



Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model

November 22, 2011

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model
© 2008 - 2011 Cisco Systems, Inc. All rights reserved.



Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model

The commands listed in this command reference are Cisco Unified Border Element (SP Edition) distributed model commands.

Cisco Unified Border Element (SP Edition) was formerly known as Cisco Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC). The name of this command reference was changed in August, 2009.

activate

To initiate the data border element (DBE) service of the session border controller (SBC), use the **activate** command in SBC-DBE configuration mode. To deactivate the DBE service, use the **no** form of this command.

activate

no activate

Syntax Description

This command has no arguments or keywords.

Command Default

The default state is that the DBE is not activated.

Command Modes

SBC-DBE configuration (config-sbc-dbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

After all DBE address configuration is completed, the **activate** command initiates the DBE service of the SBC. The command ensures that the DBE is not started in an inconsistent state.

Use the **sbc dbe** command to enter into SBC-DBE configuration mode first.

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration mode, and activates the DBE service with the **activate** command:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# activate
```

Related Commands

Command	Description
sbc dbe	Creates the data border element (DBE) service on a session border controller (SBC) and enters into the SBC-DBE configuration mode.
deactivation-mode	Specifies the action the data border element (DBE) of a session border controller (SBC) takes upon deactivation of the DBE service.

attach-controllers

To configure a data border element (DBE) to attach to an H.248 controller, use the **attach-controllers** command in VDBE configuration mode. To detach the DBE from its controller, use the **no** form of this command.

attach-controllers

no attach-controllers

Syntax Description This command has no arguments or keywords.

Command Default The default is that no controllers are attached.

Command Modes VDBE configuration (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines The attachment and detachment of the DBE from its controller does not always complete immediately. To view the current attachment status, use the **show sbc dbe controllers** command.

Examples In a configuration where the DBE has been created and controllers have been configured, the following example shows how to attach the DBE to a controller in VDBE configuration mode:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# attach-controllers
Router(config-sbc-dbe-vdbe)# end
```

Related Commands	Command	Description
	vdbe	Configures a virtual data border element (vDBE) and enters the VDBE configuration mode.
	show sbc dbe controllers	Displays the media gateway controllers and the controller address configured on each DBE.

bandwidth-fields mandatory

To set the bandwidth description of Session Description Protocol (SDP) as mandatory, use the **bandwidth-fields mandatory** command in Virtual Data Border Element (VDBE) configuration mode. To set the bandwidth description as optional, use the **no** form of this command.

bandwidth-fields mandatory

no bandwidth-fields

Syntax Description

This command has no arguments or keywords.

Command Default

The default behaviour is that the bandwidth description of SDP is optional.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

To use this command, you must be in a user group that is associated with a task group that includes the proper task IDs. To use this command, you must be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

Examples

The following example shows how to set the bandwidth description of the SDP as mandatory in the VDBE configuration mode:

```
Router# configure terminal
Router# sbc sbc dbe
Router(config-sbc-dbe)# vdb global
Router(config-sbc-dbe-vdbe)# bandwidth-fields mandatory
```

Related Commands

Command	Description
vdb	Enters VDBE configuration mode.

bandwidth-police tman

To configure the data border element (DBE) to perform no bandwidth policing unless either Traffic Management (Tman) properties, tman/pdr and tman/sdr, or all, are specified in the media and signaling flows, use the **bandwidth-police tman** command in Virtual Data Border Element (VDBE) configuration mode. To reset to the default behavior, use the **no** form of this command.

bandwidth-police tman

no bandwidth-police tman

Syntax Description This command has no arguments or keywords.

Command Default The default behavior is to perform bandwidth policing based on information from the b-line of the session description protocol (SDP).

Command Modes VDBE configuration (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines In Cisco IOS XE Release 2.6, this command implements the Optional Tman Bandwidth Parameter Policing feature. The command configures the DBE to perform no traffic policing unless either Traffic Management (Tman) properties, tman/pdr and tman/sdr, or all, are specified in the media and signaling flows. In effect, this command disables bandwidth traffic policing if either tman/pdr or tman/sdr is missing, and disregards the b-line information. When the DBE performs no traffic policing, it means the DBE does not drop packets if bandwidth is exceeded.

The Optional Tman Bandwidth Parameter Policing feature improves H.248 interworking capability with the Traffic Management (Tman) package. This feature is used to disable bandwidth policing from using b-line information when Tman parameters are missing. This complies with the Tman package definition of the ETSI Ia profile (ETSI ES 283 018 V2.4.1 (2008-09), 5.17.1.5.5), which states that traffic policing shall not be done based on the b-line.

If the **bandwidth-police tman** command is configured and tman/pdr or tman/sdr is received from the media gateway controller (MGC), the DBE performs bandwidth policing using tman/pdr or tman/sdr.

The **no bandwidth-police tman** form of the command sets the default behavior, which is to perform bandwidth policing based on information from the bandwidth, b- line, of the SDP when Tman parameters are missing. This default behavior was the behavior prior to Cisco IOS XE Release 2.6 where, if *both* tman/pdr and tman/sdr are missing, the DBE would do bandwidth policing based on information from the b-line.

The command is implemented in the following manner:

When the feature is *turned on* with the **bandwidth-police tman** command configured on the DBE:

- If the DBE receives *no* Tman parameters, the DBE does not perform traffic policing.
- If tman/pol=ON and the DBE receives tman/pdr or tman/sdr parameters, the DBE performs bandwidth traffic policing based on Tman parameters.
- If tman/pol=ON and the DBE receives *no* tman/pdr or tman/sdr parameters, the DBE does not perform traffic policing.
- If tman/pol=OFF and the DBE receives *no* tman/pdr or tman/sdr parameters, the DBE does not perform traffic policing.

When the feature is *turned off* with the **no bandwidth-police tman** command configured on the DBE:

- If the DBE receives *no* Tman parameters, the DBE performs traffic policing based on the b-line information in the SDP.
- If the DBE receives Tman parameters, the DBE performs traffic policing based on Tman parameters.
- If tman/pol=OFF and the DBE receives *no* tman/pdr or tman/sdr parameters, the DBE does not perform traffic policing.
- If tman/pol=OFF and the DBE receives tman/pdr or tman/sdr parameters, the DBE does not perform traffic policing.



Note

When the feature is *turned off* with the **no bandwidth-police tman** command, the DBE behavior is generally the same behavior as prior to Cisco IOS XE Release 2.6.

Examples

In the following example, the DBE is configured to perform no traffic policing unless tman/pdr and/or tman/sdr properties in the Traffic Management (Tman) package are specified; if tman/pdr and tman/sdr are in the flow, policing is performed using tman/pdr or tman/sdr.

```
Router# configure terminal
Router(config)# sbc global db
Router(config-sbc-dbe)# vdb global
Router(config-sbc-dbe-vdb)# bandwidth-police tman
```

The following example sets the default behavior to configure the DBE to perform bandwidth policing based on information from the b-line of the SDP; this assumes the DBE received no Tman parameters:

```
Router# configure terminal
Router(config)# sbc global db
Router(config-sbc-dbe)# vdb global
Router(config-sbc-dbe-vdb)# no bandwidth-police tman
```

Related Commands

Command	Description
sbc db	Creates the DBE service on a SBC and enters into the SBC-DBE configuration mode.
vdb	Configures a VDBE and enters the VDBE configuration mode.

clear sbc dbe media-stats

To clear all the statistics collected by the media gateway manager of the data border element (DBE), use the **clear sbc dbe media-stats** command in privileged EXEC mode.

clear sbc {*sbc-name*} **dbe media-stats**

Syntax Description	<i>sbc-name</i> Name of the session border controller (SBC) service.
---------------------------	--

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	This command clears the statistics displayed by the show sbc dbe media-stats command and the show sbc dbe forwarder-stats command. It does not clear the statistics displayed by the show sbc dbe media-flow-stats command.
-------------------------	--

Examples	The following example clears all the statistics collected by the media gateway manager of a DBE on an SBC called "mySbc": Router# clear sbc mySbc dbe media-stats
-----------------	---

Related Commands	Command	Description
	show sbc dbe forwarder-stats	Displays the global list of statistics for the DBE forwarding process.
	show sbc dbe media-stats	Displays general DBE statistics. These statistics do not include data from active calls.

congestion-cleared

To configure that the congestion has cleared when the level of system resources reaches the congestion cleared threshold, use the **congestion-cleared** command in VDBE configuration mode. To disable this configuration, use the **no** form of this command.

congestion-cleared {*percentage*}

no congestion-cleared {*percentage*}

Syntax Description

<i>percentage</i>	The percentage of system resources used at which the DBE signals to the SBE that congestion has cleared when the percentage is reached.
-------------------	---

Command Default

The system default percentage is 60% if you do not configure the **congestion-cleared** command or if you configure **no congestion-cleared**.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

When the DBE has previously signaled a congestion event to the SBE, the DBE will signal that the congestion has cleared when the level of system resources used reaches the congestion cleared threshold. This threshold is configured using the **congestion-cleared** command.

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and configures the DBE to signal to the SBE that congestion has cleared at 90% percent of system resources consumed:

```
Router(config)# sbc mySbc db
Router(config-sbc-dbe)# vdb
Router(config-sbc-dbe-vdbe)# congestion-cleared 90
Router(config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
congestion-threshold	Configures the data border element (DBE) to signal a congestion event to the signaling border element (SBE) when a maximum percentage has been reached.

congestion-threshold

To configure the data border element (DBE) to signal a congestion event to the signaling border element (SBE) when a maximum percentage has been reached, use the **congestion-threshold** command in VDBE configuration mode. To disable this configuration, use the **no** form of this command.

congestion-threshold [*percentage*]

no congestion-threshold [*percentage*]

Syntax Description

percentage (Optional) The percentage value of system resources to signal congestion to the SBE.

Command Default

The system default percentage is 80% if you do not configure the **congestion-threshold** command, or if you issue the default **congestion-threshold** command, or if you configure **no congestion-threshold**.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

When the DBE reaches the maximum configured congestion-threshold percentage for either number of calls or media bandwidth, it sends a congestion message to the SBE.

Examples

The following example creates a DBE service on an SBC called "mySbc," enters into SBC-DBE configuration and VDBE configuration modes, and shows how to configure the DBE to signal a congestion event to the SBE when 95% percent of capacity is reached.

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# congestion-threshold 95
Router(config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
congestion-cleared	Configures that the congestion has cleared when the level of system resources reaches the congestion cleared threshold.

control-address h248 ipv4

To configure a data border element (DBE) to use a specific IPv4 H.248 control address, use the **control-address h248 ipv4** command in VDBE configuration mode. To deconfigure a DBE from using an IPv4 H.248 control address, use the **no** form of this command.

control-address h248 ipv4 {*A.B.C.D*}

no control-address h248 ipv4

Syntax Description

<i>A.B.C.D</i>	The IP address for the IPv4 H.248 control address of the DBE, which is the local IP address used to connect to the SBE.
----------------	---

Command Default

No default behavior or values are available.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

If the remote address on any controller is configured, the H.248 control address cannot be changed or deleted, unless you first remove the remote address. To remove the remote address, use the **no remote-address ipv4** command.

Examples

The following example tries to change the control address to IP address 210.229.108.253, while H.248 controllers are configured, and receives the message that the control address cannot be changed while the controllers are configured:

```
Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 210.229.108.253
SBC: control-address cannot be changed while controllers are configured.
```

The following example creates a DBE service on an SBC called "mySbc," enters into SBC-DBE configuration and VDBE configuration modes, and configures the DBE to use 10.0.0.1 as its H.248 control address:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdb
Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 10.0.0.1
Router(config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
attach-controllers	Configures a data border element (DBE) to attach to an H.248 controller.

control-dscp marker-dscp pdr-coefficient

To enable the Two-Rate Three-Color Policing and Marking feature on the data border element (DBE) for each affected traffic flow and to color traffic with a configured differentiated services code point (DSCP) value and configured peak data rate (pdr) coefficient, use the **control-dscp marker-dscp pdr-coefficient** command in VDBE configuration mode. To disable the feature for all traffic flows, use the **no** form of this command.

control-dscp *value1* **marker-dscp** *value2* **pdr-coefficient** *value3*

no control-dscp *value1* **marker-dscp** *value2* **pdr-coefficient** *value3*

Syntax	Description
control-dscp <i>value1</i>	<p>Enables the Two-Rate Three-Color Policing and Marking feature for each affected flow if <i>value1</i>, which is checked against the DSCP value in the diffserv package transmitted via H.248, matches the diffserv DSCP value. <i>value1</i> specifies a DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords:</p> <ul style="list-style-type: none"> af11—AF11 dscp (001010) Assured Forwarding (AF) class af12—AF12 dscp (001100) af13—AF13 dscp (001110) af21—AF21 dscp (010010) af22—AF22 dscp (010100) af23—AF23 dscp (010110) af31—AF31 dscp (011010) af32—AF32 dscp (011100) af33—AF33 dscp (011110) af41—AF41 dscp (100010) af42—AF42 dscp (100100) af43—AF43 dscp (100110) cs1—CS1(precedence 1) dscp (001000) Class Selector (CS) class cs2—CS2(precedence 2) dscp (010000) cs3—CS3(precedence 3) dscp (011000) cs4—CS4(precedence 4) dscp (100000) cs5—CS5(precedence 5) dscp (101000) cs6—CS6(precedence 6) dscp (110000) cs7—CS7(precedence 7) dscp (111000) ef—EF dscp (101110) Expedited Forwarding (EF) class

marker-dscp <i>value2</i>	Colors traffic packets with a DSCP <i>value2</i> . This traffic conforms to the peak data rate (pdr), but does not conform to the sustainable data rate (sdr) that is permitted for the flow. <i>value2</i> specifies a DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, or ef.
pdr-coefficient <i>value3</i>	Calculates the pdr value, using <i>value3</i> , to use as input for coloring traffic packets that conform to pdr, but not to sdr. <i>value3</i> has a value in the range of 101 to 65535. Note The pdr coefficient value is calculated as $pdr = sdr * value3 / 100$, and the pdr value must be greater than the sdr value.

Command Default None

Command Modes VDBE configuration mode (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines The **control-dscp** command is used to enable the Two-Rate Three-Color Policing and Marking feature on the DBE. The **marker-dscp pdr-coefficient** command is used to color traffic that does not conform to the lower sustainable data rate (sdr), but conforms to the higher peak data rate (pdr). This refinement of traffic is done with a DSCP marker (*value2*) and pdr value configured by the CLI (not transmitted from the H.248 diffserv package).

The pdr coefficient value is calculated by the CLI (it is not passed from the H.248 diffserv package) and is used for coloring traffic that conforms to this calculated pdr. The calculated pdr uses the formula: $pdr = sdr * value3 / 100$. *value3* has a range of values (101 to 65535) and is not a DSCP value. The pdr value must be greater than the sdr value.

Examples The following example enables the Two-Rate Three-Color Policing and Marking feature for flows with a diffserv DSCP value matching the configured **control-dscp** value of **af31**. If the feature is enabled on a flow, the **marker-dscp af11** keyword is used to color af11 class of packets that conform to pdr, but do not conform to sdr. In the example, a *value3* of 150 is entered to calculate the pdr coefficient (where pdr is calculated as $pdr = sdr * 150 / 100$).

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# control-dscp af31 marker-dscp af11 pdr-coefficient 150
Router(config-sbc-dbe-vdbe)# exit
```

Related Commands

Command	Description
show sbc dbeforwarder-stat	Displays the global list of statistics for the DBE forwarding processor.

controller h248

To configure the H.248 controller for a data border element (DBE) or enter into Controller H.248 configuration mode, use the **controller h248** command in VDBE configuration mode. To delete the H.248 controller, use the **no** form of this command.

controller h248 {*controller-index*}

no controller h248 {*controller-index*}

Syntax Description

<i>controller-index</i>	The number that identifies the H.248 controller for the DBE, in case you want to configure more than one controller.
-------------------------	--

Command Default

No default behavior or values are available.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Once a controller is configured and attached, it must be detached with the **no attach-controllers** command before you can modify any controller information.



Note

This command is invalid for the unified model, where both the SBE and DBE logical entities co-exist on the same network element.

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and configures an H.248 controller with index 1.

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# controller h248 1
```

The following example configures an H.248 controller with index 1 and tries to configure an IPv4 remote address on the controller. The message indicates that the controller must be detached first before the remote address can be modified.

```
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 210.229.108.253
SBC: remote-address cannot be changed while controllers are attached.
```


Related Commands

Command	Description
sbc db	Creates the data border element (DBE) service on a session border controller (SBC) and enters into the SBC-DBE configuration mode.
vdbe	Configures a virtual data border element (vDBE) and enters the VDBE configuration mode.

deactivation-mode

To specify the action the data border element (DBE) of a session border controller (SBC) takes upon deactivation of the DBE service, use the **deactivation-mode** command in SBC-DBE configuration mode. To revert deactivation behavior to the default of normal behavior, use the **no** form of this command.

deactivation-mode {*deact-type*}

no deactivation-mode

Syntax Description

<i>deact-type</i>	Specifies the action the DBE takes upon deactivation of the DBE service. Set to one of the following types: <ul style="list-style-type: none"> • abort—All calls are dropped with no signaling sent to the signaling border element (SBE). • normal—All calls are immediately terminated when this service change is signaled to the SBE. This is the default behavior if <i>deact-type</i> is not specified or the no deactivation-mode command is executed. • quiesce—No new calls accepted. Deactivation occurs only after existing calls have terminated naturally.
-------------------	--

Command Default

If the deactivation mode is not configured, or the default **deactivation-mode** command or **no deactivation-mode** commands are used, the state of the DBE service becomes normal.

Command Modes

SBC-DBE configuration (config-sbc-dbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **no activate** command to deactivate the DBE service. The **deactivation-mode** command tells the DBE how to behave or what action to take after the DBE is deactivated.

Use the **sbc dbe** command to enter into SBC-DBE configuration mode first.

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration mode, and sets the DBE to deactivate in quiesce mode to prepare the device for hardware maintenance.

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# deactivation-mode quiesce
Router(config-sbc-dbe)# end
```

Related Commands

Command	Description
sbc db	Creates the data border element (DBE) service on a session border controller (SBC) and enters into the SBC-DBE configuration mode.
activate	Initiates the data border element (DBE) service of the session border controller (SBC).

debug sbc filter

To enable logging based on a number of filters, use the **debug sbc filter** command in privileged EXEC mode. To disable logging based on these filters, use the **no** form of this command.

```
debug sbc {sbc-name} filter [adjacency {adj-name}] [bill {billing-id}] [ipv4 {ipv4-address}]
[ipv6 {ipv6-address}] [number {number}] [billing] [call] [media] [overview] [protocol] [bm
| cac | control | h323 | icc | radius | routing | sip | mgm]
```

```
no debug sbc {sbc-name} filter [adjacency {adj-name}] [bill {billing-id}] [ipv4 {ipv4-address}]
[ipv6 {ipv6-address}] [number {number}] [billing] [call] [media] [overview] [protocol] [bm
| cac | control | h323 | icc | radius | routing | sip | mgm]
```

Syntax Description

<i>sbc-name</i>	Name of the session border controller (SBC) service.
adjacency	Output of logs relating to this adjacency.
<i>adj-name</i>	Name of the adjacency.
bill	Log output of calls with a specified billing ID.
<i>billing-id</i>	Billing ID.
ipv4	Output logs that include the IPv4 IP address.
<i>ipv4-address</i>	IPv4 IP address.
ipv6	Output logs that include the IPv6 IP address.
<i>ipv6-address</i>	IPv6 IP address.
number	Output logs of calls with a specified number.
<i>number</i>	Either the caller number or dialed number.
billing	Logs about billing events.
call	Logs about call events.
media	Logs about media events.
overview	Logs showing the flow of control through the session border controller (SBC) components.
protocol	Logs showing protocol messages.
bm	Logs from the Bandwidth Manager (BM) component.
cac	Logs from the Call Admission Control (CAC) components.
control	Logs from the H.248 controller components.
h323	Logs from the H.323 components.
icc	Logs from the Interworking Call Control (ICC) components.
radius	Logs from the RADIUS components.
routing	Logs from the routing components.
sip	Logs from the Session Initiation Protocol (SIP) components.
mgm	Logs from the Media Gateway Manager (MGM) component.

Command Default

Debugging is off.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines You can specify any number of optional keywords, but each keyword can only be specified once. At least one keyword must be specified for the **debug sbc filter** command. You can issue multiple **debug sbc filter** commands.



Note

The debug logs are only output if the appropriate filter keywords have been specified.

The keywords are composed of the following types of filters:

- String filters—Allow the user to turn on logs about common SBC objects such as adjacencies. An object matches the string filter if the object exactly matches the string or the prefix matches the string.

String filters include the following keywords:

- **adjacency** {*adj-name*}
- **bill** {*billing-id*}
- **ipv4** {*ipv4-address*}
- **ipv6** {*ipv6-address*}
- **number** {*number*}

- Component filters—Turn on logs from individual components (or groups of components) within the SBC service. Only one component filter may be specified per **debug sbc filter** command.

Component filters include the following keywords:

bm, cac, control, h323, icc, radius, routing, sip, mgm

- Cross-SBC filters—Turn on logs across all components of the SBC service.

