Logging enabled
All time max records: 4
Max records: 4
Current records: 4
Current log size: 64
Proposed log size 64
Oldest, newest index: 0 : 3
```

Step 2 **show subscriber trace history** {**all** | **dpm** | **pm**} [**all** | **client-ip-address***ip-address* | **mac-address***mac-address* | **reason***number* | **uid***session-id*]

Use this command to display a summary of all session traces stored in the trace history log, or to display a complete trace for a specific session by using one of the optional keywords. The following example shows output for the client with IP address 10.0.0.2.

Example:

```
Router# show subscriber trace history dpm client-ip-address 10.0.0.2
DPM session info: 5CB2A60
MAC: aaaa.2222.cccc IP: 10.0.0.2
UID: 3 reason: PM callback to clear
========================
ET 11:33:48.767 PST Mon Aug 30 2010 dhcp get class
       rc no c-aware cfg
ET 11:34:07.327 PST Mon Aug 30 2010 i-if change
       ,MAC ok,ignore: same i/f
ET 11:34:07.327 PST Mon Aug 30 2010 dhcp discover
       rc OK,proc prev req
ET 11:34:07.327 PST Mon Aug 30 2010 dhcp get class
       rc no c-aware cfg
ET 11:34:10.835 PST Mon Aug 30 2010 i-if change
       ,MAC ok,ignore: same i/f
ET 11:34:10.835 PST Mon Aug 30 2010 dhcp discover
       rc OK,proc prev req
ET 11:34:10.835 PST Mon Aug 30 2010 dhcp get class
       rc no c-aware cfg
ET 11:34:14.843 PST Mon Aug 30 2010 i-if change
       ,MAC ok,ignore: same i/f
ET 11:34:14.843 PST Mon Aug 30 2010 dhcp discover
       rc OK,proc prev req
ET 11:34:14.843 PST Mon Aug 30 2010 dhcp get class
       rc no c-aware cfg
ET 11:34:38.391 PST Mon Aug 30 2010 i-if change
       ,MAC ok,ignore: same i/f
ET 11:34:38.391 PST Mon Aug 30 2010 dhcp discover
       rc OK,proc prev req
ET 11:34:38.391 PST Mon Aug 30 2010 dhcp get class
```

```
       rc no c-aware cfg
ET 11:34:41.923 PST Mon Aug 30 2010 i-if change
       ,MAC ok,ignore: same i/f
ET 11:34:41.923 PST Mon Aug 30 2010 dhcp discover
       rc OK,proc prev req
ET 11:34:41.923 PST Mon Aug 30 2010 dhcp get class
       rc no c-aware cfg
ET 11:34:45.931 PST Mon Aug 30 2010 i-if change
       ,MAC ok,ignore: same i/f
ET 11:34:45.931 PST Mon Aug 30 2010 dhcp discover
       rc OK,proc prev req
ET 11:34:45.931 PST Mon Aug 30 2010 dhcp get class
       rc no c-aware cfg
ET 11:35:13.591 PST Mon Aug 30 2010 PM callback
       Terminate, rc end sess,Case: REQ_TERMINATE
```

Step 3 **clear subscriber trace history** {**dpm** | **pm**}
Use this command to clear the event trace history log for the specified module.

Example:

```
Router# clear subscriber trace history dpm
```

Displaying DPM Statistics

Use the following commands to display information about event traces for DPM session contexts.

SUMMARY STEPS

1. **debug subscriber policy dpm timestamps**
2. **show ip dhcp sip session** [**detailed** | **mac-address** *mac-address*]
3. **show ip dhcp sip statistics**
4. **clear subscriber policy dpm statistics**

DETAILED STEPS

Step 1 **debug subscriber policy dpm timestamps**
Use this command to include timestamp information for DPM messages in debugging output.

Example:

```
Router# debug subscriber policy dpm timestamps
SG dhcp message timestamps debugging is on
```

Step 2 **show ip dhcp sip session** [**detailed** | **mac-address** *mac-address*]
Use this command to display event traces for DHCP session contexts. The following example shows output for the client with the MAC address e84e.0614.9dc1.

Example:

```
Router# show ip dhcp sip session mac-address e84e.0614.9dc1
DHCP SIP Session context with MAC Address: e84e.0614.9dc1
UID                :19
SSS Hdl            :0x87000030
AAA Uid            :39
Access IE Hdl      :0xAE000013
IP Session Hdl     :0x2200000E
SHDB Hdl           :0xCD000015
Current State      :Up
Last State         :Address Authorization
Last Event         :Address Authorization Done Ev
Last to Last State :Authorized
Last to Last Event :Address Authorize Ev
Access interface   :Tunnel1
Incoming interface :Tunnel1
Elapsed-time(start):never
IP Addr            :50.0.0.37
Elapsed-time
  since Addr acked :00:08:29
VRF ID               :0
IP Domain            :0
Class name         :orange_open (len = 11)
Circuit ID         :hotspot:130.0.40.5:OPEN:CPE2
Remote ID          :unauthenticated
Class ID           :MSFT 5.0
Session Type       :Dedicated
Default Configs are set as:
    Class name     :orange_open (len = 11)
    IP Domain      :0
    VRF ID         :0
Session updated    :False
Dynamic sync       :False
```

Step 3 **show ip dhcp sip statistics**

Use this command to display statistics for DHCP session contexts.

Example:

```
Router# show ip dhcp sip statistics
Total Sessions           1
Total lite Sessions      0
Config callbacks         13
Author callbacks         12
SSS Successes            14
IPsub Triggrs            12
IPsub Successes          13
IPsub Failures           0
Sessions started         15
Sessions destroyed       14
Sessions restarted       22
Sessions failed          0
Avg SSS response time    358 ms
Avg IPsub response time  85025492 ms

Session up events        0
Session down events      0
Dynamic updates          0
Sync failures            0

Summary of sessions in each state:
0 )Initial                       0
1 )Waiting for config            0
2 )Authorized                    0
3 )Address Authorization         0
```

```
4 )Up                           1
5 )Down                         0
6 )Waiting for cleanup          0
7 )Restart on data              0
8 )Restart on dhcp              0
9 )Sync-restart                 0
10)Start-on-sync/reload         0
11)Restart-wait addr            0
12)Dead                         0
```

Step 4 **clear subscriber policy dpm statistics**
Use this command to clear the statistics for DPM contexts.

Example:

```
Router# clear subscriber policy dpm statistics
```

Configuration Examples for ISG Troubleshooting Enhancements

Example Enabling Event Tracing for ISG Sessions

The following example shows a configuration with the DPM and PM event tracing enabled and retained. Trace history logging is enabled for the DPM and PM so traces for sessions that are marked as interesting are stored in their respective history log. Up to 100 sessions (default) can be stored in the PM history log, and up to 200 sessions can be stored in the DPM history log.

```
subscriber trace event dpm retain
subscriber trace event pm retain
subscriber trace history pm
subscriber trace history dpm size 200
```

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

Related Topic	Document Title
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
DPM/PM Debuggability Enhancements	12.2(33)SB9 15.1(2)S Cisco IOS XE Release 3.3S	This feature enhances debugging for ISG subscriber sessions enabling you to isolate issues through expanded statistics collection and event tracing. The following commands were introduced or modified: **clear subscriber policy dpm statistics**, **clear subscriber trace history**, **debug subscriber policy dpm timestamps**, **show ip dhcp sip session** [**detailed** | **mac-address** *mac-address*] , **show ip dhcp sip statistics** , **show subscriber trace history**, **show subscriber trace statistics**, **subscriber trace event**, **subscriber trace history**.