



Unexpected Source Address Alerting

You can configure the SBC to provide alerts for any received unexpected source addresses. After the SBC receives an unexpected source address, it creates a log and generates an SNMP trap.

Feature History for Unexpected Source Address Alerting

Release	Modification
Release 3.4.1	This feature was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.
Release 3.6.0	No modification.

Contents

This module contains the following sections:

- [Prerequisites for Unexpected Source Address Alerting](#), page SBC-263
- [Restrictions for Unexpected Source Address Alerting](#), page SBC-264
- [Information About Unexpected Source Address Alerting](#), page SBC-264
- [How to Configure Unexpected Source Address Alerting](#), page SBC-264
- [Examples of Configuring Unexpected Source Address Alerting](#), page SBC-265
- [Additional References](#), page SBC-267

Prerequisites for Unexpected Source Address Alerting

The following prerequisites are required before you can receive alerts for unexpected source addresses:

- You must be in a user group associated with a task group that includes the proper task IDs for SBC commands being used. For detailed information about user groups and task IDs, see the defined task ID required per command in the *Cisco IOS XR Session Border Controller Command Reference*.
- You must install and activate the package installation envelope (PIE) for the SBC software.
For detailed information about PIE installation, refer to the *Upgrading and Managing Cisco IOS XR Software* module in the *Cisco IOS XR Getting Started Guide*.
- The SBC must already be created. See the procedures described in the [SBC Configuration Prerequisites](#) section.

Restrictions for Unexpected Source Address Alerting

Review the following restrictions for unexpected source address alerting:

- This configuration option should only be enabled on trusted networks where any single such instance might indicate a threat to network security.
- Alerts on the same flow are rate-limited as are the total number of alerts reported at any one time to ensure management systems are not flooded with reports. There is not a one-to-one correspondence between alerts and incorrect packets.
- Diagnosing and resolving the issue of rogue packets is beyond the scope of the SBC function.
- Any and all packets from unexpected sources are dropped.

Information About Unexpected Source Address Alerting

If a packet with unexpected source address/port is received by the DBE on a media address, port, or (if applicable) VRF used by a current call, then the DBE creates a log and generates an SNMP trap on the appropriate media-flow-stats MIB.

The log (level 63) is output to the console automatically (by default). The log is a member of the MEDIA debug log group. The log includes the local address, port, and VRF where the packets were received and also the source address and port of the received packet.

An alert is generated the first time an unexpected packet is received on a port after the port is opened for a call. If additional unexpected packets are received on the same media port, additional alerts are generated. Any additional alerts are rate-limited. After the call is completed, the media port is assigned to a new call, and the state is reset. A new alert is then generated if any additional unexpected packets are subsequently received.

The SNMP trap that is generated will contain the following fields:

- The address and port where the unexpected packet was received.
- The address and port where the unexpected packet originated.

**Note**

The blacklist trap will include ID AMB_TRAP_MW_DBL_BLACKLIST (as defined in db10mib.h) and the alerting trap will include ID AMB_TRAP_MGM_MEDIA_SOURCE_ALERT (as defined in bmm0mib.h).

How to Configure Unexpected Source Address Alerting

SUMMARY STEPS

1. **configure**
2. **sbc** *service-name* **dbe**
3. **vdbe** *vdbe-name*
4. **unexpected-source-alerting**
5. **commit**
6. **exit**