Cross-SBC filters include the following keywords:

billing, call, media, overview, protocol



Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support personnel. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example shows all debug logs for the H.248 control channel to the SBE on an SBC called “mySbc”:

```
Router# debug sbc mySbc filter control
```

The following example shows all debug logs relating to media flows on an SBC called “mySbc”:

```
Router# debug sbc mySbc filter media
```

The following example shows all debug logs relating to media flows with a source or destination address of 10.0.1.1 on an SBC called “mySbc” including output logs for the specified IPv4 IP address:

```
Router# debug sbc mySbc filter media ipv4 10.0.1.1
```

The following example shows that if you want to show all debug logs that relate to media flowing to and from 10.0.1.1 *or* 10.0.1.2, you must issue the following two commands:

```
Router# debug sbc mySbc filter media ipv4 10.0.1.1
```

```
Router# debug sbc mySbc filter media ipv4 10.0.1.2
```

Related Commands

Command	Description
debug sbc log-level	Sets the debug logging level for logging to the cyclic buffer or to the system logger.
logging buffered	Logs messages to an internal buffer.
logging console	Logs messages to console connections.
logging host	Logs messages to a syslog server host.
logging monitor	Limits messages logged to the terminal lines (monitors) based on severity.
logging on	Enables logging of system messages.
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

debug sbc ips

To turn on inter-process signal (IPS) tracing, use the **debug sbc ips** command in privileged EXEC mode. To turn off IPS tracing, use the **no** form of this command.

debug sbc {*sbc-name*} **ips**

no debug sbc {*sbc-name*} **ips**

Syntax Description	<i>sbc-name</i> Name of the session border controller (SBC) service.
---------------------------	--

Command Default	Debugging is off.
------------------------	-------------------

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	Inter-process signal (IPS) tracing provides details of inter-component signals flowing between the internal components of the session border controller (SBC) process. IPS traces are stored internally in an in-memory buffer and can be dumped to the file system using the sbc dump-diagnostics command. IPS traces are in a binary format and are intended to be used by Cisco customer support engineers to diagnose problems.
-------------------------	--

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support personnel. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples	The following example turns on IPS tracing on the SBC service called “mySbc”:
-----------------	---

```
Router# debug sbc mySbc ips
```

Related Commands	Command	Description
	sbc dump-diagnostics	Dumps any in-memory diagnostics currently gathered by the SBC service to either the current default, or the specified file system.

debug sbc log-level

To set the debug logging level for logging to the cyclic buffer or to the system logger, use the **debug sbc log-level** command in privileged EXEC mode. To disable the debug logging level, use the **no** form of this command.

debug sbc {*sbc-name*} **log-level** {**buffer** | **console**} {*level*}

no debug sbc {*sbc-name*} **log-level** {**buffer** | **console**}

Syntax Description

<i>sbc-name</i>	Name of the session border controller (SBC) service.
buffer	Specifies logging to the cyclic buffer, which is an internal, in-memory, log buffer. The contents of the cyclic buffer can be written to a file system using the sbc dump-diagnostics command.

console	Sends logging to the system logger, which may or may not appear on the console, depending on how the system logger is configured.
level	<p>Logging level you set. Values are 0 through 100. A level of 0 gives all debug logging and a level of 100 gives no debug logging activity. The default logging level is 63.</p> <p>The following are the more commonly used logging level values:</p> <ul style="list-style-type: none"> • 90 Fatal errors—SBC failed to initialize or is terminating unexpectedly. • 80 Errors—SBC subcomponent failed to initialize or is terminating unexpectedly. This type of log is generally followed by a log level 90. • 70 Unexpected conditions—Various resource failures, leading to operations failing. Examples may be failure to set up call, failure to inject DTMF into flow, state replication failure, failure to open association with MGC, and H.248 association lost. • 63 Configuration errors—Configuration errors, particularly due to resource failures. Call setup failures due to configuration errors. This is the default logging level. • 60 Operational events—Configuration problems, such as bad configuration or configuration not replicating successfully. • 55 Call logs—Same as level 50. • 50 Auditable events—Waypoints in normal operation, for example, initial internal audit complete, catch-up replication complete, subcomponent initialization complete. Other auditable events may be Call setup failures, Unexpected or illegal media packets received, and Media events, such as media_up and media_down. • 40 Statistics—Various logs about problems with messages received from the MGC. • 30 Verbose operational events—Details of all H.248 messages sent and received. Details of any parse errors. • 20 Verbose statistics—Logs describing basic operations, such as messages between SBC components. • 10 Internal diagnostic logs—Similar to level 20. Internal events within the SBC which may be useful for debugging in the absence of IPS trace.

Command Default Debugging is off.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

In the **no** form of this command, you do not need to specify the logging level because the command sets the logging level to the default.

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support personnel. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

In the following example, setting the debug logging level to 90 logs fatal errors directly to the console:

```
Router# debug sbc mySbc log-level console 90
```

In the following example, setting the debug logging level to 0 writes all logs to the cyclic buffer:

```
Router# debug sbc mySbc log-level buffer 0
```

Related Commands

Command	Description
sbc dump-diagnostics	Dumps any in-memory diagnostics currently gathered by the SBC service to either the current default, or the specified file system.
logging buffered	Logs messages to an internal buffer.
logging console	Logs messages to console connections.
logging host	Logs messages to a syslog server host.
logging monitor	Limits messages logged to the terminal lines (monitors) based on severity.
logging on	Enables logging of system messages.
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.

debug sbc mpf

To turn on debugging messages in the DBE forwarding processor for both session border controller (SBC) services and low-level drivers, use the **debug sbc mpf** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sbc {*sbc-name*} **mpf** {**all** | **error** | **info** | **flow**}

no debug sbc {*sbc-name*} **mpf** {**all** | **error** | **info** | **flow**}

Syntax Description

<i>sbc-name</i>	Name of the session border controller (SBC) service.
all	Turns on all debugging messages in the DBE forwarding process, including error, information, and flow messages.
error	Turns on error debugging messages in the DBE forwarding process and provides debug information for any error conditions, such as failing to forward a media packet because there is no destination address for the flow, or failing to insert a DTMF telephone event due to an overflowed queue.
info	Turns on informational debugging messages in the DBE forwarding process and provides debug information on basic operations such as initialization or termination of the DBE forwarding process.
flow	Turns on flow debugging messages in the DBE forwarding process and provides debug information on each flow as it is allocated and freed, and on any significant events on the flow (such as media UP/DOWN).

Command Default

Debugging is off.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines



Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support personnel. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example shows the debug output from the **debug sbc mpf all** command and the SBC service called “global.” The type of debugging message is indicated in bold and is not part of the debug output.

```
Router# debug sbe global mpf all
```

Flow Debugging Messages

```
(Func: zismps_rcv_pmi_flowp_alloc) Flow pair allocated (flow_pair_index = 20).
(Func: zismps_send_pmi_flowp_events_ind) Flow pair events (flow_pair_index = 20)
```

```
Side A: 1 ( media_up)
Side B: 0 ().
(Func: zismps_send_pmi_flowp_events_ind) Flow pair events (flow_pair_index = 20)
```

```
Side A: 0 ()
Side B: 1 ( media_up).
(Func: zismps_rcv_pmi_flowp_delete) Flow pair deleted (flow_pair_index = 20).
(Func: zismps_free_flow_pair) Flow pair freed (flow_pair_index = 20).
```

Informational Debugging Messages

```
Func: zismpf_reset) Resetting media packet forwarder
(Func: zismps_rcv_pmi_deactivate) MPF stub deactivated.
```

```
(Func: zismps_rcv_pmi_init) MPF stub initialized.
```

Error Debugging Message

```
(Func: zismpp_divert_packet) Incoming DTMF queue full - packet dropped
```

Related Commands

Command	Description
show sbc dbe forwarder-stats	Displays the global list of statistics for the DBE forwarding process.

dtmf-duration

To configure the default duration of a dual-tone multifrequency (DTMF) event in milliseconds, use the **dtmf-duration** command in VDBE configuration mode. To reconfigure the default duration of a DTMF event in milliseconds, use the **no** form of this command.

dtmf-duration {*duration*}

no dtmf-duration

Syntax Description	<i>duration</i>	The default duration time of a DTMF event in milliseconds. The range is 0 to 1000.
---------------------------	-----------------	--

Command Default	The default is 200 ms if this command is not configured, or the no dtmf-duration command is issued.
------------------------	--

Command Modes	VDBE configuration (config-sbc-dbe-vdbe)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples	The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and configures the default duration of a DTMF event to be 250 milliseconds.
-----------------	---

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# dtmf-duration 250
Router(config-sbc-dbe-vdbe)# end
```

h248-association-timeout

To configure the data border element (DBE) to reset the H.248 association with the Media Gateway Controller (MGC) when the controller does not respond to any event notification, use the **h248-association-timeout** command in VDBE configuration mode. To configure the DBE to reset the H.248 association only when the controller fails to respond to the inactivity timer (it/ito) event, use the **no** form of this command. (This behavior is the default and standard H.248 protocol behavior.)

h248-association-timeout

no h248-association-timeout

Syntax Description

This command has no arguments or keywords.

Command Default

The default is **no h248-association-timeout**; only failure to notify the MGC of the it/ito event causes the H.248 association with the MGC to be reset. (This behavior is the standard H.248 protocol behavior.)

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example configures the DBE to reset the H.248 association with the MGC controller when the controller does not respond to any event notification:

```
Router (config)# sbc mySbc dbe
Router (config-sbc-dbe)# vdb
Router (config-sbc-dbe-vdbe)# h248-association-timeout
Router (config-sbc-dbe-vdbe)# end
```

The following example configures the DBE to reset the H.248 association only when the controller fails to respond to the inactivity timer (it/ito) event:

```
Router (config)# sbc mySbc dbe
Router (config-sbc-dbe)# vdb
Router (config-sbc-dbe-vdbe)# no h248-association-timeout
Router (config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
h248-event-storage	Enables H.248 event storage, which retains all H.248 events until the stream on which they occurred is deleted
h248-preserve-gates	Configures the DBE to preserve media terminations or contexts when there is a media timeout while the H.248 association with the controller is down.

h248-event-storage

To enable permanent storage of all H.248 events, use the **h248-event-storage** command in VDBE configuration mode. To disable permanent storage of H.248 events, where H.248 events are only retained until they are acknowledged by the media gateway controller (MGC), use the **no** form of the command.

h248-event-storage

no h248-event-storage

Syntax Description

This command has no arguments or keywords.

Command Default

The default is that H.248 events are only stored until they are acknowledged by the MGC. The default is **no h248-event-storage**.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

It is important to understand that H.248 event storage is always turned on. There are two modes of H.248 storage:

- Permanent storage of H.248 events, enabled by the **h248-event-storage** command.
In this mode, H.248 events are stored permanently. To reduce the memory required to store event information, the DBE only stores the most recent H.248 event of each type for each stream, except for dual-tone multifrequency (DTMF) events, which are always stored.
- Storage of H.248 events only until the events are acknowledged by the media gateway controller (MGC). This is enabled by the **no h248-event-storage** command and is the system default.
H.248 events other than those relating to a media timeout are deleted by the MGC after the MGC has acknowledged them. In this mode, the H.248 events relating to a media timeout are retained if the H.248 association fails.

Examples

The following example configures the data border element (DBE) to enable permanent H.248 event storage:

```
Router (config)# sbc mySbc dbe
Router (config-sbc-dbe)# vdb
Router (config-sbc-dbe-vdbe)# h248-event-storage
Router (config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
h248-association-timeout	Configures the DBE to reset the H.248 association with the MGC when the controller does not respond to any event notification.
h248-preserve-gates	Configures the DBE to preserve media terminations or contexts when there is a media timeout while the H.248 association with the controller is down.

h248-inactivity-duration

To define the duration of the provisioned inactivity timer, use the **h248-inactivity-duration** command in VDBE configuration mode. To reconfigure the duration of the provisioned inactivity timer to the default value (0 milliseconds), use the **no** form of this command.

h248-inactivity-duration *duration*

no h248-inactivity-duration

Syntax Description	<div> <div><i>duration</i></div> <div>Duration of the provisioned inactivity timer in multiples of 10 milliseconds. The range is 0 to 65,535.</div> <div>For example, if you specify a <i>duration</i> value of 10, the provisioned inactivity timer uses a duration interval of 100 milliseconds.</div> </div>				
Command Default	If the h248-inactivity-duration command is not specified, the default is 0 milliseconds, which indicates the timer is not in effect.				
Command Modes	VDBE configuration (config-sbc-dbe-vdbe)				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE Release 2.1</td><td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td></tr> </table>	Release	Modification	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				
Usage Guidelines	<p>The advantage of a provisioned inactivity timer is that the DBE can detect MGC failure whether or not the MGC has subscribed to the inactivity timer event.</p> <p>The MGC can still subscribe to the inactivity timer event, and situations can occur when a different duration interval is specified for the MGC than that specified for the DBE in the provisioned inactivity timer. When two conflicting values are specified, the MGC subscription duration value overrides the provisioned duration value. However, if the MGC cancels its subscription, or the association fails, the provisioned duration value goes back into effect. The provisioned inactivity timer is started when a successful response is received to the initial ServiceChange request to the MGC.</p>				
Examples	<p>The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and configures the DBE to use a duration of 100 milliseconds for the provisioned inactivity timer:</p> <pre> Router(config)# sbc mySbc dbe Router(config-sbc-dbe)# vdbe Router(config-sbc-dbe-vdbe)# h248-inactivity-duration 10 Router(config-sbc-dbe-vdbe)# end </pre>				

h248-media-alert-event

To enable the Middlebox Pinhole Timer Expired event when the DBE detects media loss, use the **h248-media-alert-event** command in VDBE configuration mode. To disable the Middlebox Pinhole Timer Expired event, use the **no** form of this command.

h248-media-alert-event

no h248-media-alert-event

Syntax Description

This command has no arguments or keywords.

Command Default

The default behavior is that this event is generated.

Command Modes

VDBE configuration mode (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The media gateway controller (MGC) may additionally request a Network Package Quality Alert event be generated, independent of the setting of this feature.

Examples

The following example enables generation of the Middlebox Pinhole Timer Expired event on detection of lost media:

```
(config)# sbc mySbc dbe
(config-sbc-dbe)# vdb
(config-sbc-dbe-vdbe)# h248-media-alert-event
(config-sbc-dbe-vdbe)# end
```

The following example disables generation of the Middlebox Pinhole Timer Expired event on detection of lost media:

```
(config)# sbc mySbc dbe
(config-sbc-dbe)# vdb
(config-sbc-dbe-vdbe)# no h248-media-alert-event
(config-sbc-dbe-vdbe)# end
```

h248-napt-package

To define which H.248 package, either the IP NAPT Traversal (ipnapt) package or the NAT Traversal (ntr) package, the DBE uses for signaling Network Address Translation (NAT) features, use the **h248-napt-package** command in VDBE configuration mode. To reconfigure the DBE to use the default NTR package, use the **no** form of this command.

h248-napt-package [*napt* | *ntr*]

no h248-napt-package

Syntax Description	<i>napt</i>	Uses the IP NAPT Traversal (ipnapt) package, defined in the H.248.37 protocol.
	<i>ntr</i>	Uses the NAT Traversal (ntr) package, defined in the ETSI TS 102 333 protocol.

Command Default If the h248-napt-package command is not specified, the ntr value is used.

Command Modes VDBE configuration mode (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines Terminations may not be programmed using both the ntr and ipnapt packages. The IP NAPT Traversal (ipnapt) package, defined in H.248.37. IP NAPT is an alternative method to the existing support of the NAT Traversal (ntr) package defined in ETSI TS 102 333. IP NAPT defines two signals, latch and relatch, to control how the DBE learns remote addresses for endpoints behind a NAT.

Examples The following example creates a data border element (DBE) service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and configures the DBE to use the IP NAPT Traversal package:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# h248-napt-package napt
Router(config-sbc-dbe-vdbe)# end
```

Related Commands	Command	Description
	h248-version	Defines the version of the H.248 protocol that the DBE uses when it forms associations with an H.248 controller.

h248-preserve-gates

To configure the data border element (DBE) to preserve media terminations or contexts when all streams within the context are in media-down state while the H.248 association with the controller is down, use the **h248-preserve-gates** command in VDBE configuration mode. To allow the DBE to delete contexts when all streams within the context are in media-down state and there is no current H.248 association with a media gateway controller (MGC), use the **no** form of this command.

h248-preserve-gates

no h248-preserve-gates

Syntax Description

This command has no arguments or keywords.

Command Default

The default is **no h248-preserve-gates**; the DBE can delete contexts when all streams within the context are in media-down state and there is no current H.248 association with the MGC. (This behavior is the standard H.248 protocol behavior.)

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

If this command is not enabled, silent gate deletion can occur. The DBE can delete contexts when all streams within the context are in media-down state, that is, when streams have no media flowing for the media-timeout duration, and there is no current H.248 association with the MGC.

Examples

The following example configures the DBE to preserve media terminations or contexts when all streams within the context are in media-down state while the H.248 association with the controller is down:

```
Router (config)# sbc mySbc dbe
Router (config-sbc-dbe)# vdb
Router (config-sbc-dbe-vdbe)# h248-preserve-gates
Router (config-sbc-dbe-vdbe)# end
```

The following example configures the DBE to allow the DBE to delete contexts when all streams within the context are in media-down state and there is no current H.248 association with an MGC:

```
Router (config)# sbc mySbc dbe
Router (config-sbc-dbe)# vdb
Router (config-sbc-dbe-vdbe)# no h248-preserve-gates
Router (config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
h248-association-timeout	Configures the DBE to reset the H.248 association with the MGC when the controller does not respond to any event notification.
h248-event-storage	Enables H.248 event storage, which retains all H.248 events until the stream on which they occurred is deleted.

h248-profile

To configure a Virtual Data Border Element (VDBE) H.248 profile name to interoperate with the data border element (DBE), use the **h248-profile** command in the vDBE configuration mode. To return to the default value, use the **no** form of this command.

h248-profile { **etsi-bgf** | **gate-ctrl** } **version** *version-number*

no h248-profile

Syntax Description

etsi-bgf	Configures the Ia profile for ETSI_BGF.
gate-ctrl	Configures the Cisco profile for SBC_GateControl.
version	Configures the profile version.
<i>version-number</i>	The profile's version number. The default version number for etsi-bgf is 2 and gate-ctrl is 3.

Command Default

Default value is gatecontrol.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.1S	The version keyword and the <i>version-number</i> argument were added to configure the profile version.

Usage Guidelines

To use this command, you must be in a user group that is associated with a task group that includes the proper task IDs. To use this command, you must also be in the correct configuration mode. The Examples section that follows shows the hierarchy of the modes required to run the command.

After the DBE is configured to use the H.248 profile name, the applicable profile name is advertised with the Service Change messages.

Examples

The following example shows how to configure the vDBE H.248 Ia profile to interoperate with the DBE:

```
Router# configure terminal
Router(config-sbc)# sbc mysbc db
Router(config-sbc-dbe)# vdb
Router(config-sbc-dbe-vdbe)# h248-profile etsi-bgf version 2
```

Related Commands

Command	Description
h248-version	Defines the version of an H.248 protocol that the DBE uses when it forms associations with an H.248 controller.
bandwidth-fields mandatory	Sets the bandwidth description of SDP as mandatory.
vdbe	Enters VDBE configuration mode.

h248-version

To define the version of the H.248 protocol that the DBE uses when it forms associations with an H.248 controller, use the **h248-version** command in VDBE configuration mode. To reconfigure to the default version, use the **no** form of this command.

h248-version *version*

no h248-version

Syntax Description

<i>version</i>	Specifies the H.248 protocol version that the DBE uses when it forms associations with an H.248 controller. The DBE can accept H.248.1 version 2 or version 3.
----------------	--

Command Default

If the **h248-version** command is not specified, the default is H.248.1 version 2.

Command Modes

VDBE configuration mode (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command configures the DBE to support H.248.1v3, thus allowing the DBE to interoperate with an SBE or media gateway controller (MGC) which requires H.248.1 version 3. The DBE can accept H.248.1 version 2 or version 3.

The DBE rejects attempts to negotiate with the MGC to a lower version once the DBE is configured to support version 3.

Examples

The following example creates a data border element (DBE) service on an SBC called "mySbc," enters into SBC-DBE configuration and VDBE configuration modes, and configures the virtual data border element (vDBE) to use H.248.1 version 3:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdb
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
h248-napt-package	Defines which H.248 package, either IP NAT Traversal package (ipnapt) or NAT Traversal package (ntr), the DBE uses for signaling Network Address Translation (NAT) features.

inbound

To configure inbound call packets to use a specific Security Parameters Index (SPI) to identify the security association to which an incoming packet is bound when the Interim Authentication Header (IAH) is enabled, use the **inbound** command in IAH Key configuration mode. To remove the configuration, use the **no** form of this command.

inbound *spi hex-key*

no inbound *spi hex-key*

Syntax Description	inbound	Specifies the inbound Security Parameters Index (SPI).
	<i>spi</i>	The SPI is an arbitrary 32-bit value that the MGC uses to identify the Security Association to which an incoming or outgoing packet is bound and specifies which hashing key to use. The spi argument has a range of 256 through 2147483647.
	<i>hex-key</i>	The hex-key argument is a string of a maximum of 64 characters. It can be a text string, such as myInboundKey45, or be in hexadecimal format, such as abcdef01234456.

Command Default	None
-----------------	------

Command Modes	IAH Key configuration mode (config-sbc-dbe-vdbe-h248-iah)
---------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	<p>The inbound command is used in conjunction with the outbound and transport (session border controller) commands. The three commands are used together to enable Interim Authentication Header (IAH) authentication of inbound and outbound call packets. If you specify a hashing scheme (ah-md5-hmac or ah-sha-hmac type of authentication), using the transport (session border controller) command, you need to configure incoming and outgoing call packets using both inbound and outbound commands. The inbound and outbound commands are used to specify the Security Parameters Index (SPI) and hex-key.</p>
------------------	---

Both inbound and outbound SPI need to be configured. If authentication is set to MD5 or SHA hashing scheme and only the inbound or outbound SPI key or neither inbound or outbound SPI key is configured, the authentication reverts back to zero authentication and the DBE issues a warning message “Both inbound and outbound keys must be configured to enable authentication.” In this event, the DBE sets all fields in the IAH header to zeroes and accepts any IAH without authentication.

Examples

The following example shows you how to configure the IAH to use the HMAC-SHA hashing scheme, set the inbound Security Parameters Index (SPI) to 300 and the outbound SPI to 400, and hash key to “myInboundKey45” and “myOutboundKey89” respectively:

```
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# h248-napt-package napt
Router(config-sbc-dbe-vdbe)# local-port 2970
Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 200.50.1.40
Router(config-sbc-dbe-vdbe)# controller h248 2
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 200.50.1.254
Router(config-sbc-dbe-vdbe-h248)# remote-port 2970
Router(config-sbc-dbe-vdbe-h248)# transport tcp interim-auth-header ah-sha-hmac
Router(config-sbc-dbe-vdbe-h248-iah)# inbound 300 myInboundKey45
Router(config-sbc-dbe-vdbe-h248-iah)# outbound 400 myOutboundKey89
Router(config-sbc-dbe-vdbe-h248)# exit
Router(config-sbc-dbe-vdbe)# attach-controllers
```

Related Commands

Command	Description
outbound	Configures outbound call packets to use a specific Security Parameters Index (SPI) to identify the security association to which an outgoing packet is bound when the Interim Authentication Header (IAH) is enabled.
transport (session border controller)	Configures the data border element (DBE) to use either UDP or TCP for H.248 control signaling with the specified H.248 controller and to configure the Interim Authentication Header (IAH) to authenticate and check the integrity of packets.

interface sbc

To create a session border controller (SBC) interface and enter interface configuration mode, use the **interface sbc** command in global configuration mode. To delete the SBC interface, use the **no** form of this command.

interface sbc {*interface-number*}

no interface sbc {*interface-number*}

Syntax Description	<i>interface-number</i>	The SBC interface number. The command creates an index of the SBC interface.
Command Default	No default behavior or values are available.	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Usage Guidelines	This command creates an SBC logical interface and enters into interface configuration mode, the submode of the SBC interface, where you can perform configuration on the SBC interface, such as configuring IP addresses.	
Examples	The following example creates SBC interface 10 and enters into interface configuration mode: Router(config)# interface sbc 10 Router(config-if)#	
Related Commands	Command	Description
	ip address	Sets a primary or secondary IP address for a Cisco interface.

ip address (session border controller)

To configure the IPv4 address and the subnet mask on a session border controller (SBC) interface, use the **ip address** command in interface configuration mode. To delete the IPv4 address on the SBC interface, use the **no** form of this command.

ip address {IPv4 address} {IPv4 subnet mask}

no ip address {IPv4 address} {IPv4 subnet mask}

Syntax Description

<i>IPv4 address</i>	IPv4 address on the SBC interface.
<i>IPv4 subnet mask</i>	IPv4 subnet mask on the SBC interface.

Command Default

No IPv4 addresses are defined for any SBC interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **ip address** command to configure the IPv4 address and the subnet mask on an SBC interface first before using the **media-address ipv4** command or the **media-address pool ipv4** command.

The subnet mask on the SBC interface is used by SBC configuration in the **media-address ipv4** command or the **media-address pool ipv4** command.

To avoid SBC configuration errors, all corresponding DBE IPv4 media addresses set by the **media-address ipv4** command and IPv4 media address pools set by the **media-address pool ipv4** command must be removed from the SBC configuration before removing the IPv4 address from the SBC interface.



Note

Configure the IPv4 addresses first, then configure the media addresses with the **media-address ipv4** command. When the media addresses have been configured, the media addresses will be automatically generated on an SBC interface. It is highly recommended that you do not change or remove the automatically configured media addresses.

Examples

The following example creates an IPv4 address 1.1.1.1 with subnet mask 255.255.0.0 on interface SBC "3":

```
Router(config)# interface sbc 3
Router(config-if)# ip address 1.1.1.1 255.255.0.0
Router(config-if)# end
```

Related Commands	Command	Description
	media-address ipv4	Adds an IPv4 address to the set of addresses that can be used by the data border element (DBE) as a local media address.
	media-address pool ipv4	Creates a pool of sequential IPv4 media addresses that can be used by the data border element (DBE) as local media addresses.
	ipv6 address (session border controller)	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on a session border controller (SBC) interface.
	ip address	Sets a primary or secondary IP address for a Cisco IOS interface.

ipv6 address (session border controller)

To configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an SBC interface, use the **ipv6 address (session border controller)** command in interface configuration mode. To remove the address and prefix from the SBC interface, use the **no** form of this command.

ipv6 address {IPv6 address/prefix-length}

no ipv6 address {IPv6 address/prefix-length}

Syntax Description

<i>IPv6 address</i>	IPv6 address on the SBC interface.
<i>/prefix-length</i>	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No IPv6 addresses are defined for any SBC interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Configure the IPv6 prefix first before you use the **media-address ipv6** or **media-address pool ipv6** commands.

To avoid SBC configuration errors, all corresponding DBE IPv6 media addresses set by the **media-address ipv6** command and IPv6 media address pools set by the **media-address pool ipv6** command must be removed from the SBC configuration before removing the IPv6 address from the SBC interface.



Note

Configure the IPv6 addresses first, then configure the media addresses with the **media-address ipv6** command. When the media addresses have been configured, the media addresses will be automatically generated on an SBC interface. It is highly recommended that you do not change or remove the automatically configured media addresses.

Examples

The following example creates an SBC interface called “3,” enters into interface configuration mode, and creates an IPv6 prefix 1::1/64 on SBC interface “3”:

```
Router(config)# interface sbc 3
Router(config-if)# ipv6 address 1::1/64
Router(config-if)# end
```

Related Commands	Command	Description
	media-address ipv6	Adds an IPv6 address to the set of addresses that can be used by the data border element (DBE) as a local media address.
	media-address pool ipv6	Creates a pool of sequential IPv6 media addresses that can be used by the data border element (DBE) as local media addresses.
	ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on a non-SBC interface.
	ip address (session border controller)	Sets the IPv4 address and the subnet mask on a session border controller (SBC) interface.

local-port

To configure a data border element (DBE) to use a specific local port when connecting to the default media gateway controller (MGC), use the **local-port** command in VDBE configuration mode. To disable this configuration, use the **no** form of this command.

local-port *{port-num}*

no local-port

Syntax Description

<i>port-num</i>	Number of the local port that the DBE uses. Port numbers range from 1 to 9999.
-----------------	--

Command Default

The default is to use any available local port.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The local port cannot be modified once any controller has been configured on the virtual data border element (vDBE). You must delete the controller before you can modify or configure the local port.

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and configures the DBE to use the local port number 5090:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdb
Router(config-sbc-dbe-vdbe)# local-port 5090
Router(config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
sbc dbe	Creates the data border element (DBE) service on a session border controller (SBC) and enters into SBC-DBE configuration mode.

local-remote-desc always

To configure the data border element (DBE) so that it always returns the local and remote descriptors in an H.248 Reply to the signaling border element (SBE), use the **local-remote-desc always** command in VDBE configuration mode. To reset to the default behavior, use the **no** form of this command.

local-remote-desc always

no local-remote-desc always

Syntax Description

This command has no arguments or keywords.

Command Default

The default behavior is that the DBE only returns a local or remote descriptor in an H.248 Reply when the descriptor is either under-specified or over-specified in the associated request.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command configures the DBE to always return the local and remote descriptors in an H.248 Reply if the descriptors are present in the H.248 request. This command enhances H.248 interoperability with the SBE.

The default behavior is that the DBE only returns a local or remote descriptor in an H.248 Reply when the descriptor is either under-specified or over-specified in the associated request. Under-specified means the SBE includes a CHOOSE (\$) wildcard in the Request. Over-specified means the SBE includes multiple codecs in the Request and allows the DBE to choose one codec from the list.

Examples

The following example configures the DBE to always include the local and remote descriptor in an H.248 Reply if those descriptors are present in the H.248 request:

```
Router# configure terminal
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdb global
Router(config-sbc-dbe-vdbe)# local-remote-desc always
```

The following example uses the **no** form of the command to configure the DBE to not include local and remote descriptor in an H.248 Reply except under the condition that the descriptors are returned only if they were under-specified or over-specified on the H.248 request:

```
Router# configure terminal
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdb global
Router(config-sbc-dbe-vdbe)# no local-remote-desc always
```

local-remote-desc always

Related Commands

Command	Description
sbcdbe	Creates the DBE service on a SBC and enters into the SBC-DBE configuration mode.
vdbe	Configures a VDBE and enters the VDBE configuration mode.

location-id

To configure the location ID for a data border element (DBE) service of the session border controller (SBC), use the **location-id** command in SBC-DBE configuration mode. To set the location ID to the default, use the **no** form of this command.

location-id {*location-id*}

no location-id

Syntax Description	<i>location-id</i> The location ID of the DBE. The location ID range is from 0 to 65535.	
Command Default	The default is 0xFFFFFFFF (-1) if the command is not configured, or the no location-id command is issued.	
Command Modes	SBC-DBE configuration (config-sbc-dbe)	
Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Usage Guidelines	<p>The no form of the command does not take an argument and sets the location ID to the default, which is 0xFFFFFFFF (-1).</p> <p>A location ID is configured on each DBE. The SBE may associate endpoints with a particular location ID and then use the location IDs to route calls between different DBEs.</p> <p>Use the sbc dbe command to enter into SBC-DBE configuration mode prior to entering the location-id command.</p>	
Examples	<p>The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration mode, and sets the location ID for a DBE to be 1:</p> <pre>Router(config)# sbc mySbc dbe Router(config-sbc-dbe)# location-id 1 Router(config-sbc-dbe)# end</pre>	
Related Commands	Command	Description
	sbc dbe	Creates the data border element (DBE) service on a session border controller (SBC) and enters into SBC-DBE configuration mode.

logging filter control protocol

To set the H.248 protocol message filter to display only the H.248 text from the console logs on the Data Border Element (DBE), use the **logging filter control protocol** command in VDBE configuration mode. To disable the H.248 protocol message filter, use the **no** form of this command.

logging filter control protocol

no logging filter control protocol

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values are available..

Command Modes

VDBE configuration mode (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR1000 Series Aggregation Services Routers.

Usage Guidelines

Use this command to set the H.248 protocol message filter for console logging to display only the H.248 text without any internal message logs.



Note

If you enable the logging filter control protocol using both a **debug** command and the **logging filter control protocol** command, the logging filter control protocol must be disabled by both commands before the filter is disabled.

Examples

The following example shows sample DBE configuration steps where the H.248 protocol message filter is enabled:

```
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdb global
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# h248-napt-package napt
Router(config-sbc-dbe-vdbe)# local-port 2971
Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 200.50.1.41
Router(config-sbc-dbe-vdbe)# logging filter control protocol
Router(config-sbc-dbe-vdbe)# controller h248 2
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 200.50.1.254
Router(config-sbc-dbe-vdbe-h248)# remote-port 2971
Router(config-sbc-dbe-vdbe-h248)# exit
Router(config-sbc-dbe-vdbe)# attach-controllers
Router(config-sbc-dbe-vdbe)# end
```

```
*Dec 20 00:19:33.090: %SYS-5-CONFIG_I: Configured from console by console
*Dec 20 00:19:36.951: %SBC-7-MSG-2E01-0074-67C592-0537: SBC/MG-CTRL:
Megaco message received.
Remote address = 200.50.1.254
Message text    =
AU=0x12345678:0x90ABCDEF:0x000000000000000000000000123456
!/3 [200.50.1.40]:2971 T=6 {
C = $ {
A = abc/sip4/gn/0/1/0/1/ac/$ {
M {
TS { SI = IV },
ST = 1 {
O { MO = SR
},
R {
v=0
c=IN IP4 3.0.0.3
m=application 5000 udp 0
},
L {
v=0
c=IN IP4 $
m=application $ udp 0
}
}
},
A = abc/sip4/gn/0/1/0/1/bb/$ {
M {
TS { SI = IV },
ST = 1 {
O { MO = SR,
ds/dscp = 1D),
R {
v=0
c=IN IP4 3.0.0.3
m=application 5000 udp 0
}
}
}
*Dec 20 00:19:36.986: %SBC-7-MSG-2E01-0073-1C5642-0992: SBC/MG-CTRL:
Megaco message sent.
Remote address = 200.50.1.254
Message text    =
!/3 [200.50.1.40]:2971
P=6{
C=1{
A=abc/sip4/gn/0/1/0/1/ac/1{
M{
ST=1{
L{
v=0
c=IN IP4 202.50.2.1
m=application 10000 udp 0
}}}},
A=abc/sip4/gn/0/1/0/1/bb/2{
M{
ST=1{
L{
v=0
c=IN IP4 202.50.2.1
m=application 10001 udp 0
}}}}}}
```

Related Commands

Command	Description
logging level	Sets the console logging level used when logging H.248 and other messages to the Data Border Element (DBE).
debug sbc log-level	Sets the debug logging level for logging to the cyclic buffer or to the system logger/console.
debug sbc filter	Enables logging based on various types of filters.
debug sbc ips	Enables inter-process signal (IPS) tracing.
debug sbc mpf	Enables debugging messages in the DBE forwarding processor for both Session Border Controller services and low-level drivers.

logging level

To enable console logging for non-default logging and set the logging level used for logging H.248 and other messages to the Data Border Element (DBE), use the **logging level** command in VDBE configuration mode. To disable the console logging, use the **no** form of this command.

logging level [*value*]

no logging level [*value*]

Syntax Description

<i>value</i>	<p>This is the specified severity logging level. Accepted values are 0 through 100.</p> <p>The default logging level is 63 if you do not specify a logging level. Note that logging level 30 generates logs showing H.248 requests and responses. The following are the more commonly used logging level values:</p> <ul style="list-style-type: none"> 90 Fatal errors—SBC failed to initialize or is terminating unexpectedly. 80 Errors—SBC subcomponent failed to initialize or is terminating unexpectedly. This type of log is generally followed by a log level 90. 70 Unexpected conditions—Various resource failures, leading to operations failing. Examples may be failure to set up call, failure to inject DTMF into flow, state replication failure, failure to open association with MGC, and H.248 association lost. 63 Configuration errors—Configuration errors, particularly due to resource failures. Call setup failures due to configuration errors. This is the default logging level. 60 Operational events—Configuration problems, such as bad configuration or configuration not replicating successfully. 55 Call logs—Same as level 50. 50 Auditable events—Waypoints in normal operation, for example, initial internal audit complete, catch-up replication complete, subcomponent initialization complete. Other auditable events may be Call setup failures, Unexpected or illegal media packets received, and Media events, such as media_up and media_down. 40 Statistics—Various logs about problems with messages received from the MGC. 30 Verbose operational events—Details of all H.248 messages sent and received. Details of any parse errors. 20 Verbose statistics—Logs describing basic operations, such as messages between SBC components. 10 Internal diagnostic logs—Similar to level 20. Internal events within the SBC which may be useful for debugging in the absence of IPS trace.
--------------	---

Command Default

Logging level 63 is on by default if you do not specify a logging level.

Command Modes

VDBE configuration mode (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR1000 Series Aggregation Services Routers.

Usage Guidelines

This command sends messages to a logging process, which controls the distribution of logging messages to the syslog server and the console. This command sets the severity logging level on the DBE and limits logging messages displayed on the console to messages for that specified level and above. For example a specified logging level of 30 would display log messages from logging levels 30, 40, 50, 60, 70, 80, and 90.

A logging level of 30 generates logs showing H.248 requests and responses. The lower the log level, the more syslog bandwidth is taken up.

Note that some messages may be displayed on the standby Route Processor (RP) because some of the components remain in the active stage on the standby RP and may produce those messages.

Session Border Controller (SBC) debug commands that set the logging level and the H.248 protocol message filter, such as **debug sbc log-level** and **debug sbc filter**, can be enabled at the same time.

The **logging level** command works with SBC and Cisco IOS debug commands as follows:

- If logging and logging level are enabled by the **logging level** command, it can only be disabled by the **logging level** command. The **undebg all** and **no debug sbc log-level** commands have no effect.
- If logging and logging level are enabled by a **debug** command, it can be disabled by the **undebg all** and **no debug sbc log-level** command.
- If two different logging levels are set by both a **debug** command and the **logging level** command, the lower logging level is applied.
- If the same level is set using both the **logging level** command and a **debug** command—to turn off logging for that level, you must disable logging using both the **logging level** command and the **debug** command.

Examples

The following example shows sample DBE configuration steps where logging level 30 is set:

```
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdb global
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# h248-napt-package napt
Router(config-sbc-dbe-vdbe)# local-port 2971
Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 200.50.1.41
Router(config-sbc-dbe-vdbe)# logging level 30
Router(config-sbc-dbe-vdbe)# controller h248 2
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 200.50.1.254
Router(config-sbc-dbe-vdbe-h248)# remote-port 2971
Router(config-sbc-dbe-vdbe-h248)# exit
Router(config-sbc-dbe-vdbe)# attach-controllers
Router(config-sbc-dbe-vdbe)# end
```


The following shows sample log output produced on an ADD request with logging level 30 set:

```
*Sep 10 06:38:39.039: %SBC-7-MSG-2E01-0092: SBC/MG-CTRL: (gctarecv.c
1397) Application has completed processing a transaction asynchronously
Transaction ID          = 3
Transaction type        = 0X01

*Sep 10 06:38:49.539: %SBC-7-MSG-2E01-0050: SBC/MG-CTRL: (gctphash.c
701) A hash table has been resized.
The previous size of the hash table was 1024 entries.
The new size of the hash table is 512 entries.
```

The following example shows log output for a single H.248 ADD request to the DBE from the MGC, with the logging filter control protocol enabled:

```
*Aug 13 06:20:02.519: %SBC-7-MSG-2E01-0074: SBC/MG-CTRL:
Megaco message received.
Remote address = 200.50.1.254
Message text =
AU=0x12345678:0x90ABCDEF:0x0000000000000000000000000000000000123456
!/3 [200.50.1.40]:2970 T=3 {
C = $ {
A = abc/sip4/gn/0/1/0/1/ac/$ {
M {
TS { SI = IV },
ST = 1 {
O { MO = SR
},
R {
v=0
c=IN IP4 3.0.0.3
m=application 5000 udp 0
},
L {
v=0
c=IN IP4 $
m=application $ udp 0
}
}
},
A = abc/sip4/gn/0/1/0/1/bb/$ {
M { TS { SI = IV },
ST = 1 {
O { MO = SR,
ds/dscp = 1D},
R {
v=0
c=IN IP4 3.0.0.3
```

Related Commands

Command	Description
logging filter control protocol	Sets the H.248 protocol message filter to display only the H.248 text from the console logs.
debug sbc log-level	Sets the debug logging level for logging to the cyclic buffer or to the system logger/console.
debug sbc filter	Enables logging based on various types of filters.

Command	Description
debug sbc ips	Enables inter-process signal (IPS) tracing.
debug sbc mpf	Enables debugging messages in the DBE forwarding processor for both Session Border Controller services and low-level drivers.

media-address ipv4

To add an IPv4 address to the set of addresses that can be used by the data border element (DBE) as a local media address, use the **media-address ipv4** command in SBC-DBE configuration mode. To remove an IPv4 address from the set of local media addresses, use the **no** form of this command.

media-address ipv4 {*A.B.C.D*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**dbe** | **mgc**}]

no media-address ipv4 {*A.B.C.D*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**dbe** | **mgc**}]

Syntax Description	<i>A.B.C.D</i> Local IP address on a session border controller (SBC) interface, which can be used for media arriving on the DBE.
nat-mode twice-nat	(Optional) Allows local addresses to be reserved for Twice-NAT pinholes.
vrf <i>vrf-name</i>	(Optional) Specifies that the IP address is associated with a specific VPN routing and forwarding (VRF) instance. If the VRF is not specified, the address is assumed to be an address on the global VPN.
managed-by	(Optional) Specifies whether the DBE or the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.
dbe	(Optional) Specifies that only the DBE is allowed to select these addresses as local addresses for flows.
mgc	(Optional) Specifies that only the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.

Command Default No default behavior or values are available.

Command Modes SBC-DBE configuration (config-sbc-dbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	The nat-mode twice-nat keyword was introduced.

Usage Guidelines

Use the **media-address ipv4** command to configure a local media address for traffic arriving on the DBE for each IP address that you specified under the SBC virtual interface with the **ip address** command.

Once you have configured a local media address, the media address cannot be modified while the DBE service is active. Deactivate the DBE with the **no activate** command first.

The media address is a pool of IP addresses on the DBE for media relay functionality. A pool of addresses is defined for the global VPN to which the DBE is attached. All vDBEs within the DBE draw media addresses from this pool.

Examples

The following example shows that IPv4 address 10.0.1.1, configured on an SBC interface, is the local address used for media traffic arriving on the DBE and it is reserved for Twice-NAT pinholes:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv4 10.0.1.1 managed-by mgc nat-mode twice-nat
Router(config-sbc-dbe-media-address)# end
```

The following example shows that IP address 10.0.1.1 (which is an address configured on an SBC interface) is used for media traffic arriving on the DBE from the global VPN:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv4 10.0.1.1
Router(config-sbc-dbe-media-address)# end
```

The following example tries to delete the media address 1.1.1.1 before first deactivating the DBE, and receives an error message:

```
Router(config-sbc-dbe)# no media-address ipv4 1.1.1.1
SBC: Unable to delete a media address whilst the DBE is active.
SBC: Please deactivate the DBE and try again.
```

Related Commands

Command	Description
media-address pool ipv4	Creates a pool of sequential IPv4 media addresses that can be used by the data border element (DBE) as local media addresses.
ip address	Configures the IPv4 address and the subnet mask on an SBC interface
sbc dbe	Creates the data border element (DBE) service on a session border controller (SBC) and enters into SBC-DBE configuration mode.
activate	Initiates the data border element (DBE) service of the session border controller (SBC).

media-address ipv6

To add an IPv6 address to the set of addresses that can be used by the data border element (DBE) as a local media address, use the **media-address ipv6** command in SBC-DBE configuration mode. To remove an IPv6 address from the set of local media addresses, use the **no** form of this command.

media-address ipv6 {*ipv6-address*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**dbe** | **mgc**}]

no media-address ipv6 {*ipv6-address*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**dbe** | **mgc**}]

Syntax Description		
<i>ipv6-address</i>		Local IPv6 address on a session border controller (SBC) interface, which can be used for media arriving on the DBE. The IPv6 address is a member of the global VRF.
nat-mode twice-nat		(Optional) Allows local addresses to be reserved for Twice-NAT pinholes.
vrf <i>vrf-name</i>		(Optional) Specifies that the IP address is associated with a specific VPN routing and forwarding (VRF) instance. If the VRF is not specified, the address is assumed to be an address on the global VPN.
managed-by		(Optional) Specifies whether the DBE or media gateway controller (MGC) is allowed to select the IPv6 address as the local address for flows.
dbe		(Optional) Specifies that only the DBE is allowed to select this address as the local address for flows.
mgc		(Optional) Specifies that only the MGC is allowed to specify this address as the local address for flows.

Command Default The default is that the IPv6 address is a member of the global VRF, and only the DBE may select the IPv6 address as the local address for flows.

Command Modes SBC-DBE configuration (config-sbc-dbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	The nat-mode twice-nat keyword was introduced.

Usage Guidelines Use the **media-address ipv6** command to configure a local media address for traffic arriving on the DBE for each IP address that you specified under the SBC virtual interface with the **ipv6 address** command.

Use the **media-address ipv6** command to enter into SBC-DBE media address IPv6 configuration mode before using the **port-range (ipv6)** command.

After you have configured a local media address, the media address cannot be modified while the DBE service is active. Deactivate the DBE with the **no activate** command before modifying the **media-address ipv6** specification.

The media address is a pool of IP addresses on the DBE for media relay functionality. A pool of addresses is defined for the global VPN to which the DBE is attached. All virtual data border elements (vDBEs) within the DBE draw media addresses from this pool.

Examples

The following example configures IPv6 address 5::1:1 as the local address, reserved for Twice-NAT pinholes:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv6 5::1:1 managed-by mgc nat-mode twice-nat
Router(cfg-sbc-dbe-media-addr-ipv6)# exit
```

The following example configures IPv6 address 5::1:1:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv6 5::1:1
Router(cfg-sbc-dbe-media-addr-ipv6)# exit
```

The following example tries to delete the IPv6 media address 5::1:1 before first deactivating the DBE, and receives an error message:

```
Router(config-sbc-dbe)# no media-address ipv6 5::1:1
SBC: Unable to delete a media address whilst the DBE is active.
SBC: Please deactivate the DBE and try again.
```

Related Commands

Command	Description
media-address pool ipv6	Creates a pool of sequential IPv6 media addresses that can be used by the data border element (DBE) as local media addresses.
ipv6 address (session border controller)	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on a session border controller (SBC) interface.
media-address ipv4	Adds an IPv4 address to the set of addresses that can be used by the data border element (DBE) as a local media address.
media-address pool ipv4	Creates a pool of sequential IPv4 media addresses that can be used by the data border element (DBE) as local media addresses.
activate	Initiates the data border element (DBE) service of the session border controller (SBC).

media-address pool ipv4

To create a pool of sequential IPv4 media addresses that can be used by the data border element (DBE) as local media addresses, use the **media-address pool ipv4** command in SBC-DBE configuration mode. This pool of addresses is added to the set of local media addresses that can be used by DBE. To remove this pool of IPv4 addresses from the set of local media addresses, use the **no** form of this command.

media-address pool ipv4 {*A.B.C.D*} {*E.F.G.H*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**db**e | **mg**c}]

no media-address pool ipv4 {*A.B.C.D*} {*E.F.G.H*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**db**e | **mg**c}]

Syntax Description		
<i>A.B.C.D</i>		Starting IPv4 media address in a range of addresses. An IPv4 media address is a local IP address on a session border controller (SBE) interface that can be used for media arriving on the DBE.
<i>E.F.G.H</i>		Ending IPv4 media address in a range of addresses. The ending IPv4 address must be numerically greater than the starting address.
nat-mode twice-nat		(Optional) Allows local addresses to be reserved for Twice-NAT pinholes.
vrf <i>vrf-name</i>		(Optional) Specifies that the IP addresses are associated with a specific VPN routing and forwarding (VRF) instance. If the VRF instance is not specified, the address is assumed to be an address on the global VPN.
managed-by		(Optional) Specifies whether the DBE or the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.
db e		(Optional) Specifies that only the DBE is allowed to select these addresses as local addresses for flows.
mg c		(Optional) Specifies that only the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.

Command Default If a pool of IPv4 media addresses is specified, but the optional parameters are not specified, the following default values are used:

- Addresses in the pool are members of the global VRF.
- Only the DBE is allowed to select these addresses as local addresses for flows.

Command Modes SBC-DBE configuration (config-sbc-dbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	The nat-mode twice-nat keyword was introduced.

Usage Guidelines

The media address pool size is limited to 1024 IPv4 addresses. If more IPv4 addresses are required, we recommend you create multiple SBC interfaces and then configure the address pools from the subnets on those interfaces.

After you have configured a local media address, the media address cannot be modified while the DBE service is active. Deactivate the DBE with the **no activate** command before modifying the **media-address pool ipv4** specification.

A media address is one of a pool of IP addresses on the DBE that are used for media relay functionality. A pool of addresses is defined for the global VPN to which the DBE is attached. All virtual data border elements (vDBEs) within the DBE draw media addresses from this pool.

Examples

The following example adds IPv4 addresses from 10.0.2.1 to 10.0.2.10 to the media address pool as local addresses, reserved for Twice-NAT pinholes:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.1 10.0.2.10 nat-mode twice-nat
Router(config-sbc-dbe-media-address-pool)# exit
```

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration mode, and configures addresses from 10.0.2.1 to 10.0.2.10 in the global VRF:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.1 10.0.2.10
Router(config-sbc-dbe-media-address-pool)# exit
```

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration mode, and configures addresses from 10.0.2.20 to 10.0.2.25 in vpn3:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.20 10.0.2.25 vrf vpn3
Router(config-sbc-dbe-media-address-pool)# exit
```

The following example tries to delete the media address 10.0.2.1 before first deactivating the DBE and receives an error message:

```
Router(config-sbc-dbe)# no media-address ipv4 10.0.2.1
SBC: Unable to delete a media address whilst the DBE is active.
SBC: Please deactivate the DBE and try again.
```

Related Commands

Command	Description
activate	Initiates the data border element (DBE) service of the session border controller (SBC).
media-address ipv4	Adds an IPv4 address to the set of addresses that can be used by the data border element (DBE) as a local media address.

media-address pool ipv6

To create a pool of sequential IPv6 media addresses that can be used by the data border element (DBE) as local media addresses, use the **media-address pool ipv6** command in SBC-DBE configuration mode. This pool of addresses is added to the set of local media addresses that can be used by the DBE. To remove this pool of IPv6 addresses from the set of local media addresses, use the **no** form of this command.

media-address pool ipv6 {*start-ipv6-address*} {*end-ipv6-address*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**dbe** | **mgc**}]

no media-address pool ipv6 {*start-ipv6-address*} {*end-ipv6-address*} [**nat-mode twice-nat** | **vrf** *vrf-name* | **managed-by** {**dbe** | **mgc**}]

Syntax Description

<i>start-ipv6-address</i>	Starting IPv6 media address in a range of addresses. An IPv6 media address is a local IP address on a session border controller (SBE) interface that can be used for media arriving on the DBE.
<i>end-ipv6-address</i>	Ending IPv6 media address in a range of addresses. The ending IPv6 address must be numerically greater than the starting address.
nat-mode twice-nat	(Optional) Allows local addresses to be reserved for Twice-NAT pinholes.
vrf <i>vrf-name</i>	(Optional) Specifies that the IP addresses are associated with a specific VPN routing and forwarding (VRF) instance. If the VRF instance is not specified, the address is assumed to be an address on the global VPN.
managed-by	(Optional) Specifies whether the DBE or the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.
dbe	(Optional) Specifies that only the DBE is allowed to select these addresses as local addresses for flows.
mgc	(Optional) Specifies that only the media gateway controller (MGC) is allowed to select these addresses as local addresses for flows.

Command Default

If a pool or range of IPv6 media addresses is specified, but the optional parameters are not specified, the following default values are used:

- Addresses in the pool are members of the global VRF.
- Only the DBE is allowed to select these addresses as local addresses for flows.

Command Modes

SBC-DBE configuration (config-sbc-dbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	The nat-mode twice-nat keyword was introduced.

Usage Guidelines

Use the **media-address pool ipv6** command to enter into SBC-DBE media address pool IPv6 configuration mode before using the **port-range (ipv6)** command.

After you have configured a local media address, the media address cannot be modified while the DBE service is active. Deactivate the DBE with the **no activate** command before modifying the **media-address pool ipv6** specification.

A media address is one of a pool of IP addresses on the DBE that are used for media relay functionality. A pool of addresses is defined for the global VPN to which the DBE is attached. All virtual data border elements (vDBEs) within the DBE draw media addresses from this pool.

Examples

The following example adds IPv6 addresses from 5::1:1 to 5::1:10 to the media address pool as local addresses, reserved for Twice-NAT pinholes:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv6 5::1:1 5::1:10 nat-mode twice-nat
Router(cfg-sbc-dbe-media-addr-pl-ipv6)# exit
```

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration mode, and adds IPv6 addresses from 5::1:1 to 5::1:10 to the media address pool:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv6 5::1:1 5::1:10
Router(cfg-sbc-dbe-media-addr-pl-ipv6)# exit
```

The following example tries to delete IPv6 addresses from 5::1:1 to 5::1:10 in the media address pool before first deactivating the DBE, and receives an error message:

```
Router(config-sbc-dbe)# no media-address pool ipv6 5::1:1 5::1:10
SBC: Unable to delete a media address whilst the DBE is active.
SBC: Please deactivate the DBE and try again.
```

Related Commands

Command	Description
media-address ipv6	Adds an IPv6 address to the set of addresses that can be used by the data border element (DBE) as a local media address.
ipv6 address (session border controller)	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on a session border controller (SBC) interface.
activate	Initiates the data border element (DBE) service of the session border controller (SBC).
media-address ipv4	Adds an IPv4 address to the set of addresses that can be used by the data border element (DBE) as a local media address.
media-address pool ipv4	Creates a pool of sequential IPv4 media addresses that can be used by the data border element (DBE) as local media addresses.

media-timeout

To set the maximum time a data border element (DBE) waits after receiving the last media packet on a call and before cleaning up the call resources, use the **media-timeout** command in SBC-DBE configuration mode. To reset the **media-timeout** value to the default value of 30 seconds, use the **no** form of this command.

media-timeout {*timeout*} **first-packet**

no media-timeout

Syntax Description	<i>timeout</i>	Timeout value measured in seconds. The range is 0 to 65535.
	first-packet	The first-packet keyword instructs the DBE to wait until it receives the first SBC packet on a flow before starting the media timeout function.

Command Default	The default is 30 seconds if media timeout is not configured.
------------------------	--

Command Modes	SBC-DBE configuration (config-sbc-dbe)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	The first-packet keyword was added.

Usage Guidelines	<p>This command sets the maximum time the DBE waits after receiving the last media packet on a call before the DBE determines that the call has ceased and begins to clear up the call resources and to signal the signaling border element (SBE) to do the same. This command is used when the SBE is not able to clear up the calls itself. The normal method for clearing a call is for the SBE to explicitly signal the DBE.</p> <p>You can halt detection of the media timeout event with the first-packet keyword of the media-timeout command. The first-packet keyword instructs the DBE to wait until it has received the first packet since the call has been established before starting the media timeout timer to start counting the number of seconds for which it has not seen an SBC packet. By the DBE waiting, SBC packets can continue to be forwarded because there is no media timeout yet. After waiting for the first packet and counting the configured number of seconds, then the DBE generates an alert to the SBE.</p> <p>Use the sbc dbe command to enter into SBC-DBE configuration mode before using the media-timeout command.</p>
-------------------------	---

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration mode, and configures the DBE to wait 10 seconds after receiving the last media packet and before cleaning up the call resources:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-timeout 10
Router(config-sbc-dbe)# end
```

The following example shows that the **media-timeout** command is configured to instruct the DBE to wait until it receives the first SBC packet on the call before it starts to count 1000 seconds, after which the DBE generates a media timeout alert to the SBE.

```
Router(config)# sbc global dbe
Router(config-sbc-dbe)# media-timeout 1000 first-packet
Router(config-sbc-dbe)# end
```

Related Commands

Command	Description
sbc dbe	Creates the data border element (DBE) service on a session border controller (SBC) and enters into SBC-DBE configuration mode.

outbound

To configure outbound call packets to use a specific Security Parameters Index (SPI) to identify the security association to which an outgoing packet is bound when the Interim Authentication Header (IAH) is enabled, use the **outbound** command in IAH Key configuration mode. To remove the configuration, use the **no** form of this command.

outbound *spi hex-key*

no outbound *spi hex-key*

Syntax Description	outbound	Specifies the outbound Security Parameters Index (SPI).
	<i>spi</i>	The SPI is an arbitrary 32-bit value that the MGC uses to identify the Security Association to which an incoming or outgoing packet is bound and specifies which hashing key to use. The spi argument has a range of 256 through 2147483647.
	<i>hex-key</i>	The hex-key argument is a string of a maximum of 64 characters. It can be a text string, such as myOutboundKey89, or be in hexadecimal format, such as 012345678abcde.

Command Default	None
------------------------	------

Command Modes	IAH Key configuration mode (config-sbc-dbe-vdbe-h248-iah)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Release 2.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **outbound** command is used in conjunction with the **inbound** and **transport (session border controller)** commands. The three commands are used together to enable Interim Authentication Header (IAH) authentication of inbound and outbound call packets. If you specify a hashing scheme (**ah-md5-hmac** or **ah-sha-hmac** authentication) using the **transport (session border controller)** command, you need to configure incoming and outgoing call packets using both **inbound** and **outbound** commands. The **inbound** and **outbound** commands are used to specify the Security Parameters Index (SPI) and hex-key.

Both inbound and outbound SPI need to be configured. If authentication is set to MD5 or SHA hashing scheme and only the inbound or outbound SPI key or neither inbound or outbound SPI key is configured, the authentication reverts back to zero authentication and the DBE issues a warning message “Both inbound and outbound keys must be configured to enable authentication.” In this event, the DBE sets all fields in the IAH header to zeroes and accepts any IAH without authentication.

Examples

The following example shows you how to configure the IAH to use the HMAC-SHA hashing scheme, set the inbound Security Parameters Index (SPI) to 300 and the outbound SPI to 400, and hash key to “myInboundKey45” and “myOutboundKey89” respectively:

```
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# h248-napt-package napt
Router(config-sbc-dbe-vdbe)# local-port 2970
Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 200.50.1.40
Router(config-sbc-dbe-vdbe)# controller h248 2
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 200.50.1.254
Router(config-sbc-dbe-vdbe-h248)# remote-port 2970
Router(config-sbc-dbe-vdbe-h248)# transport tcp interim-auth-header ah-sha-hmac
Router(config-sbc-dbe-vdbe-h248-iah)# inbound 300 myInboundKey45
Router(config-sbc-dbe-vdbe-h248-iah)# outbound 400 myOutboundKey89
Router(config-sbc-dbe-vdbe-h248)# exit
Router(config-sbc-dbe-vdbe)# attach-controllers
```

Related Commands

Command	Description
inbound	Configures inbound call packets to use a specific Security Parameters Index (SPI) to identify the security association to which an incoming packet is bound when the Interim Authentication Header (IAH) is enabled.
transport (session border controller)	Configures the data border element (DBE) to use either UDP or TCP for H.248 control signaling with the specified H.248 controller and to configure the Interim Authentication Header (IAH) to authenticate and check the integrity of packets.

overload-time-threshold

To configure the threshold for media gateway (MG) overload control detection, use the **overload-time-threshold** command in SBC-DBE configuration mode. To reset the threshold value to its default value of 100 milliseconds, use the **no** form of this command.

overload-time-threshold {*time*}

no overload-time-threshold

Syntax Description	<i>time</i>	The time threshold in milliseconds. The possible values are 0 to 4026531839.
---------------------------	-------------	--

Command Default	If a time threshold value is not configured, the default value is 100 milliseconds.
------------------------	---

Command Modes	SBC-DBE configuration (config-sbc-dbe)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	<p>The overload-time threshold defines the maximum delay allowed by a session border controller (SBC) that has subscribed to overload control events for the data border element (DBE) to add a new flow.</p> <p>If the threshold is exceeded, the DBE generates an overload event notification.</p> <p>If an SBC has subscribed for overload control events, the data border element (DBE) sends an overload event notification to the signaling border element (SBE) for every request to add a new flow whose execution takes longer than this threshold.</p>
-------------------------	--

Examples	<p>The following example creates a DBE service on an SBC called “mySbc,” and configures the overload control detection threshold to be 400 milliseconds. If an SBC has subscribed for overload control events, then the DBE will send an event notification every time a request to add a new flow takes longer than 400 milliseconds to process:</p>
-----------------	---

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# overload-time-threshold 400
Router(config-sbc-dbe)# end
```

package

To configure the data border element (DBE) to interoperate with the media gateway controller (MGC) using the Enhanced Root (eroot) package, use the **package** command in VDBE configuration mode. The eroot package is a proprietary package for the transport of the location ID and Media Gateway (MG) ID from the SBE. To disable use of the eroot package, use the **no** form of this command.

package {*package-name*}

no package {*package-name*}

Syntax Description

<i>package-name</i>	Name of the package to be enabled. Currently, the only possible value is eroot . If this command is not configured, the eroot package is enabled by default.
---------------------	---

Command Default

If this command is not configured, the eroot package is enabled.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example enables the eroot package:

```
Router (config)# sbc mySbc dbe
Router (config-sbc-dbe)# vdb
Router (config-sbc-dbe-vdbe)# package eroot
Router (config-sbc-dbe-vdbe)# end
```

The following example disables the eroot package:

```
Router (config)# sbc mySbc dbe
Router (config-sbc-dbe)# vdb
Router (config-sbc-dbe-vdbe)# no package eroot
Router (config-sbc-dbe-vdbe)# end
```


package segment max-pdu-size

To configure a data border element (DBE) to use the H.248 Segmentation package and to specify the maximum protocol data unit (PDU) size that the User Datagram Protocol (UDP) should use for H.248 control signaling, use the **package segment max-pdu-size** command in VDBE configuration mode. To reconfigure the default maximum PDU size of 0 and disable the package, use the **no** form of the command.

package segment max-pdu-size *{size}*

no package segment max-pdu-size

Syntax Description

<i>size</i>	The maximum UDP PDU size in bytes. The range is 0 to 65535. A value of 0 means package segmentation is disabled.
-------------	--

Command Default

The default is 0 if the command is not configured, or the **no package segment max-pdu-size** command is issued.

Command Modes

VDBE configuration (config-sbc-dbe-vdbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example enables the H.248 Segmentation package and configures the DBE to use 64000 bytes as the maximum PDU size during segmentation:

```
Router (config)# sbc mySbc dbe
Router (config-sbc-dbe)# vdbe
Router (config-sbc-dbe-vdbe)# package segment max-pdu-size 64000
Router (config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
package segment seg-timer-value	When the H.248 Segmentation package is in effect, configures the time interval within which the DBE should expect to receive any outstanding message segments from the media gateway controller (MGC) after the SegmentationCompleteToken is received.
show sbc dbe controllers	Displays the media gateway controllers and the controller address configured on each DBE.

port-range (ipv4)

To create a port range associated with an IPv4 media address or a pool of IPv4 media addresses, use the **port-range** command in the corresponding SBC-DBE media address configuration mode or the SBC-DBE media address pool configuration mode. To delete a port range, use the **no** form of this command.

port-range {*min-port*} {*max-port*} [**any** | **voice** | **video** | **signaling** | **fax**]

no port-range {*min-port*} {*max-port*}

Syntax Description

<i>min-port</i>	The starting port number of the range. The possible values are 1 to 65535, but the <i>min-port</i> value specified must be less than or equal to the <i>max-port</i> value specified. If a <i>min-port</i> value is not configured, the default value is 16384.
<i>max-port</i>	The ending port number of the range. The possible values are 1 to 65535, but the <i>max-port</i> value specified must be greater than or equal to the <i>min-port</i> value specified. If a <i>max-port</i> value is not configured, the default value is 32767.
any	(Optional) Specifies that the class of service affinity for the port range is any class of service. If a class of service value is not configured, this is the default value.
voice	(Optional) Specifies that the class of service affinity for the port range is voice.
video	(Optional) Specifies that the class of service affinity for the port range is video.
signaling	(Optional) Specifies that the class of service affinity for the port range is signaling.
fax	(Optional) Specifies that the class of service affinity for the port range is fax.

Command Default

If the **port-range** command is not configured, the default *min-port* value is 16384, the default *max-port* value is 32767, and the default class of service affinity is **any**.

Command Modes

SBC-DBE media address configuration (config-sbc-dbe-media-address) or SBC-DBE media address pool configuration (config-sbc-dbe-media-address pool)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **port-range** command in SBC-DBE media address configuration mode to specify a port range for a single media address.

Use the **media-address ipv4** command to enter SBC-DBE media address configuration mode before entering the **port-range** command for a single media address.

Use the **port-range** command in SBC-DBE media address pool configuration mode to specific a port range for a pool of media addresses.

Use the **media-address pool ipv4** command to enter SBC-DBE media address pool configuration mode before entering the **port-range** command for a pool of media addresses.

Examples

The following example creates a new port range between 10000 to 20000 with a service class affinity of voice for a single media address:

```
Router(config-sbc-dbe-media-address)# port-range 10000 20000 voice
```

The following example modifies the service class affinity set for the media address by the previous example to any class of service:

```
Router(config-sbc-dbe-media-address)# port-range 10000 20000 any
```

The following example deletes the port range set for the media address by the previous example:

```
Router(config-sbc-dbe-media-address)# no port-range 10000 20000
```

The following example creates a new port range between 10000 to 20000 with a service class affinity of voice for a pool of media addresses:

```
Router(config-sbc-dbe-media-address pool)# port-range 10000 20000 voice
```

The following example modifies the service class affinity set for the pool of media addresses by the previous example to any class of service:

```
Router(config-sbc-dbe-media-address pool)# port-range 10000 20000 any
```

The following example deletes the port range set for the pool of media addresses by the previous example:

```
Router(config-sbc-dbe-media-address pool)# no port-range 10000 20000
```

Related Commands

Command	Description
media-address ipv4	Adds an IPv4 address to the set of addresses that can be used by the data border element (DBE) as a local media address.
media-address pool ipv4	Creates a pool of IPv4 addresses that can be used by the data border element (DBE) as local media addresses.

port-range (ipv6)

To create a port range associated with a single IPv6 media address or a pool of IPv6 media addresses, use the **port-range** command in the corresponding SBC-DBE media address IPv6 configuration mode or the SBC-DBE media address pool IPv6 configuration mode. To delete a port range, use the **no** form of this command.

port-range {*min-port*} {*max-port*} **signaling**

no port-range {*min-port*} {*max-port*}

Syntax Description

<i>min-port</i>	The starting port number of the range. The possible values are 1 to 65535, but the <i>min-port</i> value specified must be less than or equal to the <i>max-port</i> value specified. If a <i>min-port</i> value is not configured, the default value is 16384.
<i>max-port</i>	The ending port number of the range. The possible values are 1 to 65535, but the <i>max-port</i> value specified must be greater than or equal to the <i>min-port</i> value specified. If a <i>max-port</i> value is not configured, the default value is 32767.
signaling	Specifies that the class of service affinity for the port range is signaling.

Command Default

If the **port-range** command is not configured, the default *min-port* value is 16384 and the default *max-port* value is 32767, and the default class of service affinity is **signaling**.

Command Modes

SBC-DBE media address IPv6 configuration (cfg-sbc-dbe-media-addr-ipv6)
SBC-DBE media address pool IPv6 configuration (cfg-sbc-dbe-media-addr-pl-ipv6)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command is used to specify only the signaling class of service for the port range for a single IPv6 media address or for a range or pool of IPv6 media addresses. “Range” means the same as “pool.”

The related **port-range** command is used for a single IPv4 media address or a range or pool of IPv4 media addresses, and can specify voice, video, signaling, fax, and any class of service affinity for the port range.

Use the **media-address ipv6** command to enter into SBC-DBE media address IPv6 configuration mode before entering the **port-range** command for a single IPv6 media address.

Use the **media-address pool ipv6** command to enter into SBC-DBE media address pool IPv6 configuration mode before entering the **port-range** command for a pool of IPv6 media addresses.

Examples

The following example creates a new port range for a single IPv6 media address where the port range values are specified between 10000 and 20000. Use the **media-address ipv6** command first to enter into the submode for the specified single IPv6 media address.

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv6 5::1:1
Router(cfg-sbc-dbe-media-addr-ipv6)# port-range 10000 20000 signaling
```

The following example deletes the port range between 10000 and 20000 for a single IPv6 media address:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address ipv6 5::1:1
Router(cfg-sbc-dbe-media-addr-ipv6)# no port-range 10000 20000
```

The following example creates a new port range for an IPv6 media address range or pool. The port range values are between 10000 and 20000. Use the **media-address pool ipv6** command first to enter into the submode for a range of IPv6 media addresses.

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv6 5::1:1 5::1:10
Router(cfg-sbc-dbe-media-addr-pl-ipv6)# port-range 10000 20000 signaling
```

The following example deletes the port range between 10000 and 20000 for a range or pool of IPv6 media addresses:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# media-address pool ipv6 5::1:1 5::1:10
Router(cfg-sbc-dbe-media-addr-pl-ipv6)# no port-range 10000 20000
```

Related Commands

Command	Description
port-range (ipv4)	Creates a port range associated with an IPv4 media address or a pool of IPv4 media addresses.
media-address ipv6	Adds an IPv6 address to the set of addresses that can be used by the data border element (DBE) as a local media address.
media-address pool ipv6	Creates a pool of sequential IPv6 media addresses that can be used by the data border element (DBE) as local media addresses

remote-address ipv4

To configure the IPv4 remote address of the H.248 controller for the signaling border element (SBE), use the **remote-address ipv4** command in Controller H.248 configuration mode. To remove the IPv4 remote address, use the **no** form of this command.

remote-address ipv4 {*remote-address*}

no remote-address ipv4 {*remote-address*}

Syntax Description

<i>remote-address</i>	The IP address of the remote H.248 controller.
-----------------------	--

Command Default

No default behavior or values are available.

Command Modes

Controller H.248 configuration (config-sbc-dbe-vdbe-h248)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

After the remote address is configured, you cannot modify or delete it unless you detach the H.248 controller first by using the **no attach-controllers** command.



Note

This command is invalid for the unified model, where both the SBE and DBE logical entities co-exist on the same network element.

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, creates an H.248 controller with index 1, enters into Controller H.248 configuration mode, and configures the remote address as 1.1.1.1 on the H.248 controller:

```
Router(config)# sbc mySbc db
Router(config-sbc-dbe)# vdb
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 1.1.1.1
Router(config-sbc-dbe-vdbe-h248)# end
```

Related Commands

Command	Description
sbc db	Creates the data border element (DBE) service on a session border controller (SBC) and enters into SBC-DBE configuration mode.
vdbe	Configures a virtual data border element (vDBE) and enters the VDBE configuration mode.
controller h248	Configures an H.248 controller for a data border element (DBE).

remote-port

To define the port to connect to the signaling border element (SBE) for an H.248 controller, use the **remote-port** command in Controller H.248 configuration mode. To unconfigure the port to connect to the SBE for an H.248 controller, use the **no** form of this command.

remote-port *{port-num}*

no remote-port

Syntax Description

<i>port-num</i>	The port number to be configured. The port number ranges from 0 to 65535.
-----------------	---

Command Default

If the port is not configured or is configured with the value 0, then the H.248 default port number is 2944.

Command Modes

Controller H.248 configuration (config-sbc-dbe-vdbe-h248)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command is invalid for the unified model, where both the SBE and DBE logical entities co-exist on the same network element.

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, enters into Controller H.248 configuration mode, creates an H.248 controller with index 1, and configures the port to 2944 on the H.248 controller with index 1.

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# remote-port 2944
Router(config-sbc-dbe-vdbe-h248)# end
```

Related Commands

Command	Description
sbc dbe	Creates the data border element (DBE) service on a session border controller (SBC) and enters into SBC-DBE configuration mode.
vdbe	Configures a virtual data border element (vDBE) and enters the VDBE configuration mode.
controller h248	Configures an H.248 controller for a data border element (DBE).

sbc dbe

To create the data border element (DBE) service on a session border controller (SBC) and enter into the SBC-DBE configuration mode, use the **sbc dbe** command in global configuration mode. To remove the DBE entity, use the **no** form of this command.

sbc {*sbc-name*} **dbe**

no sbc {*sbc-name*} **dbe**

Syntax Description

<i>sbc-name</i>	The SBC service name.
-----------------	-----------------------

Command Default

No default behavior or values are available.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example creates a DBE service on an SBC called “mySbc,” and enters into SBC-DBE configuration mode:

```
Router(config)# sbc mySbc dbe  
Router(config-sbc-dbe)# end
```

Related Commands

Command	Description
interface sbc	Creates the session border controller (SBC) interface.

sbc dump-diagnostics

To dump any in-memory diagnostics currently gathered by the SBC service to either the current default, or the specified file system, use the **sbc dump-diagnostics** command in privileged EXEC mode. To disable the dump, use the **no** form of this command.

sbc dump-diagnostics [*file-system*]

no sbc dump-diagnostics [*file-system*]

Syntax Description

file-system (Optional) Base file system on which to store diagnostics.

Command Default

If no file system is specified, the command dumps SBC diagnostics to a default location.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command generates the following files:

- ipstrc_buf*.* —Contains binary IPS trace files used by Cisco customer support engineers
- pdtrc_buf*.* — Contains log messages that are stored in the logging buffer (as specified by the **debug sbc log-level buffer** command)

Examples

The following example dumps in-memory diagnostics to a specified file system called “disk2”:

```
Router# sbc dump-diagnostics disk2:
```

Related Commands

Command	Description
debug sbc ips	Turns on inter-process signal (IPS) tracing.

sbc interface-id

To map a physical interface on the data border element (DBE) to the physical-interface-id contained in the termination ID for the purpose of notifying the signaling border element (SBE) when a physical interface has experienced a state change, use the **sbc interface-id** command in interface configuration mode. To disable the mapping, use the **no** form of this command.

sbc interface-id {value}

no sbc interface-id {value}

Syntax Description	<div> <div><i>value</i></div> <div>The integer ID of the physical interface. The interface can only be Ethernet and Etherchannel interfaces.</div> </div> <div> <div></div> <div>The physical interface ID is the physical-interface-id in the termination ID.</div> </div>
---------------------------	---

Command Default	No default behavior or values are available..
------------------------	---

Command Modes	Interface configuration mode (config-if)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR1000 Series Aggregation Services Routers.

Usage Guidelines	<p>The sbc interface-id command has the following restrictions and conditions:</p> <ul style="list-style-type: none"> • It can only be used on Etherchannel (gigabit Etherchannel and fast Etherchannel) and on all Ethernet interfaces. Etherchannel may also be called port channel. • It cannot be configured on VLAN subinterfaces or any subinterfaces. • When a ServiceChange notification is sent, the termination ID is always reported wildcarded. • It is generated well before the Media Timeout event which has a 30 seconds default.
-------------------------	--

In order for the SBE to be informed about status changes on a physical interface on the DBE, you can use the **sbc interface-id** command to map that physical interface to the physical-interface-id contained in the termination ID. Thus the SBE is able to associate status changes on the physical interface with a pinhole. The command inserts the termination ID in the ServiceChange H.248 message. Therefore, when the physical interface changes status, the media gateway (MG) is able to report a service change with that particular termination ID to the SBE.

This command is used in conjunction with the ServiceChange Notification for Interface Status Change feature. See the *Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model* for more information on the feature at:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbc/2_xe/sbc_2_xe_book.html

Examples

In the following example, enter the **sbc interface-id** command for port-channel interface 99 in order to associate the physical-interface-id 2 contained in the termination ID for the pinhole with port-channel interface 99:

```
Router(config)# interface port-channel 99

Router(config-if)# sbc interface-id 2
Router(config-if)# no ip address
Router(config-if)# end
```

Subsequently, when port-channel interface 99 changes status, a service change with a wildcarded termination-id is reported to the SBE, where 2 is the physical-interface-id in tier-5 of the nine-tier termination ID and the SBE is able to associate status changes on interface 99 with a pinhole:

```
*/***/2/***/**
```

In the following configuration output example, the **sbc interface-id** command maps physical-interface-id 1 contained in the termination ID for the pinhole to GigabitEthernet interface 1:

```
interface gigabitethernet1

sbc interface-id 1
no ip address
negotiation auto
no keepalive
no cdp enable
end
```

Subsequently, when GigabitEthernet interface 1 changes status, a service change with a wildcarded termination-id is reported to the SBE, where 1 is the physical-interface-id in tier-5 of the nine-tier termination ID and the SBE is able to associate status changes on GigabitEthernet interface 1 with a pinhole:

```
*/***/1/***/**
```

Related Commands

Command	Description
interface	Configures an interface type and enters interface configuration mode.

sck-pool-size

To configure the buffer size of a Session Initiation Protocol (SIP) socket control, use the **sck-pool-size** command in the SBE configuration mode. To reconfigure the buffer size of the SIP socket control to the default value, use the **no** form of this command.

sck-pool-size *pool_size*

no sck-pool-size *pool_size*

Syntax Description	<i>pool_size</i> Pool size number. The range is from 1 to 65535. The default is 400.	
Command Default	None	
Command Modes	SBE configuration mode	
Command History	Release	Modification
	Cisco IOS Release 15.2(04)S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Examples	The following example shows how to configure the buffer size of an SIP socket control: Router> enable Router# configure terminal Router(config)# sbc 123 Router(config-sbc)# sbe Router(config-sbc-sbe)# sck-pool-size 23	

show interface sbc

To show session border controller (SBC) interface status and configuration, use the **show interface sbc** command in user EXEC or privileged EXEC configuration mode.

show interface sbc {*interface-num*}

Syntax Description

<i>interface-num</i>	Specifies the SBC interface number.
----------------------	-------------------------------------

Command Default

No default behavior or values are available.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **show interface sbc** command only collects IPv4 packet statistics for packets originating from the interface.

The **show interface sbc** command does not collect any IPv6 packet statistics for packets destined to and originating from the interface.

Examples

The following example shows the status of SBC interface 3:

```
Router# show interface sbc 3
```

Related Commands

Command	Description
show sbc dba addresses	Displays the H.248 control addresses and media addresses configured on DBEs.
show sbc dba controllers	Displays the media gateway controllers and the controller address configured on each DBE.
show sbc dba forwarder-stats	Displays the global list of statistics for the DBE forwarding process.
show sbc dba media-stats	Displays general DBE statistics. These statistics do not include data from active calls.

Command	Description
show sbc dbc media-flow-stats	Displays the statistics about one or more media flows collected on the DBE.
show sbc dbc signaling-flow-stats	Displays the statistics about one or more signaling flows collected on the DBE.

show sbc dba addresses

To list the H.248 control addresses and media addresses configured on data border elements (DBEs), use the **show sbc dba addresses** command in user EXEC or privileged EXEC mode.

show sbc {sbc-name} dba addresses

Syntax Description

<i>sbc-name</i>	Name of the session border controller (SBC) service.
-----------------	--

Command Default

No default behavior or values are available.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows the H.248 control and media addresses, VRF name, port ranges, and service class configured on a DBE that is on an SBC called "mySbc":

```
Router# show sbc mySbc dba addresses
```

```
SBC Service "mySbc"
```

```
  H.248 control address:10.0.0.1
```

Media-Address	VRF	Port-Range	Service-Class
1.1.1.1	Global	5-6	signaling
1.1.1.2-1.1.1.3	Global	16384-20000	any
1.1.1.5-1.1.1.6	Global		
6::2-6::3	Global	4-6	signaling
6::5	Global		
1111:2222:3333:4444::1-1111:2222:3333:4444::5	Global	2-6	signaling
1111:2222:3333:4444::8	Global		

Related Commands

Command	Description
show sbc dba controllers	Displays the media gateway controllers and the controller address configured on each DBE.
show sbc dba forwarder-stats	Displays the global list of statistics for the DBE forwarding process.
show sbc dba media-stats	Displays general DBE statistics. These statistics do not include data from active calls.

Command	Description
show sbc dbe media-flow-stats	Displays the statistics about one or more media flows collected on the DBE.
show sbc dbe signaling-flow-stats	Displays the statistics about one or more signaling flows collected on the DBE.
unexpected-source-alerting	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

show sbc dbc controllers

To list the media gateway controllers (MGCs) and the controller address configured on each data border element (DBE), use the **show sbc dbc controllers** command in user EXEC or privileged EXEC mode.

show sbc {sbc-name} dbc controllers

Syntax Description

<i>sbc-name</i>	Name of the session border controller (SBC) service.
-----------------	--

Command Default

No default behavior or values are available.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	Output was modified to add Session Establishment Time, Transaction Long Timer, and TMAX Timeout fields.

Examples

The following example shows that the controller is attached and a new field displaying the Session Establishment Time ("**since 2008/02/19 13:56:30**") that was added in Cisco IOS XE Release 2.2:

```
Router# show clock
```

```
*09:06:03.135 UTC Mon Feb 18 2008
```

```
Router# show sbc global dbc controllers
```

```
SBC Service "global"
```

```
vDBE in DBE location 1
```

```
DBE Admin Status: Active
```

```
Media gateway controller in use:
```

```
H.248 controller address
```

```
200.50.1.254:2970
```

```
Status: Attached, since 2008/02/19 13:56:30
```

	Sent	Received	Failed	Retried
Requests	1	0	0	1
Replies	0	1		0

```
Segmentation:
```

```
MGC PDU Size: N/A
```

```
MG PDU Size: N/A
```

```
MGC Seg timer: N/A
```

```
MG Seg timer: N/A
```

```
Segments Sent: N/A
```

```
Segments Rcvd: N/A
```

```
Configured controllers:
H.248 controller 2:
```

The following example establishes controller connection prior to the TMAX timeout being changed:

```
Router# show sbc global dbc controller
SBC Service "global"
  vDBE in DBE location 1

  DBE Admin Status:      Active
  DBE Transaction Long Timer 15000 (ms)
  DBE TMAX Timeout 10000 (ms)

  Media gateway controller in use:
    H.248 controller address
      200.50.1.254:2970
    Status:      Attached, since 2008/02/22 17:35:43

    Requests      Sent      Received      Failed      Retried
    Replies       0        1             0           0

  Segmentation:
    MGC PDU Size:  N/A
    MG PDU Size:   N/A
    MGC Seg timer: N/A
    MG Seg timer:  N/A
    Segments Sent: N/A
    Segments Rcvd: N/A

  Configured controllers:
    H.248 controller 2:
      Remote address: 200.50.1.254:2970
      Transport:      UDP
```

The following example shows that the Tmax timeout has been changed to 20 seconds and entering the **show controller** command again displays the new fields, Transaction Long Timer and TMAX Timeout, added in Cisco IOS XE Release 2.2:

```
Router# show sbc global dbc controllers
SBC Service "global"
  vDBE in DBE location 1

  DBE Admin Status:      Active
  DBE Transaction Long Timer 25000 (ms)
  DBE TMAX Timeout 20000 (ms)

  Media gateway controller in use:
    H.248 controller address
      200.50.1.254:2970
    Status:      Detached

    Requests      Sent      Received      Failed      Retried
    Replies       0        0             0           0

  Segmentation:
    MGC PDU Size:  N/A
    MG PDU Size:   N/A
```

```

MGC Seg timer: N/A
MG Seg timer: N/A
Segments Sent: N/A
Segments Rcvd: N/A

```

```

Configured controllers:
H.248 controller 2:
  Remote address: 200.50.1.254:2970
  Transport:      UDP

```

The following example shows the H.248 controllers configured on the virtual data border element (vDBE) with a location ID of 1 on an SBC called “mySbc.” In this example, the H.248 status is active.

Router# **show sbc mySbc dbe controllers**

```

SBC Service "mySbc"
  vDBE in DBE location 1

  DBE Admin Status: Active
  Media gateway controller in use:
    H.248 controller address
      200.100.1.254:2991
    Status: Detached

    Sent      Received    Failed    Retried
Requests    1           0         0         2
Replies     0           0         0         0

  Segmentation:
    MGC PDU Size: 33 bytes
    MG PDU Size: N/A
    MGC Seg timer: 44 ms
    MG Seg timer: N/A
    Segments Sent: N/A
    Segments Rcvd: N/A

  Configured controllers:
    H.248 controller 1:
      Remote address: 200.100.1.254:2991
      Transport:      UDP (with IAH)

```

The following example shows the H.248 controllers configured on the virtual data border element (vDBE) with a location ID of 1 on an SBC called “mySbc.” In this example, the H.248 status is inactive.

Router# **show sbc mySbc dbe controllers**

```

SBC Service "mySbc"
  vDBE in DBE location 1

  DBE Admin Status: Inactive
  Media gateway controller in use:

  Configured controllers:
    H.248 controller 5:
      Remote address: 10.1.1.1:6
      Transport:      UDP

```

Table 1 describes the significant fields shown in the display.

Table 1 *show sbc dbc controllers Field Descriptions*

Field	Description
DBE Admin Status	Possible values are Active and Inactive.
Media gateway controller in use:	Statistics that follow are applicable to the MGC(s) in use.
H.248 controller address	H.248 controller address.
Status:	Status of the controller. Possible values are Attached and Detached.
Requests	Number of H.248 requests sent, received, failed, or retried.
Replies	Number of H.248 replies sent, received, failed, or retried.
Segmentation:	Statistics that follow are applicable to the H.248 Segmentation package.
MGC PDU Size	Maximum protocol data unit (PDU) size, in bytes, that the User Datagram Protocol (UDP) should use for H.248 control signaling.
MG PDU Size	Not applicable.
MGC Seg timer	Time interval, in milliseconds, on the segmentation timer.
MG Seg timer	Not applicable.
Segments Sent:	Number of segments sent.
Segments Rcvd:	Number of segments received.
Configured controllers:	Statistics that follow are applicable to configured H.248 controllers.
Remote address	Remote address of the configured controller.
Transport	Transport in use on the configured controller. Possible values are UDP, UDP (with IAH), TCP, and TCP (with IAH)
Session Establishment Time	This has the format (YY/MM/DD hour/minute/second). If the router time is changed, the operator is expected to detect this from any console log, as the Session Establishment Time is not updated.
Transaction Long Timer	This timer determines the total time the DBE waits (and keep retrying) from initially sending a request until receiving a response. It is set to TMAX + MaxRTT, where TMAX is configurable and MaxRTT is hard coded to 0.5 seconds. The association to the MGC is lost if this timer expires before the transaction reply is received.
TMAX Timeout	This is the maximum delay in seconds. It is a parameter of the TMAX timer that limits the maximum delay of retransmissions by the DBE when sending messages to the MGC. The default is 10 seconds.

Related Commands

Command	Description
show sbc dbe addresses	Displays the H.248 control addresses and media addresses configured on DBEs.
show sbc dbe forwarder-stats	Displays the global list of statistics for the DBE forwarding process.
show sbc dbe media-stats	Displays general DBE statistics. These statistics do not include data from active calls.
show sbc dbe media-flow-stats	Displays the statistics about one or more media flows collected on the DBE.
show sbc dbe signaling-flow-stats	Displays the statistics about one or more signaling flows collected on the DBE.
unexpected-source-alerting	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

show sbc dbf flow-stats

To list all flow statistics, both signaling and media flows, collected on the data border element (DBE), use the **show sbc dbf flow-stats** command in user EXEC or privileged EXEC mode.

```
show sbc {sbc-name} dbf flow-stats [{summary | detail}] [vrf vrf-name] [ {ipv4 A.B.C.D | ipv6
ipv6-address} [port port-number]] [context {id}| termination {termination substring}]
```

Syntax Description	
<i>sbc-name</i>	Name of the session border controller (SBC) service.
summary	(Optional) Displays a summary of all flow statistics, including pinhole flows, for the DBE.
detail	(Optional) Displays detailed flow statistics, including pinhole flows, for the DBE.
vrf <i>vrf-name</i>	(Optional) Displays only flows to or from the specified VPN routing and forwarding instance (VRF).
ipv4 <i>A.B.C.D</i>	(Optional) Displays only flows to or from the specified IPv4 media IP address.
ipv6 <i>ipv6-address</i>	(Optional) Displays only flows to or from the specified IPv6 media IP address.
port <i>port-number</i>	(Optional) Displays only flows to or from the specified port number.
context	(Optional) Shows summary or detailed display of all pinhole flows within the context ID.
<i>id</i>	(Optional) Specifies the context ID number.
termination	(Optional) Shows summary or detailed display of pinhole flows that match the termination substring.
<i>termination substring</i>	(Optional) Specifies the termination substring number.

Command Default No default behavior or values are available.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines Not all endpoints report RTP Control Protocol (RTCP) endpoint statistics. In addition, not all endpoints that report RTCP statistics report all the fields shown.

When the “Media Flowing” field is reported as Yes, it either means that media has been observed flowing on the call within the media timeout period, or the call has failed over within the last media timeout period and the SBC has not yet had a chance to observe whether media is flowing or not.


```

Data Received:          0 (bytes)
Data Sent:              0 (bytes)
Data Discarded:        0 (bytes)
GM Discarded Packets:   0
Time To Recovery:       Not known
Media Flowing:         No
Unexpected SrcAddr Packets: No
Max Burst size:         0 (bytes)
Delay variation tolerance: 0 (microseconds)
SDP string:             m=application $ udp 0
Graceful deactivation:  No
DiffServ Code Point:    B8
Media Loss Event:       No
NAT Latch Event:        No

```

The following example displays a summary of all flows with context ID number 1:

```

Router# show sbc global dbe flow-stats summary context 1
SBC Service "global"
Media flow statistics
Context ID 1          Stream ID 2
Side A:              Name mycompany/voice/gn/0/1/0/1/ac/3    Media Flowing: No
  Local Address/Port: 202.50.2.1/10002
  Remote Address/Port: 10.10.127.22/17384
  Status:             OutofService
Side B:              Name mycompany/voice/gn/0/2/0/1/bb/4    Media Flowing: No
  Local Address/Port: 202.50.2.1/10004
  Remote Address/Port: 200.0.0.1/19384
  Status:             OutofService

SBC Service "global"
Signaling flow statistics
Context ID 1          Stream ID 1
Side A:              Name mycompany/sip4/gn/0/1/0/1/ac/1    Media Flowing: No
  Local Address/Port: 202.50.2.1/10000
  Remote Address/Port: 3.0.0.3/5000
  Status:             InService
Side B:              Name mycompany/sip4/gn/0/1/0/1/bb/2    Media Flowing: No
  Local Address/Port: 202.50.2.1/10001
  Remote Address/Port: 3.0.0.3/5000
  Status:             InService

```

The following example displays a summary of flows with the termination string, mycompany:

```

Router# show sbc global dbe flow-stats summary termination mycompany
SBC Service "global"
Media flow statistics
Context ID 1          Stream ID 2
Side A:              Name mycompany/voice/gn/0/1/0/1/ac/3    Media Flowing: No
  Local Address/Port: 202.50.2.1/10002
  Remote Address/Port: 10.10.127.22/17384
  Status:             OutofService
Side B:              Name mycompany/voice/gn/0/2/0/1/bb/4    Media Flowing: No
  Local Address/Port: 202.50.2.1/10004
  Remote Address/Port: 200.0.0.1/19384
  Status:             OutofService

SBC Service "global"
Signaling flow statistics
Context ID 1          Stream ID 1
Side A:              Name mycompany/sip4/gn/0/1/0/1/ac/1    Media Flowing: No
  Local Address/Port: 202.50.2.1/10000

```

```

Remote Address/Port: 3.0.0.3/5000
Status:                InService
Side B:                Name mycompany/sip4/gn/0/1/0/1/bb/2    Media Flowing:  No
Local Address/Port:   202.50.2.1/10001
Remote Address/Port:  3.0.0.3/5000
Status:                InService

```

The following example displays a summary of flows with the combination of context ID 1 and the termination string, mycompany:

```

Router# show sbc global dbe flow-stats summary context 1 termination mycompany
SBC Service "global"
Media flow statistics
Context ID 1                Stream ID 2
Side A:                    Name mycompany/voice/gn/0/1/0/1/ac/3    Media Flowing:  No
Local Address/Port:       202.50.2.1/10002
Remote Address/Port:      10.10.127.22/17384
Status:                   OutofService
Side B:                    Name mycompany/voice/gn/0/2/0/1/bb/4    Media Flowing:  No
Local Address/Port:       202.50.2.1/10004
Remote Address/Port:      200.0.0.1/19384
Status:                   OutofService

SBC Service "global"
Signaling flow statistics
Context ID 1                Stream ID 1
Side A:                    Name mycompany/sip4/gn/0/1/0/1/ac/1    Media Flowing:  No
Local Address/Port:       202.50.2.1/10000
Remote Address/Port:      3.0.0.3/5000
Status:                   InService
Side B:                    Name mycompany/sip4/gn/0/1/0/1/bb/2    Media Flowing:  No
Local Address/Port:       202.50.2.1/10001
Remote Address/Port:      3.0.0.3/5000
Status:                   InService

```

Table 2 *show sbc dbe flow-stats Field Descriptions*

Field	Description
Context ID	The context ID to which the flow is associated.
Stream ID	Stream ID.
State of Media Flow	Flow (or Termination) state (Active, Allocated, or Unknown). Active—The DBE has programmed the flow pair and media has started flowing in at least one direction. Allocated—The DBE has programmed the flow pair, but no media has started to flow. Unknown—The DBE has not yet been given enough information by the controller to be able to program the flow pair.

Table 2 *show sbc dbe flow-stats Field Descriptions (continued)*

Field	Description
State of Signaling Flow	Flow state (Active, Allocated, or Unknown). <ul style="list-style-type: none"> Active—DBE has programmed the flow pair and the media has started flowing in at least one direction. Allocated—DBE has programmed the flow pair, but no media has started to flow. Unknown—DBE has not yet been given enough information by the controller to be able to program the flow pair.
Call Established Time	Call established time in the format 23:51:29 UTC Jun 21 2007.
Flow Priority	Priority of the call (Routine or Urgent).
Side A	Information for the initiating side of the call.
Side B	Information for the terminating side of the call.
Name	Name of the flow.
Reserved Bandwidth	Bandwidth reserved for the call in bytes per second. (This value maps to the tman/sdr value.)
Status	Status is InService or OutofService. InService—Flow on this side is in service. OutofService—No media is forwarded.
VRF Name	Either the VRF name, or “Global” when there is no VRF.
VLAN Tags (Priorities)	VLAN tags and Ethernet priorities information.
Local Address	Local address on the DBE on which packets are received for this side of the call.
Local Port	Local port on the DBE on which packets are received for this side of the call.
Remote Address	Address of the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Port	Port on the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Source Address Mask	If specified, all packets matching the Remote Source Address Mask are classified as belonging to this flow rather than just those matching the full remote and port. (This value maps to the gm/sam value.)
Packets Received	Number of packets received from the remote endpoint.
Packets Sent	Number of packets forwarded to the remote endpoint.
Packets Discarded	Number of packets dropped (due to bandwidth policing, for example).
Data Received	Number of bytes of data received from the remote endpoint.
Data Sent	Number of bytes of data forwarded to the remote endpoint.

Table 2 *show sbc dbe flow-stats Field Descriptions (continued)*

Field	Description
Data Discarded	Number of bytes of data dropped (due to bandwidth policing, for example). (This value maps to the gm/sam value.)
GM Discarded Packets	This counter is always set to zero because it is not currently implemented. It will be the number of data packets received from the remote endpoint that have been discarded locally because of source address/port filtering.
Time To Recovery	The tsc/ttr value from Termination State Control (TSC) package, in milliseconds.
RTCP Packets Sent	If there are RTCP packets flowing in the call, the number of RTP packets (within the most recently received RTCP) that the endpoint reports as being sent.
RTCP Packets Received	If there are RTCP packets flowing in the call, the number of RTP packets (within the most recently received RTCP) that the endpoint reports as being received.
RTCP Packets Lost	If there are RTCP packets flowing in the call, the number of RTP packets (within the most recently received RTCP) that the endpoint reports as being lost.
DTMF Interworking	Indicates whether DTMF interworking is in operation for the flow.
Media Flowing	Indicates whether packets are flowing from the endpoint.
Unexpected SrcAddr Packets	<p>If unexpected-source-alerting is switched on with the unexpected-source-alerting command, this counter records the number of alerts generated for the flow when media packets for a call are received from an unexpected source address and port.</p> <p>An unexpected source event happens when a packet is received, matched to a flow (but not by a full 5-tuple comparison), and found to have come from the wrong remote address.</p>
Delay variation tolerance	The delay variation tolerance (tman/dvt) associated with the Tman package. Defines the delay variation tolerance for the stream in tenths of microseconds when enforcing the PDR value in the first leaky bucket.
SDP string	The SDP string is that present on the H.248 ADD request to provision the call.
Graceful deactivation	Description to be added.
DiffServ Code Point	The Diffserv Code point is the (DSCP value) provided on the H.248 request to mark the media packets. This reflects the ds/dscp parameters.
Media Loss Event	Media Loss Event is “Yes” if the flow has the nt/qualert subscription.
NAT Latch Event	The NAT Latch Event is “Yes” if the flow has adr/rsac subscribed.

Table 2 *show sbc dbe flow-stats Field Descriptions (continued)*

Field	Description
Billing ID	Signaling border element (SBE) billing ID for this side of the call.
Media directions allowed	Allowed directions of media flow for this side of the call (inactive, sendonly, recvonly, or sendrecv).

Related Commands

Command	Description
show sbc dbe addresses	Displays the H.248 control addresses and media addresses configured on DBEs.
show sbc dbe controllers	Displays the media gateway controllers and the controller address configured on each DBE.
show sbc dbe forwarder-stats	Displays the global list of statistics for the DBE forwarding process.
show sbc dbe media-stats	Displays general DBE statistics. These statistics do not include data from active calls.
show sbc dbe signaling-flow-stats	Displays the statistics about one or more signaling flows collected on the DBE.
unexpected-source-alerting	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

show sbc dbe forwarder-stats

To display the global list of statistics for the DBE forwarding process, use the **show sbc dbe forwarder-stats** command in user EXEC mode or privileged EXEC mode.

show sbc {*sbc-name*} **dbe forwarder-stats**

Syntax Description	<i>sbc-name</i> Name of the session border controller (SBC) service.
---------------------------	--

Command Default	No default behavior or values are available.
------------------------	--

Command Modes	User EXEC (>) Privileged EXEC (#)
----------------------	--------------------------------------

Command History	Release Modification
	Cisco IOS XE Release 2.1 This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	This command provides a live snapshot of the current state of the DBE forwarding process by showing low-level statistics on the packets processed by the process. This command is intended to be used by Cisco customer support engineers to diagnose media problems.
-------------------------	---

Because DBE forwarding statistics can overwrite after approximately 4 billion packets, overall packet counts might not be accurate. For more accurate statistics on completed calls, use the **show sbc dbe media-stats** command. For accurate information on active flows, use the **show sbc dbe media-flow-stats** command.

Examples	The following example shows the list of statistics for the DBE forwarding process:
-----------------	--

```
Router# show sbc global dbe forwarder-stats
```

```
IOSd MPF Stub Message statistics
```

```
-----
```

```
Total global PMI messages received      = 1
Total global PMI messages transmitted   = 1
Total call PMI messages received        = 0
Total call PMI messages transmitted     = 0
Total global PMI message handling failures = 0
Total call PMI message handling failures = 0
Total global TDL messages received      = 1
Total global TDL messages transmitted   = 1
Total call TDL messages received        = 0
Total call TDL messages transmitted     = 0
Total global TDL message handling failures = 0
Total call TDL message handling failures = 0
Total packets injected                  = 0
Total packets punted                     = 0
```

show sbc dbe forwarder-stats

```

Total injected packets dropped          = 0
Total punted packets dropped            = 0
Total global message timeouts           = 0
Total call message timeouts             = 0

Call ID database is NOT Initialised

IOSd MPF Stub Call statistics
-----
Number of currently in-use Calls        = 0
High-water number of in-use Calls      = 0
Maximum number of in-use Calls supported = 0

SBC Media Forwarder Statistics
-----
Summary information:
  Total packets received                = 28416
  Total packets forwarded                = 14336
  Total packets dropped                  = 14080
  Total packets punted                  = 0
  Incoming packets diverted to SBC subsystem = 0
  Outgoing packets inserted by SBC subsystem = 0

Detailed breakdown of statistics:

Dropped packets:
  IP TTL expired                        = 0
  No associated flow                    = 0
  Wrong source for flow                 = 0
  Ingress flow receive disabled         = 0
  Egress flow send disabled             = 0
  Not conforming to flowspec            = 14080
  Badly formed RTP                      = 0
  Badly formed RTCP                    = 0
  Excessive RTCP packet rate            = 0
  Borrowed for outgoing DTMF           = 0
  Unknown destination address           = 0
  Misdirected                          = 0
  Feature disabled                      = 0
  Reprocess limit exceeded              = 0

Punted packets:
  H.248 control packets                 = not implemented
  Packets containing options            = 0
  Fragmented packets                    = 0
  Unexpected IP protocol                = 0
  Packets from invalid port range       = 0

Punted packets dropped through rate limiting = 0
Packets colored with configured DSCP       = 0

Diverted DTMF packets dropped:
  Excessive DTMF packet rate            = 0
  Bad UDP checksum                      = not implemented
  Diverted packet queue full            = not implemented
  Other                                 = not implemented

Inserted packets dropped:
  Flow inactive or disabled             = 0
  No outgoing packet buffer available    = 0
  Outgoing Queue full                   = 0
  Other                                 = 0

Generated event information:

```



```

Number of media UP events           = 0
Number of media DOWN events        = 0
Number of unexpected source events  = 0

Platform specific statistics:
Packets learn source address       = 0
Packets Learn source address timed out = 0
Packets conformed                  = 0
Packets exceed                     = 0
Packets RTCP receive               = 0

SBC Media Forwarder statistics can wrap after
approximately 18 quintillion packets. For more accurate
statistics on completed calls, please use
show sbc ... dbe media-stats

```

Table 3 *show sbc dbe forwarder-stats Field Descriptions*

Field	Description
IOSd MPF Stub Message statistics	
Total global PMI messages received	Total global packet management interface (PMI) messages received by the DBE forwarding process. This counter increments during normal operation.
Total global PMI messages transmitted	Total global packet management interface (PMI) messages transmitted by the DBE forwarding process. This counter increments during normal operation.
Total call PMI messages received	Total packet management interface (PMI) messages related to calls received by the DBE forwarding process. This counter increments during normal operation.
Total call PMI messages transmitted	Total packet management interface (PMI) messages related to calls transmitted by the DBE forwarding process. This counter increments during normal operation.
Total global PMI message handling failures	Failure counters indicating that something has gone wrong with handling total global packet management interface (PMI) messages. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total call PMI message handling failures	Failure counters indicating that something has gone wrong with handling total packet management interface (PMI) messages related to calls. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total global TDL messages received	Total global type definition language (TDL) messages received by the DBE forwarding process. This counter increments during normal operation.
Total global TDL messages transmitted	Total global type definition language (TDL) messages transmitted by the DBE forwarding process. This counter increments during normal operation.

Table 3 *show sbc dbf forwarder-stats Field Descriptions (continued)*

Field	Description
Total call TDL messages received	Total type definition language (TDL) messages related to calls received by the DBE forwarding process. This counter increments during normal operation.
Total call TDL messages transmitted	Total type definition language (TDL) messages related to calls transmitted by the DBE forwarding process. This counter increments during normal operation.
Total global TDL message handling failures	Failure counters indicating that something has gone wrong with handling total global type definition language (TDL) messages. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total call TDL message handling failures	Failure counters indicating that something has gone wrong with handling total type definition language (TDL) messages related to calls. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total packets injected	Total dual-tone multifrequency (DTMF) packets inserted into the Real-time Transport Protocol (RTP) stream. If DTMF interworking is configured, then these counters are expected to increase.
Total packets punted	Total dual-tone multifrequency (DTMF) packets removed from the Real-time Transport Protocol (RTP) streams. If DTMF interworking is configured, then these counters are expected to increase.
Total injected packets dropped	Failure counters indicating that something has gone wrong—total DTMF packets inserted into RTP streams that have dropped. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
Total punted packets dropped	Failure counters indicating that something has gone wrong—total DTMF packets removed from RTP streams that have dropped. The suggested action is to monitor the counters and if they are increasing or are associated with another failure, then call TAC.
IOSd MPF Stub Call statistics	
Number of currently in-use Calls	Number of calls currently in use.
High-water number of in-use Calls	The maximum number of calls that have ever been in use.
Maximum number of in-use Calls supported	This will only be filled in once the Call IS database moves to initialized state.
SBC Media Forwarder Statistics	
Summary information	
Total packets received	Total packets received by the DBE forwarding process.
Total packets forwarded	Total packets forwarded by the DBE forwarding process.

Table 3 *show sbc dbf forwarder-stats Field Descriptions (continued)*

Field	Description
Total packets dropped	Total packets dropped by the DBE forwarding process for any reason.
Total packets punted	Total packets punted to the IP stack by the DBE forwarding process.
Incoming packets diverted to SBC subsystem	Number of incoming packets diverted to the Media Gateway Manager (MGM).
Outgoing packets inserted by SBC subsystem	Number of outgoing packets inserted by MGM.
Detailed breakdown of statistics	
Dropped packets	
IP TTL expired	Number of packets rejected by DBE forwarding process and dropped because the IP time to live (TTL) has expired.
No associated flow	Number of packets rejected by DBE forwarding process and dropped because they do not correspond to a matching media flow.
Wrong source for flow	Number of packets rejected by DBE forwarding process and dropped because the source IP address and source port do not match the expected source address and source port for the flow.
Ingress flow receive disabled	Number of packets rejected by DBE forwarding process and dropped because receiving packets from the remote endpoint is disabled.
Egress flow send disabled	Number of packets rejected by DBE forwarding process and dropped because sending packets to the remote endpoint is disabled.
Not conforming to flowspec	Number of packets rejected by DBE forwarding process and dropped because they do not conform according to flowspec traffic policing for the flow. A flowspec is the traffic parameters of a stream of IP packets between two applications in IPv6.
Badly formed RTP	Number of packets rejected by DBE forwarding process and dropped due to Real Time Protocol (RTP) errors.
Badly formed RTCP	Number of packets rejected by DBE forwarding process and dropped due to Real Time Control Protocol (RTCP) errors.
Excessive RTCP packet rate	Number of RTCP packets rejected by DBE forwarding process and dropped because too many RTCP packets were sent on a given flow. The DBE forwarding process allows two RTCP packets per second for each flow.
Borrowed for outgoing DTMF	Number of packets rejected by DBE forwarding process and dropped because they were borrowed from their own flow in order to allow an outgoing packet to be inserted into a flow.
Unknown destination address	Number of packets rejected by DBE forwarding process and dropped because the destination address is unknown.

Table 3 *show sbc dbe forwarder-stats Field Descriptions (continued)*

Field	Description
Misdirected	Number of packets that was dropped due to having an address that would have caused the packets to be punted.
Feature disabled	Number of packets that was received while SBC was in the process of being deactivated. Depending on the volume of traffic, this number will remain small. This counter only increments during the deactivation process. Once the feature (SBC) is fully deactivated (with the no activate command), this counter will no longer increment.
Reprocess limit exceeded	Error condition counter. Counts errors when an SBC packet is re-processed too many times because the destination address was changed to be a local address on the DBE. After the destination address is translated and forwarded, the packet ends up in the SBC path again. This counter does not typically increase.
Punted packets	
H.248 control packets	Not implemented in command output.
Packets containing options	Number of packets rejected by DBE forwarding process and punted because the IP header contains IP options.
Fragmented packets	Number of packets rejected by DBE forwarding process and punted to the IP stack because the IP datagram is fragmented.
Unexpected IP protocol	Number of packets rejected by DBE forwarding process and punted because they are neither UDP nor TCP, or they are TCP but they are not destined for a signaling pinhole.
Packets from invalid port range	Number of packets rejected by DBE forwarding process and punted because the destination UDP port is outside the VoIP UDP port range.
Punted packets dropped through rate limiting	Number of packets not punted to the IP stack and dropped due to rate limiting.
Packets colored with configured DSCP	Number of packets colored with configured marker DSCP value by Two-Rate-Three-Color Marker feature.
Diverted DTMF packets dropped	
Excessive DTMF packet rate	Number of incoming packets diverted to MGM but dropped due to rate limiting. These packets are included in the divert count and drop count.
Bad UDP checksum	Not implemented in command output.
Diverted packet queue full	Not implemented in command output.
Other	Not implemented in command output.
Inserted packets dropped	
Flow inactive or disabled	Number of outgoing packets inserted by MGM but dropped because the request is invalid. These packets are included in the insert count and drop count.

Table 3 *show sbc dbe forwarder-stats Field Descriptions (continued)*

Field	Description
No outgoing packet buffer available	Number of outgoing packets inserted by MGM but dropped because no packet buffers are available. These packets are included in the insert count and drop count.
Outgoing Queue full	Number of outgoing packets inserted by MGM but dropped because the outgoing packet queue is full. These packets are included in the insert count and drop count.
Other	Number of outgoing packets inserted by MGM but dropped for other reasons. These packets are included in the insert count and drop count.
Generated event information	
Number of media UP events	Number of media UP events generated.
Number of media DOWN events	Number of media DOWN events generated.
Number of unexpected source events	Number of unexpected source address events generated.
Platform specific statistics	
Packets learn source address	For flows that have source address latching configured, a count of the number of packets that are latched.
Packets Learn source address timed out	If a flow has be programmed to relatch the source address and a new source address was not received in the specified timeframe, then this counts the timeout.
Packets conformed	Count of the number of packets that the policer indicated conformed to the flow specifier.
Packets exceed	Count of the number of packets that the policer indicated exceeded the flow specifier
Packets RTCP receive	Count of the number of RTCP packets received.

Related Commands

Command	Description
show sbc dbe addresses	Displays the H.248 control addresses and media addresses configured on DBEs.
show sbc dbe controllers	Displays the media gateway controllers and the controller address configured on each DBE.
show sbc dbe media-flow-stats	Displays the statistics about one or more media flows collected on the DBE.
show sbc dbe media-stats	Displays general DBE statistics. These statistics do not include data from active calls.
show sbc dbe signaling-flow-stats	Displays the statistics about one or more signaling flows collected on the DBE.

show sbc dbe history

To display a histogram of active calls history in a graph format, use the **show sbc dbe history** command in user EXEC or privileged EXEC mode.

show sbc {*sbc-name*} dbe history

Syntax Description

<i>sbc-name</i>	Name of the session border controller (SBC) service. Global is the only accepted name.
-----------------	--

Command Default

No default behavior or values are available.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **show sbc dbe history** command displays a histogram of active calls. The histogram represents a frequency distribution of calls over certain intervals. The following types of call history are shown:

- calls in-use per second (for the last minute)
- calls in-use per min (for the last hour)
- calls in-use per hour (for the last 72 hours)

Because the maximum number of calls supported is large, the Y-axis does not always start from zero, but instead displays the active range for the histogram interval.

The command output is similar to the Cisco IOS **show processes cpu history** command.

The following example displays a histogram of calls in-use per second, for the last 60 seconds. It shows that the highest number of calls happens at the 11.3th second with 1139 active calls:


```

11111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111
111111122222222222333322222111111110000111111111111100000
999456700090010199909900990000090900990000000000909001009
1200
1190
1180
1170
1160
1150
1140
1130          ***
1120      *****
1110 *****
1100...5...1...1...2...2...3...3...4...4...5...5...
           0       5       0       5       0       5       0       5
        Calls (last 60 seconds)

```

The following example displays a histogram of calls in-use, specifically the maximum calls and average calls, for the last 60 minutes. It shows that the highest number of calls happens at the 21th minute with 2129 active calls:

[illegible]

 `show sbc dbe history`**Related Commands**

Command	Description
<code>show processes cpu history</code>	Displays detailed CPU utilization statistics, including CPU history in a graph format.

show sbc dbe media-flow-stats

To list the media flow statistics collected on the data border element (DBE), use the **show sbc dbe media-flow-stats** command in user EXEC or privileged EXEC mode.

```
show sbc {sbc-name} dbe media-flow-stats [{summary | detail}] [vrf vrf-name] [{ipv4 A.B.C.D
| ipv6 ipv6-address} [port port-number]] [context {id}| termination {termination substring}]
```

Syntax Description	
<i>sbc-name</i>	Name of the session border controller (SBC) service.
summary	(Optional) Displays a summary of the media flow statistics, including pinhole flows, for the DBE.
detail	(Optional) Displays detailed media statistics, including pinhole flows, for the DBE.
vrf <i>vrf-name</i>	(Optional) Displays only media flows to or from the specified VPN routing and forwarding instance (VRF).
ipv4 <i>A.B.C.D</i>	(Optional) Displays only media flows to or from the specified IPv4 media IP address.
ipv6 <i>ipv6-address</i>	(Optional) Displays only media flows to or from the specified IPv6 media IP address.
port <i>port-number</i>	(Optional) Displays only media flows to or from the specified port number.
context	(Optional) Shows summary or detailed display of all pinhole flows within the context ID.
<i>id</i>	(Optional) Specifies the context ID number.
termination	(Optional) Shows summary or detailed display of pinhole flows. that match the termination substring.
<i>termination substring</i>	(Optional) Specifies the termination substring number.

Command Default No default behavior or values are available.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
	Cisco IOS XE Release 2.2	The context and termination keywords were added. New fields (Max Burst size, Delay variation tolerance, SDP string, Graceful deactivation, DiffServ Code Point, Media Loss Event, and NAT Latch Event) were added to the output display.

Not all endpoints report RTP Control Protocol (RTCP) endpoint statistics. In addition, not all endpoints that report RTCP statistics report all the fields shown.

The following example displays signaling and media flow pairs and additional fields added in Cisco IOS XE Release 2.2:

[illegible]

SBC-113

The following example shows detailed statistics from an IPv6 media flow collected on the DBE:

```
SBC Service "mySbc"
Media Flow:
Context ID:          13
Stream ID:           2
State of Media Flow: Allocated
Call Established Time: 23:51:29 UTC Jun 21 2007
Flow Priority:       Routine
Side A:
Name                 abc/voice/gn/0/1/0/1/ac/1
Reserved Bandwidth:  23 (bytes/second)
Status               InService
VRF Name:            Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address:        3333:1111:1111:2222:3333:4444:5555:7777
Local Port:           30000
Remote Address:        2222:1111:1111:2222:3333:4444:5555:7777
Remote Port:          20000
```

Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model

The following example shows summary statistics collected for media flows on the DBE:

Router# **show sbc mySbc dbe media-flow-stats summary**

```
SBC Service "mySbc"
Context ID 1          Stream ID 2
Side A:               Name abc/voice6/gn/0/1/0/1/ac/3      Media Flowing: No
  Local Address/Port: 3:100:1:1:1:1:1/30000
  Remote Address/Port: 2:100:1:1:1:1:1/20000
  Status:              In Service
Side B:               Name abc/voice6/gn/0/1/0/1/bb/4      Media Flowing: No
  Local Address/Port: 2:100:1:1:1:1:1/20000
  Remote Address/Port: 3:100:1:1:1:1:1/30000
  Status:              In Service
Context ID 2          Stream ID 2
Side A:               Name abc/voice4/gn/0/1/0/1/ac/7      Media Flowing: No
  Local Address/Port: 202.100.1.3/20002
  Remote Address/Port: Not known
  Status:              In Service
Side B:               Name abc/voice4/gn/0/1/0/1/bb/8      Media Flowing: No
  Local Address/Port: 202.100.1.3/20000
  Remote Address/Port: 200.100.1.1/30000
  Status:              In Service
```

Table 4 *show sbc dbe media-flow-stats Field Descriptions*

Field	Description
Context ID	The context ID to which the flow is associated.
Stream ID	Stream ID.
State of Media Flow	Flow (or Termination) state (Active, Allocated, or Unknown). Active—The DBE has programmed the flow pair and media has started flowing in at least one direction. Allocated—The DBE has programmed the flow pair, but no media has started to flow. Unknown—The DBE has not yet been given enough information by the controller to be able to program the flow pair.
Call Established Time	Call established time in the format 23:51:29 UTC Jun 21 2007.
Flow Priority	Priority of the call (Routine or Urgent).
Side A	Information for the initiating side of the call.
Side B	Information for the terminating side of the call.
Name	Name of the flow.
Reserved Bandwidth	Bandwidth reserved for the call in bytes per second. (This value maps to the tman/sdr value.)
Status	Status is InService or OutofService. InService—Flow on this side is in service. OutofService—No media is forwarded.
VRF Name	Either the VRF name, or “Global” when there is no VRF.
VLAN Tags (Priorities)	VLAN tags and Ethernet priorities information.

Table 4 *show sbc dbf media-flow-stats Field Descriptions (continued)*

Field	Description
Local Address	Local address on the DBE on which packets are received for this side of the call.
Local Port	Local port on the DBE on which packets are received for this side of the call.
Remote Address	Address of the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Port	Port on the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Source Address Mask	If specified, all packets matching the Remote Source Address Mask are classified as belonging to this flow rather than just those matching the full remote and port. (This value maps to the gm/sam value.)
Packets Received	Number of packets received from the remote endpoint.
Packets Sent	Number of packets forwarded to the remote endpoint.
Packets Discarded	Number of packets dropped (due to bandwidth policing, for example).
Data Received	Number of bytes of data received from the remote endpoint.
Data Sent	Number of bytes of data forwarded to the remote endpoint.
Data Discarded	Number of bytes of data dropped (due to bandwidth policing, for example). (This value maps to the gm/sam value.)
GM Discarded Packets	This counter is always set to zero because it is not currently implemented. It will be the number of data packets received from the remote endpoint that have been discarded locally because of source address/port filtering.
Time To Recovery	The tsc/ttr value from Termination State Control (TSC) package, in milliseconds.
RTCP Packets Sent	If there are RTCP packets flowing in the call, the number of RTP packets (within the most recently received RTCP) that the endpoint reports as being sent.
RTCP Packets Received	If there are RTCP packets flowing in the call, the number of RTP packets (within the most recently received RTCP) that the endpoint reports as being received.
RTCP Packets Lost	If there are RTCP packets flowing in the call, the number of RTP packets (within the most recently received RTCP) that the endpoint reports as being lost.
DTMF Interworking	Indicates whether DTMF interworking is in operation for the flow.
Media Flowing	Indicates whether packets are flowing from the endpoint.

Table 4 *show sbc dbe media-flow-stats Field Descriptions (continued)*

Field	Description
Unexpected SrcAddr Packets	<p>If unexpected-source-alerting is switched on with the unexpected-source-alerting command, this counter records the number of alerts generated for the flow when media packets for a call are received from an unexpected source address and port.</p> <p>An unexpected source event happens when a packet is received, matched to a flow (but not by a full 5-tuple comparison), and found to have come from the wrong remote address.</p>
Billing ID	Signaling border element (SBE) billing ID for this side of the call.
Media directions allowed	Allowed directions of media flow for this side of the call (inactive, sendonly, recvonly, or sendrecv).
Max Burst size	The maximum burst size (tman/mbs) associated with the Tman package.
Delay variation tolerance	The delay variation tolerance (tman/dvt) associated with the Tman package. Defines the delay variation tolerance for the stream in tenths of microseconds when enforcing the PDR value in the first leaky bucket.
SDP string	The SDP string is that present on the H.248 ADD request to provision the call.
Graceful deactivation	Description to be added.
DiffServ Code Point	The Diffserv Code point is the (DSCP value) provided on the H.248 request to mark the media packets. This reflects the ds/dscp parameters.
Media Loss Event	Media Loss Event is “Yes” if the flow has the nt/qualert subscription.
NAT Latch Event	The NAT Latch Event is “Yes” if the flow has adr/rsac subscribed.

Related Commands

Command	Description
show sbc dbe flow-stats	Lists all flow statistics, both signaling and media flows, collected on the data border element (DBE).
show sbc dbe addresses	Displays the H.248 control addresses and media addresses configured on DBEs.
show sbc dbe controllers	Displays the media gateway controllers and the controller address configured on each DBE.
show sbc dbe forwarder-stats	Displays the global list of statistics for the DBE forwarding process.
show sbc dbe media-stats	Displays general DBE statistics. These statistics do not include data from active calls.

Command	Description
show sbc dbe signaling-flow-stats	Displays the statistics about one or more signaling flows collected on the DBE.
unexpected-source-alerting	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

show sbc dbc media-stats (session border controller)

To list general data border element (DBE) statistics, use the **show sbc dbc media-stats** command in user EXEC or privileged EXEC mode.

show sbc {sbc-name} dbc media-stats

Syntax Description

<i>sbc-name</i>	Name of the Session Border Controller (SBC) service.
-----------------	--

Command Default

No default behavior or values are available.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.4	This command is supported in the unified model.
Cisco IOS XE Release 3.2S	The output of the command was updated to include information about the transcoded calls.

Usage Guidelines

The **show sbc dbc media-stats** statistics do not include data from active calls. The global counters keep track of packets received and sent on calls that have already ended.

The Active Flows statistic counts the number of flows for which media has been observed within the media-timeout period, or where the call has failed over within the last media-timeout period and the Session Border Controller (SBC) has not yet had a chance to observe whether media is flowing or not.

The Unclassified Pkts statistic includes all packets received on the VLAN interface that are not matched to a valid media flow. This includes media packets not matched to a flow, signaling packets, and any other traffic.

Examples

The following example shows general DBE statistics on a DBE that is on an SBC called "mySbc." These DBE statistics do not include data from active calls.

```
Router# show sbc mySbc dbc media-stats
```

```
SBC Service "MySBC"
  Available Bandwidth      = Unlimited
  Available Flows          = 131072
  Available Packet Rate    = Unlimited
  Active Media Flows       = 0
  Peak Media Flows        = 0
  Total Media Flows       = 0
  Active Transcoded Flows  = 1
```

```

Peak Transcoded Flows    = 1
Total Transcoded Flows   = 1
Active Signaling Flows   = 0
Peak Signaling Flows     = 0
Total Signaling Flows    = 0
SBC Packets Received     = 0
SBC Octets Received      = 0
SBC Packets Sent         = 0
SBC Octets Sent          = 0
SBC Packets Discarded    = 0
SBC Octets Discarded     = 0
No Media Count           = 0

```

Table 5 describes the significant fields shown in the display.

Table 5 *show sbc dbc media-stats Field Descriptions*

Field	Description
Max Term per Context	Maximum number of terminations per context.
Available Bandwidth	Total amount of bandwidth available for new calls.
Available Flows	Total amount of flows available for new calls.
Available Packet Rate	Amount of media packets per second available to new calls.
Active Media Flows	Current number of active calls.
Peak Media Flows	Maximum number of concurrent calls recorded.
Total Media Flows	Total number of calls set up on the DBE since the statistics were last cleared.
Active Transcoded Flows	Current number of active transcoded calls.
Peak Transcoded Flows	Maximum number of transcoded calls recorded.
Total Transcoded Flows	Total number of transcoded calls on the DBE.
Active Signaling Flows	Current number of flows that are actively forwarding signaling traffic.
Peak Signaling Flows	Peak number of active signaling flows since the statistics were last reset.
Total Signaling Flows	Accumulated total number of signaling flows. This count contains both active signaling flows and signaling flows that were allocated but never connected.
SBC Packets Received	Total number of SBC packets received by the DBE for completed calls.
SBC Octets Received	Number of octets of SBC data received by the DBE for completed calls.
SBC Packets Sent	Total number of SBC packets sent by the DBE for completed calls.
SBC Octets Sent	Number of octets of SBC data sent by the DBE for completed calls.
SBC Packets Discarded	Number of SBC packets discarded on completed calls.

Table 5 *show sbc dbe media-stats Field Descriptions (continued)*

Field	Description
SBC Octets Discarded	Number of SBC octets discarded on completed calls.
No Media Count	Number of calls that have been dropped because there was no media flowing on the call.

Related Commands

Command	Description
show sbc dbe addresses	Displays the H.248 control addresses and media addresses configured on DBEs.
show sbc dbe controllers	Displays the media gateway controllers and the controller address configured on each DBE.
show sbc dbe forwarder-stats	Displays the global list of statistics for the DBE forwarding process.
show sbc dbe media-flow-stats	Displays the statistics about one or more media flows collected on the DBE.
show sbc dbe signaling-flow-stats	Displays the statistics about one or more signaling flows collected on the DBE.
unexpected-source-alerting	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

show sbc dbe signaling-flow-stats

To list the signaling flow statistics collected on the data border element (DBE), use the **show sbc dbe signaling-flow-stats** command in user EXEC or privileged EXEC mode.

```
show sbc {sbc-name} dbe signaling-flow-stats [{summary | detail}] [vrf vrf-name] [{ipv4
A.B.C.D | ipv6 ipv6-address}] [port port-number]] [context {id}| termination {termination
substring}]
```

Syntax Description

<i>sbc-name</i>	Name of the session border controller (SBC) service.
summary	(Optional) Displays a summary of the signaling flow statistics, including pinhole flows, for the DBE.
detail	(Optional) Displays detailed signaling flow statistics, including pinhole flows, for the DBE.
vrf <i>vrf-name</i>	(Optional) Displays only signaling flows to or from the specified VPN routing and forwarding instance (VRF).
ipv4 <i>A.B.C.D</i>	(Optional) Displays only signaling flows to or from the specified IPv4 media IP address.
ipv6 <i>ipv6-address</i>	(Optional) Displays only signaling flows to or from the specified IPv6 media IP address.
port <i>port-number</i>	(Optional) Displays only signaling flows to or from the specified port number.
context	(Optional) Shows summary or detailed display of all pinhole flows within the context ID.
<i>id</i>	(Optional) Specifies the context ID number.
termination	(Optional) Shows summary or detailed display of pinhole flows. that match the termination substring.
<i>termination substring</i>	(Optional) Specifies the termination substring number.

Command Default

No default behavior or values are available.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	The context and termination keywords were added. New fields (Max Burst size, Delay variation tolerance, SDP string, Graceful deactivation, DiffServ Code Point, Media Loss Event, and NAT Latch Event) were added to the output display.

Usage Guidelines

When the “Media Flowing” field is reported as Yes, it either means that media has been observed flowing on the call within the media timeout period, or the call has failed over within the last media timeout period and the SBC has not yet had a chance to observe whether media is flowing or not.

Examples

The following example displays signaling and media flow pairs and additional fields added in Cisco IOS XE Release 2.2:

```
Router# show sbc global dbe signaling-flow-stats
SBC Service "global"
Media Flow:
  Context ID:          6
  Stream ID:           1
  State of Signaling Flow: Allocated
  Call Established Time: 16:53:58 UTC Feb 20 2008
  Flow Priority:       Unspecified
Side A:
  Name:                mycompany/sip4/gn/0/1/0/1/ac/1
  Reserved Bandwidth:  0 (bytes/second)
  Status:              InService
  VRF Name:            Global
  VLAN Tags(Priorities): 0(0), 0(0)
  Local Address:        202.50.2.1
  Local Port:          10000
  Remote Address:       3.0.0.3
  Remote Port:          5000
  Packets Received:     0
  Packets Sent:         0
  Packets Discarded:    0
  Data Received:        0 (bytes)
  Data Sent:            0 (bytes)
  Data Discarded:       0 (bytes)
  GM Discarded Packets: 0
  Time To Recovery:     Not known
  Media Flowing:        No
  Unexpected SrcAddr Packets: No
  Max Burst size:       0 (bytes)
  Delay variation tolerance: 0 (microseconds)
  SDP string:           m=application $ udp 0
  Graceful deactivation: No
  DiffServ Code Point:  0
  Media Loss Event:     No
  NAT Latch Event:      No
Side B:
  Name:                mycompany/sip4/gn/0/1/0/1/bb/2
  Reserved Bandwidth:  0 (bytes/second)
  Status:              InService
  VRF Name:            Global
  VLAN Tags(Priorities): 0(0), 0(0)
  Local Address:        202.50.2.1
  Local Port:          10001
  Remote Address:       3.0.0.3
  Remote Port:          5000
  Packets Received:     0
  Packets Sent:         0
  Packets Discarded:    0
  Data Received:        0 (bytes)
  Data Sent:            0 (bytes)
  Data Discarded:       0 (bytes)
  GM Discarded Packets: 0
  Time To Recovery:     Not known
  Media Flowing:        No
```

<===== additional fields for Side A

```

Unexpected SrcAddr Packets: No
Max Burst size:             0 (bytes)           <===== additional fields for side B
Delay variation tolerance:  0 (microseconds)
SDP string:                 m=application $ udp 0
Graceful deactivation:     No
DiffServ Code Point:       B8
Media Loss Event:          No
NAT Latch Event:           No

```

The following example displays detailed statistics from an IPv4 signaling flow collected on the DBE:

Router# **show sbc mySbc dbe signaling-flow-stats detail**

SBC Service "mySbc"

Media Flow:

```

Context ID:                2
Stream ID:                 1
State of Signaling Flow: Active
Call Established Time: 12:55:11 UTC Aug 11 2007
Flow Priority:              Routine
Side A:
  Name                     abc/sip/gn/0/1/0/1/ac/1
  Reserved Bandwidth:      43 (bytes/second)
  Status                   InService
  VRF Name:                Global
  VLAN Tags(Priorities):   0(0), 0(0)
  Local Address:           202.50.255.110
  Local Port:              5000
  Remote Address:          100.50.255.110
  Remote Port:             5000
  Remote Source Address Mask: 100.50.255.0/24
  Packets Received:        1344
  Packets Sent:            0
  Packets Discarded:       444
  Data Received:           885 (bytes)
  Data Sent:               0 (bytes)
  Data Discarded:          292 (bytes)
  GM Discarded Packets:    0
  Time To Recovery:        Not known
  Media Flowing:           Yes
  Unexpected SrcAddr Packets: No
  Max Burst size:          0 (bytes)
  Delay variation tolerance: 0 (microseconds)
  SDP string:              m=application $ udp 0
  Graceful deactivation:   No
  DiffServ Code Point:     0
  Media Loss Event:        No
  NAT Latch Event:         No

```

Side B:

```

Name                     abc/sip/gn/0/1/0/1/bb/2
Reserved Bandwidth:      0 (bytes/second)
Status                   InService
VRF Name:                Global
VLAN Tags(Priorities):   0(0), 0(0)
Local Address:           202.50.255.110
Local Port:              5001
Remote Address:          200.50.255.110
Remote Port:             10000
Packets Received:        1335
Packets Sent:            900
Packets Discarded:       1335

```

```

Data Received:          880 (bytes)
Data Sent:              593 (bytes)
Data Discarded:        880 (bytes)
GM Discarded Packets:   0
Time To Recovery:       Not known
Media Flowing:          No
Unexpected SrcAddr Packets: No
Max Burst size:         0 (bytes)
Delay variation tolerance: 0 (microseconds)
SDP string:             m=application $ udp 0
Graceful deactivation:  No
DiffServ Code Point:    B8
Media Loss Event:       No
NAT Latch Event:       No

```

The following example displays detailed statistics from an IPv6 signaling flow collected on the DBE:

Router# **show sbc global dbe signaling-flow-stats detail**

SBC Service "global"

Media Flow:

```

Context ID:          2
Stream ID:           1
State of Signaling Flow: Allocated
Call Established Time: 12:55:11 UTC Aug 11 2007
Flow Priority:       Routine
Side A:
  Name                abc/sip/gn/0/1/0/1/ac/1
  Reserved Bandwidth: 23 (bytes/second)
  Status              InService
  VRF Name:           Global
  VLAN Tags(Priorities): 0(0), 0(0)
  Local Address:      1111:2222:3333:4444:5555:6666:7777:3331
  Local Port:         5000
  Remote Address:      Not known
  Remote Port:         Not known
  Remote Source Address Mask: 2222:1111:1111:2222:3333:4444:5555:7777/48
  Packets Received:    0
  Packets Sent:        0
  Packets Discarded:   0
  Data Received:       0 (bytes)
  Data Sent:           0 (bytes)
  Data Discarded:      0 (bytes)
  GM Discarded Packets: Not known
  Time To Recovery:    Not known
  Media Flowing:       No
  Unexpected SrcAddr Packets: No
  Max Burst size:      0 (bytes)
  Delay variation tolerance: 0 (microseconds)
  SDP string:          m=application $ udp 0
  Graceful deactivation: No
  DiffServ Code Point: B8
  Media Loss Event:    No
  NAT Latch Event:     No

```

Side B:

```

Name                abc/sip/gn/0/1/0/1/bb/2
Reserved Bandwidth: 0 (bytes/second)
Status              InService
VRF Name:           Global
VLAN Tags(Priorities): 0(0), 0(0)
Local Address Mask: 2222:1111:1111:2222:3333:4444:5555:7777/48

```



```

Local Port: 0
Remote Address: 3333:1111:1111:2222:3333:4444:5555:7777
Remote Port: 10000
Packets Received: 0
Packets Sent: 0
Packets Discarded: 0
Data Received: 0 (bytes)
Data Sent: 0 (bytes)
Data Discarded: 0 (bytes)
GM Discarded Packets: 0
Time To Recovery: Not known
Media Flowing: No
Unexpected SrcAddr Packets: No
Max Burst size: 0 (bytes)
Delay variation tolerance: 0 (microseconds)
SDP string: m=application $ udp 0
Graceful deactivation: No
DiffServ Code Point: B8
Media Loss Event: No
NAT Latch Event: No

```

The following example shows summary statistics collected for signaling flows on the DBE:

Router# **show sbc mySbc dbe signaling-flow-stats summary**

```

SBC Service "mySbc"
Context ID 1          Stream ID 1
Side A:               Name abc/sip6/gn/0/1/0/1/ac/1      Media Flowing: Yes
  Local Address/Port: 1:100:1:1:1:1:1:1/5060
  Remote Address/Port: 2:100:1:1:1:1:1:1/5000
  Status:              In Service
Side B:               Name abc/sip6/gn/0/1/0/1/bb/2      Media Flowing: Yes
  Local Address/Port: 2:100:1:1:1:1:1:1/5000
  Remote Address/Port: 3:100:1:1:1:1:1:1/5060
  Status:              In Service
Context ID 2          Stream ID 1
Side A:               Name abc/sip4/gn/0/1/0/1/ac/5      Media Flowing: Yes
  Local Address/Port: 202.100.1.1/5000
  Remote Address/Port: 100.100.1.1/5000
  Status:              In Service
Side B:               Name abc/sip4/gn/0/1/0/1/bb/6      Media Flowing: Yes
  Local Address/Port: 202.100.1.1/5001
  Remote Address/Port: 200.100.1.1/5000
  Status:              In Service

```

Table 6 *show sbc dbe signaling-flow-stats Field Descriptions*

Field	Description
Context ID	Context ID to which the flow is associated.
Stream ID	Stream ID.

Table 6 *show sbc dbe signaling-flow-stats Field Descriptions (continued)*

Field	Description
State of Signaling Flow	Flow state (Active, Allocated, or Unknown). <ul style="list-style-type: none"> Active—DBE has programmed the flow pair and the media has started flowing in at least one direction. Allocated—DBE has programmed the flow pair, but no media has started to flow. Unknown—DBE has not yet been given enough information by the controller to be able to program the flow pair.
Call Established Time	Call established time in the format 23:51:29 UTC Jun 21 2007.
Flow Priority	Priority of the call (Routine or Urgent).
Side A	Information for the initiating side of the call
Side B	Information for the terminating side of the call
Name	Name of the flow.
Reserved Bandwidth	Bandwidth reserved for the call in bytes per second.
Status	Status is InService or OutofService. InService—Flow on this side is in service. OutofService—No media is forwarded.
VRF Name	Either the VRF name, or “Global” when there is no VRF.
VLAN Tags (Priorities)	VLAN tags and Ethernet priority information.
Local Address	Local address on the DBE on which packets are received for this side of the call.
Local Port	Local port on the DBE on which packets are received for this side of the call.
Remote Address	Address of the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Port	Port on the remote endpoint from which packets are expected to be sent for this side of the call.
Remote Source Address Mask	If specified, all packets matching the Remote Source Address Mask are classified as belonging to this flow rather than just those matching the full remote and port.
Packets Received	Number of packets received from the remote endpoint.
Packets Sent	Number of packets forwarded to the remote endpoint.
Packets Discarded	Number of packets dropped (due to bandwidth policing, for example).
Data Received	Number of bytes of data received from the remote endpoint.
Data Sent	Number of bytes of data forwarded to the remote endpoint.
Data Discarded	Number of bytes of data dropped (due to bandwidth policing, for example).

Table 6 *show sbc dbe signaling-flow-stats Field Descriptions (continued)*

Field	Description
GM Discarded Packets	This counter is always set to zero because it is not currently implemented. It will be the number of data packets received from the remote end point and discarded locally because of source address/port filtering.
Time To Recovery	The tsc/ttr value from Termination State Control (TSC) package, in milliseconds.
Media Flowing	Indicates whether packets are flowing from the endpoint.
Unexpected SrcAddr Packets	<p>If unexpected-source-alerting is switched on with the unexpected-source-alerting command, this counter records the number of alerts generated for the flow when media packets for a call are received from an unexpected source address and port.</p> <p>An unexpected source event happens when a packet is received, matched to a flow (but not by a full 5-tuple comparison), and found to have come from the wrong remote address.</p>
Max Burst size	The maximum burst size (tman/mbs) associated with the Tman package.
Delay variation tolerance	The delay variation tolerance (tman/dvt) associated with the Tman package. Defines the delay variation tolerance for the stream in tenths of microseconds when enforcing the PDR value in the first leaky bucket.
SDP string	The SDP string is that present on the H.248 ADD request to provision the call.
Graceful deactivation	Description to be added.
DiffServ Code Point	The Diffserv Code point is the (DSCP value) provided on the H.248 request to mark the media packets. This reflects the ds/dscp parameters.
Media Loss Event	Media Loss Event is “Yes” if the flow has the nt/qualert subscription.
NAT Latch Event	The NAT Latch Event is “Yes” if the flow has adr/rsac subscribed.

Related Commands

Command	Description
show sbc dbe flow-stats	Lists all flow statistics, both signaling and media flows, collected on the data border element (DBE).
show sbc dbe addresses	Displays the H.248 control addresses and media addresses configured on DBEs.
show sbc dbe controllers	Displays the media gateway controllers and the controller address configured on each DBE.
show sbc dbe forwarder-stats	Displays the global list of statistics for the DBE forwarding process.

show sbc dbe signaling-flow-stats

Command	Description
show sbc dbe media-stats	Displays general DBE statistics. These statistics do not include data from active calls.
show sbc dbe media-flow-stats	Displays the statistics about one or more media flows collected on the DBE.
unexpected-source-alerting	Enables the generation of alerts when media packets for a call are received from an unexpected source address and port.

termination-id rootidname

To configure the termination ID rootidname string in the ServiceChange Notification for Interface Status Change feature, use the **termination-id rootidname** command in VDBE configuration mode. To configure a default value of “Cisco” for the termination ID rootidname, use the **no** form of this command.

termination-id rootidname {*name*}

no termination-id rootidname {*name*}

Syntax Description	<p><i>name</i></p> <p>Name of the termination ID namestring in the ServiceChange Notification for Interface Status Change feature.</p> <p>The termination ID rootidname string is in the first tier or root of the nine-tier termination ID. The termination ID namestring is usually the company's name.</p>
---------------------------	---

Command Default	The default value of the termination ID rootidname is “Cisco.”
------------------------	--

Command Modes	VDBE configuration (config-sbc-dbe-vdbe)
----------------------	--

Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE Release 2.2</td><td>This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</td></tr> </table>	Release	Modification	Cisco IOS XE Release 2.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Release	Modification				
Cisco IOS XE Release 2.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.				

Usage Guidelines	<p>This command is used in conjunction with the ServiceChange Notification for Interface Status Change feature. See the <i>Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model</i> for more information at:</p>
-------------------------	--

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbc/2_xe/sbc_2_xe_book.html

The ServiceChange Notification for Interface Status Change feature enables the media gateway (MG) to generate a ServiceChange H.248 notification to the media gateway controller (MGC) containing the termination ID of the physical interface on the data border element (DBE) when the interface experiences status changes. The termination ID is a nine-tier namestring associated with a pinhole or pair of terminations. The termination ID rootidname is in the first tier or root of the nine-tier termination ID.

You can use the **termination-id rootidname** command to configure the termination ID rootidname as a namestring such as “xyzcompany.” Then in that case, the MG reports “xyzcompany/*/*/*/<interface-id>/*/*/*” to the MGC with the ServiceChange notification.

The default value of the termination ID rootidname is “Cisco.” Therefore, if the command is not issued or **no termination-id rootidname** is issued, then “Cisco/*/*/*/<interface-id>/*/*/*” is reported to the MGC with the ServiceChange.

■ termination-id rootidname

Examples

The following example enters into VDBE configuration modes and configures “xyzcompany” as the path name of the termination ID rootidname string when the MG reports a ServiceChange notification to the MGC due to an interface status change:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# termination-id rootidname xyzcompany
Router(config-sbc-dbe-vdbe)# end
```

Related Commands

Command	Description
sbc interface-id	Maps a physical interface on the data border element (DBE) to the physical-interface-id contained in the termination ID for the purpose of notifying the signaling border element (SBE) when a physical interface has experienced a state change

test sbc profile-to-editor sip

To display the editor that is inherited from a Session Initiation Protocol (SIP) profile when the SIP profile is enabled instead of the SIP editor, use the **test sbc profile-to-editor sip** command in the privileged EXEC mode.

test sbc profile-to-editor sip *profile-type profile-name*

Syntax Description

<i>profile-type</i>	Type of SIP profile. It can be one of the following values: <ul style="list-style-type: none">body-profiledefault-profilesheader-profilemethod-profileoption-profileparameter-profile
<i>profile-name</i>	Name of SIP profile.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

We recommend that you enable SIP editor instead of SIP profile. Customers who have already deployed SIP profile can use the **test sbc profile-to-editor sip** command during the transition from SIP profile to SIP editor.



Note


The **test sbc profile-to-editor sip** command only displays the editor that is inherited from the SIP profile for customers' reference when migrating from SIP profile to SIP editor. Customers must configure the editor manually using the **sip editor-type** command.

Examples

The following is a sample output of the **test sbc profile-to-editor sip** command:

```
Router# test sbc profile-to-editor sip header-profile dtmf-notify

whitelist
  header event entry 1
    action pass
  header call-info entry 1
  action pass
```

 test sbc profile-to-editor sip**Related Commands**

Command	Description
sip <i>editor-type</i>	Sets a default editor type to be applied to an adjacency that has not been explicitly set.

tmax baseroot

To configure the T-MAX timer to use the baseroot package value, use the **tmax baseroot** command in VDBE configuration mode. To restore the default behavior, use the **no** form of this command.

tmax baseroot

no tmax

Syntax Description This command has no arguments or keywords.

Command Default The default behavior is that T-MAX timer uses the value configured by the **tmax-timer** command.

Command Modes VDBE configuration (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.6.2	The command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines This command configures the T-MAX timer to choose the smaller value of either normalMGCExecutionTime or MGCPProvisionalResponseTimerValue timer that is specified by the media gateway controller (MGC) root package.

Examples The following example shows how the **tmax baseroot** command is used to configure the T-MAX timer in the VDBE configuration mode:

```
Router# configure terminal
Router# sbc sbc dbe
Router(config-sbc-dbe) # vdbe global
Router(config-sbc-dbe-vdbe) # tmax baseroot
```

Related Commands	Command	Description
	tmax-timer	Defines the value of the T-MAX timer, which limits the maximum delay of retransmissions by the H.248 stack on a data border element (DBE) when sending messages to the MGC.
	h248-association-time out	Configures the DBE to reset the H.248 association with the MGC when the controller does not respond to any event notification.
	h248-inactivity-duration	Defines the duration of the provisioned inactivity timer.
	transaction-pending	Enables transaction pending on the DBE by changing the number of H.248 transactions before a request in process times out.

tmax-timer

To define the value of the T-MAX timer, which limits the maximum delay of retransmissions by the H.248 stack on a data border element (DBE) when sending messages to the media gateway controller (MGC) over an unreliable transport media (such as the User Datagram Protocol [UDP]), use the **tmax-timer** command in VDBE configuration mode. To reconfigure the default value of 10 seconds, use the **no** form of the command.

tmax-timer {*timer-value*}

no tmax-timer

Syntax Description	<i>timer-value</i>	Value of the maximum delay in seconds. The range is 5 to 50.
--------------------	--------------------	--

Command Default	The default is 10 seconds if the command is not configured, or the no tmax-timer command is issued.
-----------------	--

Command Modes	VDBE configuration (config-sbc-dbe-vdbe)
---------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	When setting the T-MAX value, consider the maximum propagation delay in your network.
------------------	---

Examples	The following example configures the DBE to use a T-MAX timer value of 20 seconds:
----------	--

```
Router (config)# sbc mySbc dbe
Router (config-sbc-dbe)# vdb
Router (config-sbc-dbe-vdbe)# tmax-timer 20
Router (config-sbc-dbe-vdbe)# end
```

transaction-pending

To enable transaction pending on the Data Border Element (DBE) by changing the number of H.248 transactions before a request in process times out, use the **transaction-pending** command in VDBE configuration mode. To re-instate the H.248 transaction limit for requests in process, use the **no** form of this command.

transaction-pending [*response-limit*]

no transaction-pending [*response-limit*]

Syntax Description	<i>response-limit</i>	Indicates the maximum number of pending responses or transactions that can be produced before a request is considered to have timed out. The range is 1 to 100. The default is 10 responses or transactions.
---------------------------	-----------------------	---

Command Default	The default is no transaction-pending .
------------------------	--

Command Modes	VDBE configuration (config-sbc-dbe-vdbe)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines	Enabling transaction pending with this command allows the DBE to tell the Signaling Border Element (SBE) that some H.248 transactions are actively being processed and have not completed. Transaction pending is used to prevent the sender from assuming the request was lost when the transaction needed more time to complete.
-------------------------	--

The notification allows some H.248 requests, especially wildcard audits, to complete the response or processing without timing out when they exceed the ten transaction limit set by the H.248.1 version 3 section 8.2.3 protocol for processing time for H.248 transactions.

Examples	The following example sets a timeout limit for H.248 requests to 50 transactions for requests in process:
-----------------	---

```
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# h248-version 3
Router(config-sbc-dbe-vdbe)# h248-napt-package napt
Router(config-sbc-dbe-vdbe)# h248-association-timeout
Router(config-sbc-dbe-vdbe)# transaction-pending 50
Router(config-sbc-dbe-vdbe)# end
```

transport (session border controller)

To configure a data border element (DBE) to use either UDP or TCP for H.248 control signaling with the specified H.248 controller and to configure the Interim Authentication Header (IAH) to authenticate and check the integrity of packets, use the **transport** command in Controller H.248 configuration mode. To remove the configuration, use the **no** form of this command.

transport {udp | tcp} [interim-auth-header] [ah-md5-hmac | ah-sha-hmac]

no transport

Syntax Description	
udp	Specifies UDP transport for H.248 signaling with the H.248 controller. UDP is the default if the transport command is not used.
tcp	Specifies TCP transport for H.248 signaling with the H.248 controller.
interim-auth-header	(Optional) Specifies the H.248 controller should insert the interim authentication header into the H.248 messages to authenticate packets and provide security. If you specify the interim-auth-header keyword, but do not specify either ah-md5-hmac or ah-sha-hmac type of authentication, then the DBE uses zero authentication where the interim authentication header is inserted in the packet and all fields in the IAH header are set to zeroes. The DBE checks the packet syntactically, however, the DBE does not authenticate whether there is an IAH header or if it's correct.
ah-md5-hmac	Specifies the DBE uses for packet authentication the hashing scheme, HMAC-MD5 (Hashing for Message Authentication-Message Digest 5). Enters into IAH Key configuration mode. MD5 produces a 128 bit hash value. If you specify a hashing scheme, you need to configure inbound and outbound options for incoming and outgoing packets, as well as specify the Security Parameters Index (SPI) and hex-key. See the inbound and outbound commands for more details.
ah-sha-hmac	Specifies the DBE uses for packet authentication the hashing scheme, HMAC-SHA (Hashing for Message Authentication-Secure Hash Algorithm). Enters into IAH Key configuration mode. SHA-1 produces a message digest that is 160 bits long. If you specify a hashing scheme, you need to configure inbound and outbound options for incoming and outgoing packets, as well as specify the Security Parameters Index (SPI) and hex-key. See the inbound and outbound commands for more details.

Command Default If the **transport** command is not specified, UDP transport is used for H.248 signaling.

Command Modes Controller H.248 configuration (config-sbc-dbe-vdbe-h248)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	The ah-md5-hmac and ah-sha-hmac keywords were added.

Usage Guidelines

The **transport (session border controller)** command is used in conjunction with the **inbound** and **outbound** commands. The three commands are used together to enable Interim Authentication Header (IAH) authentication of inbound and outbound call packets. If you specify a hashing scheme (**ah-md5-hmac** or **ah-sha-hmac** authentication) using the **transport (session border controller)** command, you need to configure incoming and outgoing call packets using both **inbound** and **outbound** commands. The **inbound** and **outbound** commands are used to specify the Security Parameters Index (SPI) and hex-key.

MD5 hashing is faster to calculate, but provides less secure authentication than SHA hashing does. The hash calculation includes a synthesized IP header consisting of a 32 bit source IP address, a 32 bit destination address, and a 16 bit UDP or TCP destination port encoded as 20 hexadecimal digits.

For the MD5 or SHA hashing scheme to work, both inbound and outbound SPI need to be configured. If only the inbound or outbound SPI key or neither inbound or outbound SPI key is configured, the authentication reverts back to zero authentication and the DBE issues a warning message “Both inbound and outbound keys must be configured to enable authentication.” In this event, the DBE sets all fields in the IAH header to zeroes and accepts any IAH without authentication.


Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, creates an H.248 controller with index 1, enters into Controller H.248 configuration mode, and configures the H.248 controller to use TCP as the transport:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdb
Router(config-sbc-dbe-vdb)# controller h248 1
Router(config-sbc-dbe-vdb-h248)# transport tcp
Router(config-sbc-dbe-vdb-h248)# end
```

The following example shows you how to configure the DBE to specify TCP for H.248 control signaling, and to configure the IAH to use the HMAC-SHA hashing scheme, set the inbound Security Parameters Index (SPI) to 300 and the outbound SPI to 400, and hash key to “myInboundKey45” and “myOutboundKey89” respectively:

```
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdb global
Router(config-sbc-dbe-vdb)# h248-version 3
Router(config-sbc-dbe-vdb)# h248-napt-package napt
Router(config-sbc-dbe-vdb)# local-port 2970
Router(config-sbc-dbe-vdb)# control-address h248 ipv4 200.50.1.40
Router(config-sbc-dbe-vdb)# controller h248 2
Router(config-sbc-dbe-vdb-h248)# remote-address ipv4 200.50.1.254
Router(config-sbc-dbe-vdb-h248)# remote-port 2970
Router(config-sbc-dbe-vdb-h248)# transport tcp interim-auth-header ah-sha-hmac
Router(config-sbc-dbe-vdb-h248-iah)# inbound 300 myInboundKey45
Router(config-sbc-dbe-vdb-h248-iah)# outbound 400 myOutboundKey89
Router(config-sbc-dbe-vdb-h248)# exit
Router(config-sbc-dbe-vdb)# attach-controllers
```

 transport (session border controller)**Related Commands**

Command	Description
inbound	Configures inbound call packets to use a specific Security Parameters Index (SPI) to identify the security association to which an incoming packet is bound when the Interim Authentication Header (IAH) is enabled.
outbound	Configures outbound call packets to use a specific Security Parameters Index (SPI) to identify the security association to which an outgoing packet is bound when the Interim Authentication Header (IAH) is enabled.

unexpected-source-alerting

To enable the generation of alerts when media packets for a call are received from an unexpected source address and port, use the **unexpected-source-alerting** command in VDBE configuration mode. To disable these alerts, use the **no** form of this command.

unexpected-source-alerting

no unexpected-source-alerting

Syntax Description This command has no arguments or keywords.

Command Default If the **unexpected-source alerting** command is not specified, unexpected source alerting is disabled.

Command Modes VDBE configuration (config-sbc-dbe-vdbe)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **unexpected-source-alerting** command should be enabled only on trusted networks, where any occurrence of packets from an unexpected source might indicate a threat to network security.

Alerts on the same flow and the total number of alerts reported at any one time are both rate-limited to ensure management systems are not flooded with reports. (As a result, 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 session border controller (SBC) function; SBC simply serves as the messenger to notify you of the existence of the rogue packets.

Any and all packets from unexpected sources are dropped.

Examples

The following example creates a data border element (DBE) service on an SBC called “mySbc,” enters into SBC-DBE configuration and VDBE configuration modes, and enables the generation of alerts when unexpected source address packets are received by a virtual data border element (vDBE):

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdb
Router(config-sbc-dbe-vdbe)# unexpected-source-alerting
Router(config-sbc-dbe-vdbe)# end
```

vdb

To enter into VDBE configuration mode, use the **vdb** command in SBC-DBE configuration mode. To delete the entire virtual data border element (vDBE) from the running configuration, use the **no** form of this command.

vdb [**global**]

no vdb [**global**]

Syntax Description

global	(Optional) The name of the vDBE that is configured. Only one vDBE named “global” is supported and can be configured. The vDBE name must be “global.”
---------------	---

Command Default

The default is global if the vDBE name is not specified.

Command Modes

SBC-DBE configuration (config-sbc-dbe)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Only one vDBE named “global” is supported. This means that DBE resources cannot be partitioned and the DBE can only connect to a single SBE at any one time.

The vDBE name is not required. If the vDBE name is not specified, the default name is “global.”

Use the **sbc dbe** command to enter into SBC-DBE configuration mode before using the **vdb** command. This command enters a submode to set vDBE parameters.

Examples

The following example creates a DBE service on an SBC called “mySbc,” enters into SBC-DBE configuration mode, and enters into VDBE configuration mode with a configured vDBE named “global”:

```
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdb global
Router(config-sbc-dbe-vdb)#
```

Related Commands

Command	Description
sbc dbe	Creates the data border element (DBE) service on a session border controller (SBC) and enters into SBC-DBE configuration mode.