7. `show services sbc service-name dbe media-flow-stats vrf vrf-name [ipv4 A.B.C.D [port port-number]]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure</code> Example: RP/0/0/CPU0:router# <code>configure</code>	Enables global configuration mode.
Step 2	<code>sbc service-name dbe</code> Example: RP/0/0/CPU0:router(config)# <code>sbc mysbc dbe</code>	Enters a submode where alerts can be configured for unexpected source addresses. Use the <i>service-name</i> argument to define the name of the service.
Step 3	<code>vdbe vdbe-name</code> Example: RP/0/0/CPU0:router(config-sbc-dbe)# <code>vdbe myvDbe</code>	Enters a submode where alerts can be configured for unexpected source addresses. Use the <i>vdbe-name</i> argument to define the name of the service.
Step 4	<code>unexpected-source-alerting</code> Example: RP/0/0/CPU0:router(config-sbc-dbe-vdbe)# <code>unexpected-source-alerting</code>	Sets alerting for unexpected source addresses. The no form of this command removes alerting for any unexpected source addresses that are received.
Step 5	<code>commit</code> Example: RP/0/0/CPU0:router(config-sbc-dbe-vdbe)# <code>commit</code>	Saves configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 6	<code>exit</code> Example: RP/0/0/CPU0:router(config-sbc-dbe-vdbe)# <code>exit</code>	Exits the unexpected-source-alerting mode to the DBE mode.
Step 7	<code>show services sbc service-name dbe media-flow-stats vrf vrf-name [ipv4 A.B.C.D [port port-number]]</code> Example: RP/0/0/CPU0:router(config-sbc-dbe)# <code>show services sbc mysbc dbe media-flow-stats vrf vpn3 ipv4 10.1.1.1 port 24000</code>	Displays detailed information about the media flow statistics configured on the DBE.

Examples of Configuring Unexpected Source Address Alerting

This section provides a sample configuration and output for configuring unexpected source address alerting including an example of the information added to the media flow statistics.

Example of Configuring Unexpected Source Address Alerting

To configure unexpected source address alerting, use the following commands:

```
configure
  sbc mysbc
  dbe
  vdbe myvDbe
  unexpected-source-alerting
end
```

Example of Enhancement to Media Flow Statistics

The following example shows the commands required to list the statistics about one or more media flows collected on the DBE. These statistics are collected in realtime when the overall command is issued.

```
configure
  sbc mysbc
  dbe
  media-flow-stats vrf vpn3 ipv4 10.1.1.1 port 24000

SBC Service "mySbc"
mediaFlow 1
  FlowPairState Open
  GateAge 15340 ms
  CallPriority Normal
  FlowPairBandwidth 1500
  DtmfPacketsQueued 0
  Side A
    VpnId vpn3
    LocalAddress 10.1.1.1
    LocalPort 24000
    RemoteAddress 192.168.1.1
    RemotePort 32420
    RtpPacketsRcvd 300
    RtpOctetsRcvd 6000
    RtpPacketsSent 100
    RtpOctetsSent 2000
    RtpPacketsDiscarded 0
    RtpOctetsDiscarded 0
    EndPointPacketsSent 300
    EndPointPacketsRcvd 97
    EndPointPacketsLost 1
    DtmfInterworking No
    MediaFlowing Yes
    RouteError No
    Unexpected SrcAddr Packets Yes
    BillingId 12AB3C4D567124C7124C12DE
  Side B
    VpnId <none>
    LocalAddress 10.1.1.2
    LocalPort 24002
    RemoteAddress 172.192.2.3
    RemotePort 24002
    RtpPacketsRcvd 100
    RtpOctetsRcvd 2000
    RtpPacketsSent 300
    RtpOctetsSent 6000
    RtpPacketsDiscarded 0
    RtpOctetsDiscarded 0
```

```

EndPointPacketsSent 100
EndPointPacketsRcvd 300
EndPointPacketsLost 0
DtmfInterworking No
MediaFlowing Yes
RouteError No
Unexpected SrcAddr Packets No
BillingId 5DAB3C4D153624C7124E1234

```

Additional References

The following sections provide references related to configuring alerting for unexpected source addresses.

Related Documents

Related Topic	Document Title
Cisco IOS XR master command reference	Cisco IOS XR Master Commands List
Cisco IOS XR SBC interface configuration commands	<i>Cisco IOS XR Session Border Controller Command Reference</i>
Initial system bootup and configuration information for a router using the Cisco IOS XR Software	<i>Cisco IOS XR Getting Started Guide</i>
Cisco IOS XR command modes	<i>Cisco IOS XR Command Mode Reference</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support from existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport