# Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model

Cisco IOS XE Release 3.3S
March 29, 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

Customer Order Number: OL-15421-06

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) Configuration Guide: Distributed Model*

# CONTENTS

# Preface

This preface describes the objectives and organization of this guide and explains how to find additional information on related products and services. This preface contains the following sections:

## Guide Revision History

The Guide Revision History records technical changes to this guide. The table shows the software release number and guide revision number for the change, the date of the change, and a brief summary of the change.

| Release No. | Revision | Date | Change Summary |
|---|---|---|---|
| 3.1S | OL-15421-06 | July 30, 2010 | This guide was updated with a new feature: ETSI Ia Profile on SBC |
| 2.6.2 | OL-15421-05 | July 8, 2010 | This guide was updated with a new feature: H.248 Timers |
| 2.6 | OL-15421-04 | February 26, 2010 | This guide was updated with new features: Optional Tman Bandwidth Parameter Policing, Return Local and Remote Descriptors in H.248 Reply, and SBC End Point Switching. |
| 2.4.1 | OL-15421-03 | August 25, 2009 | The name of this guide was changed from *Cisco IOS XE Integrated Session Border Controller Configuration Guide for the Cisco ASR 1000 Series Aggregation Services Routers* to *Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model.* |

| | | | |
|---|---|---|---|
| 2.3 | OL-15421-03 | February 27, 2009 | This guide was updated with the In-Service Provisioning of H.248 Controllers feature; RTCP maximum burst size policing parameter feature, and number of active calls audited with a huge buffer size information. |
| 2.2 | OL-15421-02 | October 3, 2008 | This guide was updated with new features: Full Support for Wildcard Response, H.248 Protocol—Acknowledgment Support for Three-Way Handshake, H.248 ServiceChange Handoff, Improved Media Timeout Detection, Interim Authentication Header Full Support, and IPsec Pinhole Support—Twice NAT for IPv4 and No NAT for IPv6. |
| 2.1 | OL-15421-01 | May 5, 2008 | This guide was first published. |

# Objectives

This guide describes the Cisco Unified Border Element (SP Edition) functions, features, restrictions, and configuration tasks for the Cisco ASR 1000 Series Aggregation Services Routers. It is not intended as a comprehensive guide to all of the software features that can be run using the Cisco ASR 1000 Series Routers, but only the Cisco Unified Border Element (SP Edition) software specific to these Routers.

For information on general Cisco IOS software features that are also available on the Cisco ASR 1000 Series Routers, see the feature module or the technology guide for that software feature.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this guide as the session border controller (SBC).

# Intended Audience

This guide is intended for the following people:

- Experienced service provider administrators
- Cisco telecommunications management engineers
- Customers who use and manage Cisco ASR 1000 Series Routers

# Organization

This guide contains the following chapters:

| Chapter | Title | Description |
|---|---|---|
| 1 | Cisco Unified Border Element (SP Edition) Distributed Model Overview | Describes general architecture, list of supported features, and deployment scenario. |
| 2 | Configuring the Cisco Unified Border Element (SP Edition) Distributed Model | Describes configuration tasks for data border element (DBE) functionality, prerequisites, restrictions, configuration examples, and the Cisco H.248 profile. |
| 3 | DTMF Interworking on the Cisco Unified Border Element (SP Edition) Distributed Model | Describes support of dual-tone multifrequency (DTMF) to interwork between two end points that do not use the same way of relaying DTMF tones. |
| 4 | Media Address Pools | Describes how to configure the DBE address by address pool, with or without port range, and define class of service for each port range. |
| 5 | Quality of Service and Bandwidth Management | Describes features the DBE has to enhance Quality of Service (QoS). |
| 6 | H.248 Packages—Signaling and Control | Describes support of standard H.248 packages. |
| 7 | H.248 Services—Signaling and Control | Describes different H.248 services and controlling functions of the DBE. |
| 8 | ETSI Ia Profile on SBC | Describes the support of ETSI Ia Profile on SBC. |
| 9 | Security in Cisco Unified Border Element (SP Edition) Distributed Model | Describes various high security features and policing of incoming data. |
| 10 | Topology Hiding | Describes the various features by which Cisco Unified Border Element (SP Edition) protects the network by hiding the network address and names for both the customer and core network sides, and properly translating the IP address and port when a user connects to the outside network. |
| 11 | High-Availability Support | Describes hardware and software redundancy support for Cisco Unified Border Element (SP Edition) on the Cisco ASR 1000 Series Routers. |
| 12 | Quality Monitoring and Statistics Gathering | Describes DBE support for monitoring events, and generation of event notification, correct billing and call usage records. |

# Related Documentation

This section refers you to other documentation that might also be useful as you configure your Cisco ASR 1000 Series Routers. The documentation listed below is available on Cisco.com.

## Cisco ASR 1000 Series Router Documentation

For information on Cisco Unified Border Element (SP Edition) commands, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

For information on the Cisco Unified Border Element (SP Edition) unified model, see:

- *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* at:

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/2_xe/sbcu_2_xe_book.html

- *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at:

  http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

For information on new Cisco ASR 1000 Series Router commands and commands in existing Cisco IOS features, see the Cisco IOS command reference books on Cisco.com. For information about Cisco IOS commands in general, you can also use the Command Lookup Tool at:

http://tools.cisco.com/Support/CLILookup or a Cisco IOS master commands list.

For Quick Start guides and installation documentation for the Cisco ASR 1000 Series Router, see the hardware documentation at:

http://www.cisco.com/en/US/products/ps9343/prod_installation_guides_list.html

For information on new software features, see *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*, new feature module documents, and the *Cisco IOS XE release notes*.

For further information, see the Cisco ASR 1000 Series Aggregation Services Routers Documentation Roadmap at:

http://www.cisco.com/en/US/docs/routers/asr1000/roadmap/asr1000rm.html

## Cisco IOS XE Release Software Publications

Documentation pertaining to Cisco IOS XE 3S configuration guides and feature modules can be found at:

http://www.cisco.com/en/US/products/ps11174/tsd_products_support_series_home.html

Documentation pertaining to Cisco IOS XE, Release 2 configuration guides and feature modules can be found at:

http://www.cisco.com/en/US/products/ps9587/tsd_products_support_configure.html

# Document Conventions

This documentation uses the following conventions:

| Convention | Description |
|---|---|
| ^ or **Ctrl** | The ^ and **Ctrl** symbols represent the Control key. For example, the key combination **^D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive. |
| *string* | A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP *community* string to *public*, do not use quotation marks around the string or the string will include the quotation marks. |

Command syntax descriptions use the following conventions:

| Convention | Description |
|---|---|
| **bold** | Bold text indicates commands and keywords that you enter exactly as shown. |
| *italics* | Italic text indicates arguments for which you supply values. |
| [x] | Square brackets enclose an optional element (keyword or argument). |
| \| | A vertical line indicates a choice within an optional or required set of keywords or arguments. |
| [x \| y] | Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice. |
| {x \| y} | Braces enclosing keywords or arguments separated by a vertical line indicate a required choice. |

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

| Convention | Description |
|---|---|
| [x {y \| z}] | Braces and a vertical line within square brackets indicate a required choice within an optional element. |

Examples use the following conventions:

| Convention | Description |
|---|---|
| `screen` | Examples of information displayed on the screen are set in Courier font. |
| **`bold screen`** | Examples of text that you must enter are set in Courier bold font. |
| < > | Angle brackets enclose text that is not printed to the screen, such as passwords. |
| ! | An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.) |
| [ ] | Square brackets enclose default responses to system prompts. |

The following conventions are used to attract the attention of the reader:

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Note** Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

**Tip** Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

# Cisco Unified Border Element (SP Edition) Distributed Model Overview

This chapter presents an overview of the Cisco Unified Border Element (SP Edition), supported features, and deployment of Cisco Unified Border Element (SP Edition) on the Cisco ASR 1000 Series Routers.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

## Contents

## General Overview

Cisco Unified Border Element (SP Edition) is integrated with other features on the Cisco ASR 1000 Series Routers without requiring additional application-specific hardware, such as service blades. Cisco Unified Border Element (SP Edition) is integrated with Layer 2 and Layer 3 services, such as security, QoS, IP Multicast, that eliminate the need to create an overlay network of standalone SBC appliances. With Integrated SBC, SBC functionality and routing functionality both reside on the Cisco ASR 1000 Series Router. The integration also allows SBC to build on the security and admission control features and virtual private network (VPN) awareness of the Cisco ASR 1000 Series Routers.

In general, session border controllers are used as key components in interconnecting Voice over IP (VoIP) and multimedia networks of different enterprise customers and service providers. SBCs are deployed at the edge of networks to meet the need for secure, intelligent border element functions. Using SBCs, the end user can make voice and video calls to another end user without being concerned about protocols, network reachability, or safety of the network.

The SBC enables direct IP-to-IP interconnect between multiple administrative domains for session-based services providing protocol interworking, security, and admission control and management. The SBC is a session-aware device that controls access to VoIP and other types of primarily media-related networks. A primary purpose of an SBC is to protect the interior of the network from excessive call load and malicious traffic.

The SBC functions break down into two logically distinct areas:

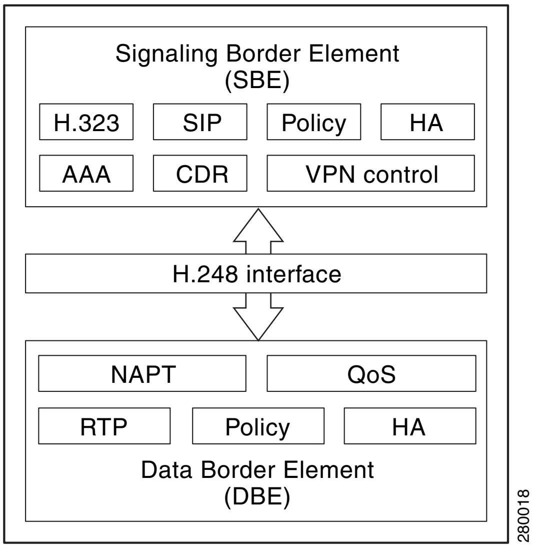
- The signaling border element (SBE) function. SBEs may support functions that include interworking between various signaling protocols such as H.323 and Session Initiation Protocol (SIP), call admission control, advanced routing policy management, network attack detection, or call billing using RADIUS or DIAMETER. As part of the call admission control function, an SBE informs the data border element (DBE) of the various quality of service (QoS) and Network Address and Port Translation (NAPT) requirements for the call. An SBE typically controls one or more media gateways.

  An SBE may be known as a media gateway controller (MGC).
- The data border element (DBE) controls access of media packets to the network, provides differentiated services and quality of service (QoS) for different media streams, and prevents service theft. The DBE consists of a set of data path functions and responds to the requests made by the SBE to open pinholes, taking into account the specified Network Address Translation (NAT)/firewall traversal and QoS requirements.

The distributed model of the Cisco Unified Border Element (SP Edition) implements the DBE function on the Cisco ASR 1000 Series Aggregation Services Routers. A table of DBE-supported features is listed in Table 1-1.

Figure 1-1 shows an example of SBC high-level architecture; your SBC architecture may differ.

***Figure 1-1 Example of SBC High-Level Architecture***



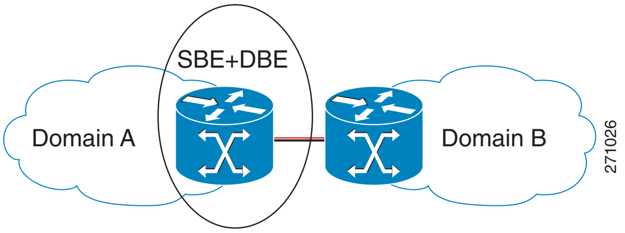
# Distributed and Unified Models

The SBC can operate in two modes or models—unified and distributed.

- In the unified model, both the SBE and DBE logical entities co-exist on the same network element.
- In the distributed model, the SBE and the DBE entities reside on different network elements. Logically, each of the SBE entities could control multiple DBE elements. The DBE is controlled by one SBE at any one time.

Figure 1-2 illustrates the Unified SBC model.

*Figure 1-2 Unified SBC Model*



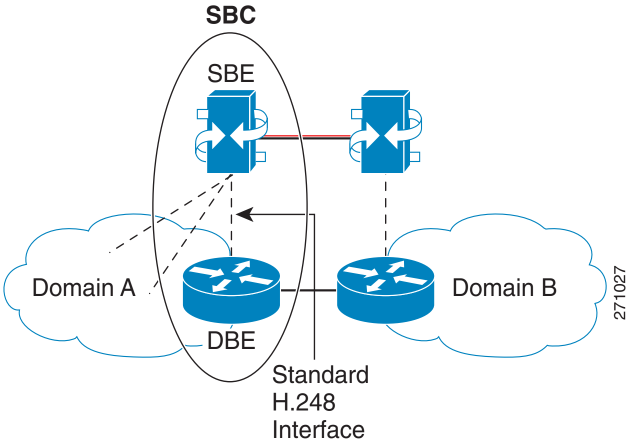
Cisco Unified Border Element (SP Edition) can run under the distributed model and provide the DBE functionality.

The distributed model offers advantages over the unified model:

- Scalable to a larger number of sessions.
- Operational advantages, because the SBE can be upgraded or serviced separately from the DBE.
- The distributed model aligns well with typical voice deployments where the SBE can be co-located with part of the call agent.
- The many-to-many interface offers capability to load share and balance across networks. Operators have the flexibility to optimize on loading of the SBE or DBE.

Figure 1-3 illustrates the Distributed SBC model.

*Figure 1-3 Distributed SBC Model*



# Supported Features on the Cisco Unified Border Element (SP Edition) Distributed Model

The supported features roadmap lists the features documented in this guide and provides links to where they are documented. Any related configuration commands for a feature are listed and documented in *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

**Note** Table 1-1 lists only the Cisco IOS XE software releases that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1-1 lists features and associated commands that are supported on the Cisco Unified Border Element (SP Edition) DBE deployment on the Cisco ASR 1000 Series Routers.

*Table 1-1 Supported Features on Cisco Unified Border Element (SP Edition) Distributed Model*

| Release | Feature Name | Related SBC Commands | Chapter Where Documented |
|---|---|---|---|
| Cisco IOS XE Release 2.1 | Billing and Call Detail Records | None. | Chapter 12, "Quality Monitoring and Statistics Gathering" |
| Cisco IOS XE Release 2.1 | DBE Signaling Pinhole Support | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | DBE Status Notification | None. | Chapter 12, "Quality Monitoring and Statistics Gathering" |
| Cisco IOS XE Release 2.1 | DSCP Marking and IP Precedence Marking | None. | Chapter 5, "Quality of Service and Bandwidth Management" |
| Cisco IOS XE Release 2.1 | DTMF Interworking on the Cisco Unified Border Element (SP Edition) Distributed Model | **dtmf-duration** | Chapter 3, "DTMF Interworking on the Cisco Unified Border Element (SP Edition) Distributed Model" |
| Cisco IOS XE Release 2.1 | Enabling the Optional H.248 Packages | **package** | Chapter 7, "H.248 Packages—Signaling and Control" |
| Cisco IOS XE Release 2.1 | Enhanced Event Notification and Auditing | **h248-association-timeout**<br>**h248-event-storage**<br>**h248-preserve-gates** | Chapter 12, "Quality Monitoring and Statistics Gathering" |

*Table 1-1 Supported Features on Cisco Unified Border Element (SP Edition) Distributed Model (continued)*

| Release | Feature Name | Related SBC Commands | Chapter Where Documented |
|---|---|---|---|
| Cisco IOS XE Release 2.1 | Extension to H.248 Audit Support | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | Extension to H.248 Termination Wildcarding Support | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | Firewall (Media Pinhole Control) | None. | Chapter 9, "Security in Cisco Unified Border Element (SP Edition) Distributed Model" |
| Cisco IOS XE Release 2.1 | Flexible Address Prefix Provisioning | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | H.248 Address Reporting Package | None. | Chapter 9, "Security in Cisco Unified Border Element (SP Edition) Distributed Model" |
| Cisco IOS XE Release 2.1 | H.248 Gate Information (Ginfo) Package Becomes Optional | None. | Chapter 7, "H.248 Packages—Signaling and Control" |
| Cisco IOS XE Release 2.1 | H.248 Network Package Quality Alert Event and Middlebox Pinhole Timer Expired Event | **h248-media-alert-event** | Chapter 12, "Quality Monitoring and Statistics Gathering" |
| Cisco IOS XE Release 2.1 | H.248 Segmentation Package Support | **package segment max-pdu-size**<br>**package segment seg-timer-value**<br>**show sbc dbe controllers** | Chapter 7, "H.248 Packages—Signaling and Control" |
| Cisco IOS XE Release 2.1 | H.248 Session Failure Reaction Package | None. | Chapter 7, "H.248 Packages—Signaling and Control" |
| Cisco IOS XE Release 2.1 | H.248 Termination State Control Package | **show sbc dbe media-flow-stats**<br>**show sbc dbe signaling-flow-stats** | Chapter 7, "H.248 Packages—Signaling and Control" |
| Cisco IOS XE Release 2.1 | H.248 Traffic Management Package Support | None. | Chapter 5, "Quality of Service and Bandwidth Management" |

*Table 1-1 Supported Features on Cisco Unified Border Element (SP Edition) Distributed Model (continued)*

| Release | Feature Name | Related SBC Commands | Chapter Where Documented |
|---|---|---|---|
| Cisco IOS XE Release 2.1 | Syntax-Level Support for H.248 VLAN Package | **show sbc dbe media-flow-stats**<br>**show sbc dbe signaling-flow-stats** | Chapter 7, "H.248 Packages—Signaling and Control" |
| Cisco IOS XE Release 2.1 | H.248.1v3 Support | **h248-version** | Chapter 7, "H.248 Packages—Signaling and Control" |
| Cisco IOS XE Release 2.1 | Cisco Unified Border Element (SP Edition) High Availability | None. | Chapter 11, "High-Availability Support," |
| Cisco IOS XE Release 2.1 | Interim Authentication Header Support | **transport** (see **interim-auth-header** keyword) | Superseded by Interim Authentication Header Full Support |
| Cisco IOS XE Release 2.1 | IP NAPT Traversal Package and Latch and Relatch Support | **h248-napt-package** | Chapter 9, "Security in Cisco Unified Border Element (SP Edition) Distributed Model" |
| Cisco IOS XE Release 2.1 | IPv4 Support for Twice NAPT | None. | Chapter 13, "Topology Hiding" |
| Cisco IOS XE Release 2.1 | IPv6 Inter Subscriber Blocking | None. | Chapter 13, "Topology Hiding" |
| Cisco IOS XE Release 2.1 | IPv6 Support | **ipv6 address (session border controller)**<br>**media-address ipv6**<br>**media-address pool ipv6**<br>**port-range (ipv6)**<br>**debug sbc filter** (see **ipv6** keyword)<br>**show sbc dbe media-flow-stats** (see **ipv6** keyword)<br>**show sbc dbe signaling-flow-stats** (see **ipv6** keyword) | Chapter 13, "Topology Hiding" |
| Cisco IOS XE Release 2.1 | Local Source Properties (Address and Port) | None. | Chapter 9, "Security in Cisco Unified Border Element (SP Edition) Distributed Model" |

*Table 1-1 Supported Features on Cisco Unified Border Element (SP Edition) Distributed Model (continued)*

| Release | Feature Name | Related SBC Commands | Chapter Where Documented |
|---|---|---|---|
| Cisco IOS XE Release 2.1 | Locally Hairpinned Sessions | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | Logging Level feature in Configuring the H.248 Logging Level | **logging level**<br>**logging filter control protocol** | Chapter 2, "Configuring the Cisco Unified Border Element (SP Edition) Distributed Model" |
| Cisco IOS XE Release 2.1 | Media Address Pools | **media-address pool ipv4**<br>**media-address pool ipv6**<br>**port-range** | Chapter 4, "Media Address Pools" |
| Cisco IOS XE Release 2.1 | MGC-Controlled Gateway-Wide Properties | None. | Chapter 7, "H.248 Packages—Signaling and Control" |
| Cisco IOS XE Release 2.1 | MGC-Specified Local Addresses or Ports | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | MultiStream Terminations | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | NAPT and NAT Traversal | None. | Chapter 9, "Security in Cisco Unified Border Element (SP Edition) Distributed Model" |
| Cisco IOS XE Release 2.1 | Nine-Tier Termination Name Hierarchy | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | Optional Local and Remote Descriptors | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | Provisioned Inactivity Timer | **h248-inactivity-duration** | Chapter 12, "Quality Monitoring and Statistics Gathering" |
| Cisco IOS XE Release 2.1 | QoS Bandwidth Allocation | None. | Chapter 5, "Quality of Service and Bandwidth Management" |
| Cisco IOS XE Release 2.1 | Remote Source Address Mask Filtering | **media-address ipv4**<br>**media-address pool ipv4** | Chapter 9, "Security in Cisco Unified Border Element (SP Edition) Distributed Model" |

*Table 1-1 Supported Features on Cisco Unified Border Element (SP Edition) Distributed Model (continued)*

| Release | Feature Name | Related SBC Commands | Chapter Where Documented |
|---|---|---|---|
| Cisco IOS XE Release 2.1 | RTCP Policing | None. | Chapter 5, "Quality of Service and Bandwidth Management" |
| Cisco IOS XE Release 2.1 | RTP-Specific Behavior Support | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | ServiceChange Notification for Interface Status Change | **sbc interface-id**<br>**termination-id rootidname** | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | T-MAX Timer | **tmax-timer** | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | tsc-Delay Timer | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.1 | transaction-pending functionality | **transaction-pending** | Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model (http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html) |
| Cisco IOS XE Release 2.1 | Two-Rate Three-Color Policing and Marking | **control-dscp marker-dscp pdr-coefficient**<br>**show sbc dbe forwarder-stats** | Chapter 5, "Quality of Service and Bandwidth Management" |
| Cisco IOS XE Release 2.2 | Full Support for Wildcard Response | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.2 | H.248 Protocol—Acknowledgment Support for Three-Way Handshake | None. | Chapter 7, "H.248 Packages—Signaling and Control" |
| Cisco IOS XE Release 2.2 | H.248 ServiceChange Handoff | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.2 | Full Support for Interim Authentication Header | **transport**<br>**inbound**<br>**outbound** | Chapter 9, "Security in Cisco Unified Border Element (SP Edition) Distributed Model" |

*Table 1-1 Supported Features on Cisco Unified Border Element (SP Edition) Distributed Model (continued)*

| Release | Feature Name | Related SBC Commands | Chapter Where Documented |
|---|---|---|---|
| Cisco IOS XE Release 2.2 | Improved Media Timeout Detection | **media-timeout** | Chapter 12, "Quality Monitoring and Statistics Gathering," |
| Cisco IOS XE Release 2.2 | IPsec Pinhole Support—Twice NAT for IPv4 and No NAT for IPv6 | **media-address ipv4**<br>**media-address pool ipv4**<br>**media-address ipv6**<br>**media-address pool ipv6** | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.3 | In-Service Provisioning of H.248 Controllers | None. | Chapter 6, "H.248 Services—Signaling and Control" |
| Cisco IOS XE Release 2.3 | RTCP maximum burst size policing parameter feature in RTCP Policing | None. | Chapter 5, "Quality of Service and Bandwidth Management" |
| Cisco IOS XE Release 2.6 | Optional Tman Bandwidth Parameter Policing | **bandwidth-police tman** | Quality of Service and Bandwidth Management |
| Cisco IOS XE Release 2.6 | Return Local and Remote Descriptors in H.248 Reply | **local-remote-desc always** | H.248 Services—Signaling and Control |
| Cisco IOS XE Release 2.6 | SBC End-Point Switching | None. | H.248 Services—Signaling and Control |
| Cisco IOS XE Release 2.6.2 | H.248 Timers | **tmax baseroot** | Chapter 6, "H.248 Timers" |
| Cisco IOS XE Release 3.1S | ETSI Ia Profile on SBC | **h248-profile**<br>**bandwidth-fields mandatory** | Chapter 8, "ETSI Ia Profile on SBC" |

# Deployment of the Cisco Unified Border Element (SP Edition) Distributed Model

Deployment of the DBE function on the Cisco ASR 1000 Series Routers integrates a subset of the Cisco Unified Border Element (SP Edition) feature set with Cisco IOS XE software. A likely deployment scenario is that typical routing and broadband features are configured on the Cisco ASR 1000 Series

Routers serving as the DBE operating with an external SBE. The Cisco Unified Border Element (SP Edition) functionality on the Cisco ASR 1000 Series Routers comprises both DBE and SBE functions, with DBE being the first to be deployed.

DBE deployment of the Cisco Unified Border Element (SP Edition) feature set is an optional feature supported on the Cisco ASR 1000 Series Routers. DBE deployment on the Cisco ASR 1000 Series Routers does not include SBE support and no SBE-related CLIs are implemented.

In the deployed distributed model, the SBE and the DBE entities reside on different network elements and the DBE is controlled by one SBE at any one time. The SBE interacts with the DBE using the H.248 Megaco (media gateway controller) protocol. The SBE controls the DBE via the H.248 interface. In this model, the bearer (or media flow) always flows through the DBE, and the SBE participates only in the signaling flow.

The DBE is responsible for the media flows and consists of a set of data path functions. The DBE responds to the requests made by the SBE to open pinholes, taking into account the specified NAT/firewall traversal and QoS requirements.

For the DBE, a new interface type is defined for the SBC virtual interface. You configure a virtual interface as part of the SBC configuration and the virtual interface has media IPs as primary or secondary IP addresses. The SBC virtual interface does not support any existing Cisco IOS features.

The Cisco IOS XE image containing Cisco Unified Border Element (SP Edition) software leverages existing Cisco IOS install and packaging facilities for software release, delivery, and installation.

Cisco IOS commands have been introduced to configure the DBE. For information on commands, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

# Cisco Unified Border Element (SP Edition) DBE Deployment Scenario

One potential deployment scenario for the distributed model of Cisco Unified Border Element (SP Edition) is in a network architecture where the service provider (SP) provides voice, data, and video services to their residential broadband customers over a single link.

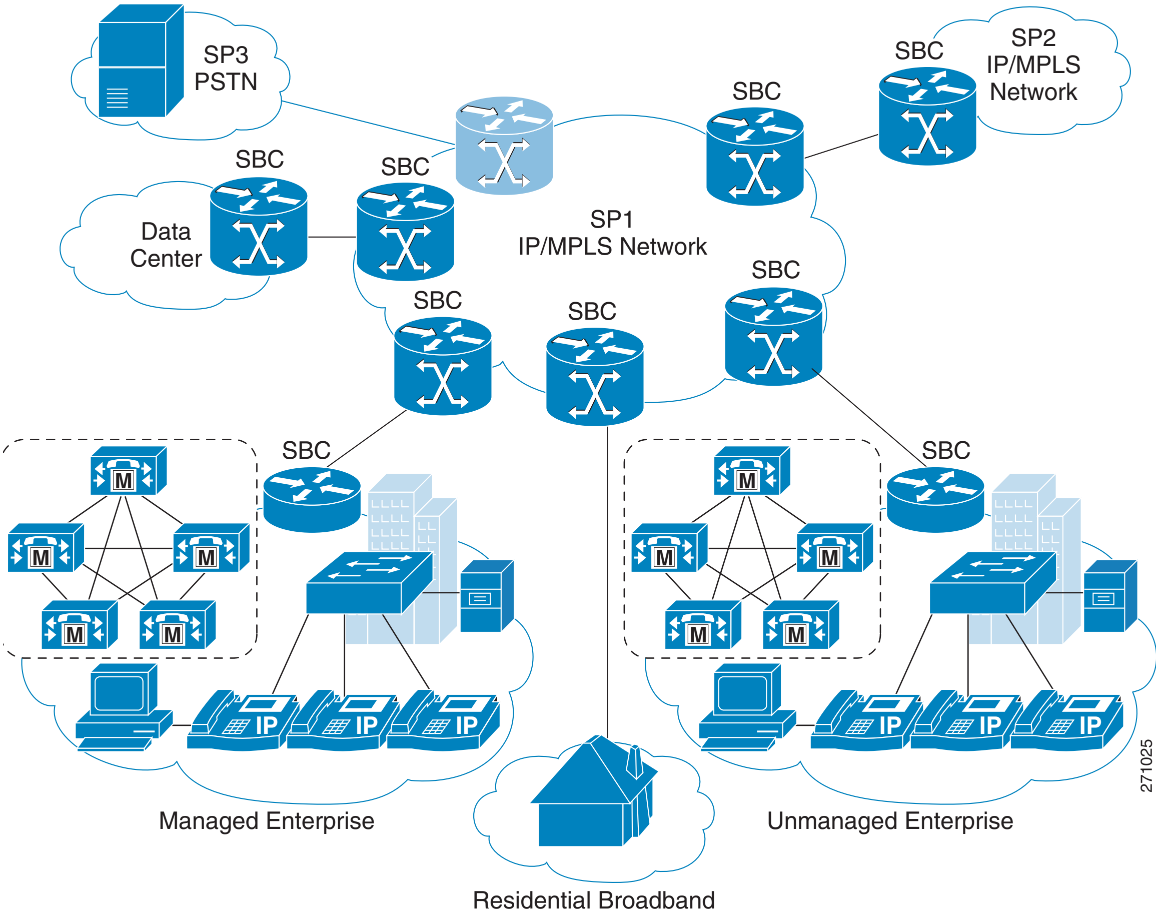
This scenario requires the SP to provide capabilities such as opening pinholes for the duration of a conversation, and doing this without exposing the devices behind the firewall to malicious threats. In addition, given that voice is extremely sensitive to issues such as delay, latency, and packet loss, ensuring adequate performance is a challenge. QoS mechanisms can be implemented to ensure proper priority is assigned to voice packets.

In this deployment scenario, multiple applications share a common link. Thus a mechanism that will limit bandwidth available to individual applications to ensure appropriate end-to-end quality is needed. For voice, this would involve correctly marking the packet to ensure appropriate priority, as well as controlling the number of simultaneous calls at the network entry point. Because the SP cannot dictate what IP phones their customers use, protocol conversion functionality is needed—especially H.323-to-SIP conversion.

Service providers require measurement of traffic for reporting and billing purposes in this potential scenario. Some carriers may also want to offer service level agreement (SLA) for voice, for which they want to be able to provide their customers with the proof that these SLAs are being met.

Figure 1-4 illustrates a deployment where Integrated SBC is used for VoIP interworking.

***Figure 1-4 Integrated SBC Used for VoIP Interworking***



CHAPTER 2

# Configuring the Cisco Unified Border Element (SP Edition) Distributed Model

This chapter describes fundamental configuration tasks required for typical data border element (DBE) deployment of the Cisco Unified Border Element (SP Edition). The Cisco ASR 1000 Series Aggregation Services Router serves as the DBE. The DBE operates with a Signaling Border Element (SBE), also called a media gateway controller (MGC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html.

Cisco Unified Border Element (SP Edition) was formerly known as the integrated session border controller. It is commonly referred to as the session border controller (SBC) in this document.

## Contents

This chapter provides information about the following topics:

## Prerequisites for the Cisco Unified Border Element (SP Edition) Distributed Model

When running SBC with 500 or more active calls, ensure you configure the huge buffer size to 65535 bytes with the **buffer huge size 65535** command. The increased buffer size is required because by default Cisco IOS software sets the “huge” buffer size to be 18084 bytes, which is not large enough for H.248 audit responses when there are more than 500 active calls.

**Note** For information on the number of active calls that can be reported or audited with a huge buffer of 65535 bytes, see the "Number of Active Calls That Can Be Audited" section on page 2-6.

# Restrictions for the Cisco Unified Border Element (SP Edition) Distributed Model

The following are *not* supported by the SBC function on the Cisco ASR 1000 Series Routers:

- Signaling Border Element (SBE) function and SBE CLIs
- Digital signal processing (DSP)
- Network management system (NMS) configuration
- Transcoding
- SBC virtual interface does not support any existing Cisco IOS features

**Note** When a VRF is removed from an SBC interface that is in use by an activated SBC, the IP addresses are not removed automatically by the SBC. The user has to manually remove the IP addresses when the SBC is deactivated.

# Configuring the Cisco Unified Border Element (SP Edition) DBE Deployment

This section contains steps to configure a typical DBE on the Cisco ASR 1000 Series Routers.

## Prerequisites

When running SBC with 500 or more active calls, configure the huge buffer size to 65535 bytes with the **buffer huge size 65535** command to ensure the buffer is large enough for H.248 audit responses.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface sbc** {*interface-number*}
4. **ip address** *ip-address*
5. **exit**
6. **sbc** {*sbc-name*} **dbe**
7. **vdbe** [**global**]
8. **h248-version** *version*
9. **h248-napt-package** [**napt** | **ntr**]

10. **local-port** {*port-num*}
11. **control-address h248 ipv4** {*A.B.C.D*}
12. **controller h248** {*controller-index*}
13. **remote-address ipv4** {*A.B.C.D*}
14. **remote-port** {*port-num*}
15. **transport** {**udp** | **tcp**} [**interim-auth-header**]
16. **exit**
17. **attach-controllers**
18. **exit**
19. **location-id** {*location-id*}
20. **media-address ipv4** {*A.B.C.D*}
21. **exit**
22. **activate**
23. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables the privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface sbc** {*interface-number*}<br>**Example:**<br>`Router(config)# interface sbc 1` | Creates an SBC virtual interface and enters into interface configuration mode. |
| **Step 4** | **ip address** *ip-address*<br>**Example:**<br>`Router(config-if)# ip address 1.1.1.1 255.0.0.0` | Configures an IP address on the SBC virtual interface. |
| **Step 5** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode. |
| **Step 6** | **sbc** {*sbc-name*} **dbe**<br>**Example:**<br>`Router(config)# sbc mySbc dbe` | Creates the DBE service on the SBC and enters into SBC-DBE configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **vdbe** [**global**]<br>**Example:**<br>Router(config-sbc-dbe)# **vdbe global** | Enters into VDBE configuration mode with a default DBE named “global”.<br>Only one DBE is supported and its name must be “global”. |
| **Step 8** | **h248-version** *version*<br>**Example:**<br>Router(config-sbc-dbe-vdbe)# **h248-version 3** | Specifies that the DBE uses an H.248 version when it forms associations with an H.248 controller.<br>Version 2 is the default. |
| **Step 9** | **h248-napt-package** [**napt** \| **ntr**]<br>**Example:**<br>Router(config-sbc-dbe-vdbe)# **h248-napt-package napt** | Defines whether the DBE uses the Network Address and Port Translation (NAPT) or NAT Traversal (NTR) H.248 package for signaling NAT features. NTR is the default. |
| **Step 10** | **local-port** {*port-num*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe)# **local-port 2947** | Configures the DBE to use the specific local port number when connecting to the default media gateway controller (MGC). |
| **Step 11** | **control-address h248 ipv4** {*A.B.C.D*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe)# **control-address h248 ipv4 210.229.108.254** | Configures the DBE to use a specific IPv4 H.248 control address, which is the local IP address the DBE uses as its own address when connecting to the SBE. |
| **Step 12** | **controller h248** {*controller-index*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe)# **controller h248 1** | Configures the H.248 controller for the DBE and enters into Controller H.248 configuration mode.<br>In the example, the configured number 1 identifies the H.248 controller for the DBE. |
| **Step 13** | **remote-address ipv4** {*A.B.C.D*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248)# **remote-address ipv4 210.229.108.252** | Configures the IPv4 remote address of the H.248 controller for the SBE.<br>In the example, 210.229.108.252 is configured as the remote SBE IP address. |
| **Step 14** | **remote-port** {*port-num*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248)# **remote-port 2947** | Configures the port number of the H.248 controller that is used to connect to the SBE. |
| **Step 15** | **transport** {**udp** \| **tcp**} [**interim-auth-header**]<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248)# **transport udp interim-auth-header** | Configures the DBE to use either UDP or TCP for H.248 control signaling. The command also configures the H.248 controller to insert the interim authentication header into the H.248 messages and set all fields in the header to zeroes. |
| **Step 16** | **exit**<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248)# **exit** | Exits Controller H.248 configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| Step 17 | **attach-controllers**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# attach-controllers` | Attaches the DBE to an H.248 controller. |
| Step 18 | **exit**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# exit` | Exits VDBE configuration mode. |
| Step 19 | **location-id** {*location-id*}<br>**Example:**<br>`Router(config-sbc-dbe)# location-id 1` | Configures a location ID for the DBE.<br>The location ID is used by the network to route calls. |
| Step 20 | **media-address ipv4** {*A.B.C.D*}<br>**Example:**<br>`Router(config-sbc-dbe)# media-address ipv4 1.1.1.1` | Adds the IPv4 address to the set of addresses, which can be used by the DBE as a local media address. This address is the SBC virtual interface address. Enters into media-address configuration mode.<br>Configure this command for each IP address that you specified under the SBC virtual interface in Step 4. |
| Step 21 | **exit**<br>**Example:**<br>`Router(config-sbc-dbe-media-address)# exit` | Exits the media-address configuration mode and enters into SBC-DBE configuration mode. |
| Step 22 | **activate**<br>**Example:**<br>`Router(config-sbc-dbe)# activate` | Initiates the DBE service of the SBC. |
| Step 23 | **end**<br>**Example:**<br>`Router(config-sbc-dbe)# end` | Exits SBC-DBE configuration mode and returns to the privileged EXEC mode. |

## Examples

The DBE does not always attach or detach from its controller immediately. You can use the **show sbc dbe controllers** command to display status information on whether the controller is attached or detached.

The following example uses the **show sbc dbe controllers** command to display status information showing that the VDBE with a location ID of 1 on an SBC called “mySbc” is attached to its controller:

```
Router# show sbc mySbc dbe controllers

SBC Service “mySbc”
  vDBE in DBE location 1

    Media gateway controller in use:
      H.248 controller address
        210.229.108.252:2944
      Status:           Attached
```

```
                  Sent       Received  Failed    Retried
      Requests    1          6          0        0
      Replies     6          1          0        0

    Configured controllers:
      H.248 controller 1:
        Remote address:    210.229.108.252:2944 (using default port)
        Transport:         UDP
```

# Troubleshooting Tips

The following are troubleshooting tips that may be helpful after you get your SBC into production.

## "Bad getbuffer" Log Message

You run over 500 active calls on your DBE deployment and you receive the following log message:

```
*Feb 11 11:35:52.909: %SYS-2-GETBUF: Bad getbuffer, bytes= 34506
-Process= "SBC main process", ipl= 0, pid= 183
-Traceback= 70EDFC 747354 9942D0 AFC6E4 B01AC4 29637B0 2960FCC 24C7F04 24C7918 24C7AD0
24D97AC 24D8790 2987C70
*Feb 11 11:35:52.909: %SBC-2-MSG-0303-0046: (sckrecv2.c 991)
Socket write error.
Sockets error code = 255
Socket ID = 0

*Feb 11 11:35:52.909: %SBC-2-MSG-0303-0025: (sckis.c 112)
General sockets layer error detected.
Sockets error code = 255

*Feb 11 11:35:52.909: %SBC-2-MSG-2E01-0014: (gctpfsm.c 730)
An association with a peer has become disconnected.
Peer's address = 200.10.255.252
Peer's port = 2944
Reason code = 0X04
```

Change your huge buffer size to 65535 bytes. This is the recommended huge buffer size for deployment of more than 500 active calls due to the need for increased buffer size for H.248 audit responses.

## Number of Active Calls That Can Be Audited

The number of active calls that can be reported or audited with a huge buffer of 65535 bytes depends on the following:

- The number of calls that can be audited depends on the details of the pinholes because these affect the size of the audit records.
- Using UDP as your H.248 transport may limit auditable calls. You can remove this limitation by using the Segmentation Package and configuring the huge buffer size to be equal to or greater than the segmentation PDU size.

# What to Do Next

See the "Configuring the H.248 Logging Level" section on page 2-7 if you want to set console logging other than default logging and turn on H.248 logging messages.

See Chapter 4, “Media Address Pools,” for information on what to configure next on the DBE.

See the “In-Service Provisioning of H.248 Controllers” section on page 6-8 for information on configuring a new controller or making changes to a controller.

# Configuring the H.248 Logging Level

This section contains steps to configure a sample configuration where console logging for H.248 messages sent and received is turned on and the H.248 protocol message filter is enabled to display only the H.248 text without any internal message logs.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sbc** {*sbc-name*} **dbe**
4. **vdbe** [**global**]
5. **h248-version** *version*
6. **h248-napt-package** [**napt** | **ntr**]
7. **local-port** {*port-num*}
8. **control-address h248 ipv4** {*A.B.C.D*}
9. **logging level** [*value*]
10. **logging filter control protocol** (Optional)
11. **controller h248** {*controller-index*}
12. **remote-address ipv4** {*A.B.C.D*}
13. **remote-port** {*port-num*}
14. **exit**
15. **attach-controllers**
16. **exit**
17. **end**

## DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | `sbc {sbc-name} dbe`<br>**Example:**<br>`Router(config)# sbc global dbe` | Creates the DBE service on the SBC and enters into SBC-DBE configuration mode. |
| Step 4 | `vdbe [global]`<br>**Example:**<br>`Router(config-sbc-dbe)# vdbe global` | Enters into VDBE configuration mode with a default DBE named "global".<br>Only one DBE is supported and its name must be "global". |
| Step 5 | `h248-version version`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# h248-version 3` | Specifies that the DBE uses an H.248 version when it forms associations with an H.248 controller.<br>Version 2 is the default. |
| Step 6 | `h248-napt-package [napt \| ntr]`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# h248-napt-package napt` | Defines whether the DBE uses the Network Address and Port Translation (NAPT) or NAT Traversal (NTR) H.248 package for signaling NAT features. NTR is the default.<br>The example shows how to configure the DBE to use NAPT. |
| Step 7 | `local-port {port-num}`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# local-port 2971` | Configures the DBE to use the specific local port number when connecting to the default media gateway controller (MGC). |
| Step 8 | `control-address h248 ipv4 {A.B.C.D}`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 200.50.1.41` | Configures the DBE to use a specific IPv4 H.248 control address, which is the local IP address the DBE uses as its own address when connecting to the SBE. |
| Step 9 | `logging level [value]`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# logging level 30` | Sets a specified logging level to generate detailed logs of H.248 messages sent and received. Turns on console logging for the specified level and logs above that level. |
| Step 10 | `logging filter control protocol`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# logging filter control protocol` | (Optional) Sets the H.248 protocol message filter for console logging to display only the H.248 text without any internal message logs. |
| Step 11 | `controller h248 {controller-index}`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# controller h248 2` | Configures the H.248 controller for the DBE and enters into Controller H.248 configuration mode.<br>In the example, the configured number 2 identifies the H.248 controller for the DBE. |
| Step 12 | `remote-address ipv4 {A.B.C.D}`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 200.50.1.254` | Configures the IPv4 remote address of the H.248 controller for the SBE.<br>In the example, 200.50.1.254 is configured as the remote SBE IP address. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | **`remote-port`** {*`port-num`*}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe-h248)#` **`remote-port 2971`** | Configures the port number of the H.248 controller that is used to connect to the SBE. |
| **Step 14** | **`exit`**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe-h248)#` **`exit`** | Exits Controller H.248 configuration mode. |
| **Step 15** | **`attach-controllers`**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)#` **`attach-controllers`** | Attaches the DBE to an H.248 controller. |
| **Step 16** | **`exit`**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)#` **`exit`** | Exits VDBE configuration mode. |
| **Step 17** | **`end`**<br>**Example:**<br>`Router(config-sbc-dbe)#` **`end`** | Exits SBC-DBE configuration mode and returns to the privileged EXEC mode. |

# Enabling the H.248 Logging Requests and Responses

Because the default logging level of 63 is set on by default, you can use the **logging level** command to enable other logging levels. In particular, logging level 30 generates logs showing H.248 requests sent and responses received. The **logging level** 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. The lower the logging level, the more syslog bandwidth is taken up.

You may want to consider the Cisco IOS console rate limiting configuration when you set your SBC logging level. Setting the SBC logging level to a level below the default of 63 can cause a substantial volume of messages to be generated. These messages are subject to standard Cisco IOS console rate limiting behavior, where warning and lower-level messages can be rate limited. Therefore, these messages and other messages may be dropped from the console output. However, they are still recorded in the logging buffer, which you can examine. Refer to the **logging rate-limit** command in the document titled *Cisco IOS Configuration Fundamentals and Network Management Command Reference* for more information.

**Note** 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.

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, logging can only be disabled by the **logging level** command. The **undebug all** and **no debug sbc log-level** commands have no effect.
- If logging and logging level are enabled by a **debug** command, logging can be disabled by the **undebug all** and **no debug sbc log-level** commands.
- 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.

### Example

The following example shows a sample log output produced on an H.248 ADD request with logging level set to 30:

```
*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.
```

# Configuration Examples

This section provides the following configuration examples:

- Configuring an SBC DBE Deployment
- Configuring the Primary IP and Primary Media IP Addresses
- Configuring the Secondary IP and Secondary Media IP Addresses

## Configuring an SBC DBE Deployment

The following steps list the tasks you need to do to configure an SBC DBE deployment on the Cisco ASR 1000 Series Routers:

1. Create an SBC virtual interface.
2. Configure IP addresses on the SBC virtual interface.
3. Create the DBE service on the SBC.
4. Configure the default VDBE.
5. Take the default **use-any-local-port** command behavior.
6. Configure the DBE to use a local H.248 control address to connect to the SBE.
7. Configure the H.248 controller for the DBE.
8. Configure the remote address of the H.248 controller for the SBE.
9. Attach the DBE to an H.248 controller.

10. Configure a location ID for the DBE.
11. Add an IPv4 address so it can be used by the DBE as a local media address.
12. Initiate the DBE service of the SBC.

The following is a sample configuration representing the ordered tasks used to configure an SBC DBE deployed on the Cisco ASR 1000 Series Routers:

```
interface sbc 1
 ip address 1.1.1.1 255.0.0.0
sbc mySbc dbe
 vdbe global
  control-address h248 ipv4 210.229.108.254
  controller h248 1
   remote-address ipv4 210.229.108.252
  attach-controllers
 location-id 1
 media-address ipv4 1.1.1.1
 activate
```

## Configuring the Primary IP and Primary Media IP Addresses

The following example shows the running configuration where the primary IP address and primary media IP addresses have been configured:

```
sbc mySbc dbe
 vdbe global
  use-any-local-port
  control-address h248 ipv4 210.229.108.254
  controller h248 1
   remote-address ipv4 210.229.108.252
  attach-controllers
 activate
 location-id 1
 media-address ipv4 1.1.1.1 <== primary local media IP address added using primary IP addr
interface sbc 1
 ip address 1.1.1.1 255.0.0.0 <=== primary IP address was configured on SBC interface
```

## Configuring the Secondary IP and Secondary Media IP Addresses

The following example shows the running configuration where a secondary IP address and secondary media IP address are configured after the primary IP address and primary media address have been configured:

```
sbc mySbc dbe
 vdbe global
  use-any-local-port
  control-address h248 ipv4 210.229.108.254
  controller h248 1
   remote-address ipv4 210.229.108.252
  attach-controllers
 activate
 location-id 1
 media-address ipv4 1.1.1.1
 media-address ipv4 25.25.25.25 <=== secondary media IP addr added using secondary IP addr
interface sbc 1
 ip address 25.25.25.25 255.0.0.0 secondary <= secondary IP addr configured on SBC interf.
 ip address 1.1.1.1 255.0.0.0
```

# Cisco H.248 Profile

H.248 profiles define option values, sets of packages, naming conventions, and other details for an entire set of applications. The SBC DBE deployment for the Cisco ASR 1000 Series Routers currently supports only one profile, SBC_GateControl. The SBC_GateControl profile, a Cisco internal profile based on ITU-T Recommendation H.248.1 Version 2, defines functionality between the DBE and the MGC.

## Overview of Profile

The profile connection model supports the following:

- Maximum number of contexts: Provisioned
- Maximum number of terminations per context: 68
- Allowed terminations type combinations: (IP,IP)

Table 2-1 shows the context attributes and values that are supported by the profile.

*Table 2-1 Context Attributes*

| Context Attribute | Supported | Values Supported |
|---|---|---|
| Topology | No | N/A |
| Priority Indicator | Yes | 0 to 15 |
| Emergency Indicator | Yes | ON/OFF |
| IEPS Indicator | Yes | ON/OFF |
| Context Attribute Descriptor | No | N/A |
| ContextIDList Parameter | No | N/A |
| AND/OR Context Attribute | No | N/A |

The termination ID structure is provisioned in the MGC. The MGC is at liberty to choose any termination naming structure. The DBE can accept 3 to 9 fields in the termination ID structure.

The following H.248 subseries transports are supported by the profile:

- Supported transports: TCP or UDP
- Segmentation supported: UDP: Optional

Use of the Interim Authentication Header defined in H.248.1v2 is optional within this profile.

# Profile Packages

This section specifies the packages that are supported in this profile. Mandatory packages are packages that are supported in the profile. Optional packages are packages that may be supported in the profile.

Table 2-2 shows the mandatory packages supported by the Cisco profile.

***Table 2-2 Mandatory Packages***

| Package Name | Package ID | Version |
|---|---|---|
| Base Root | root | 2 |
| Congestion Handling | chp | 1 |
| DTMF Detection | dd | 1 |
| DTMF Generation | dg | 1 |
| Diffserv | ds | 1 |
| Extended VPN Discrimination | evpnd | 1 |
| Inactivity Timer | it | 1 |
| Middlebox or EMP | emp | 1 |
| NAT Traversal | ntr | 1 |
| Network | nt | 1 |
| RTP | rtp | 1 |
| Traffic Management | tman | 1 |

Table 2-3 shows the optional packages supported by the Cisco profile.

***Table 2-3 Optional Packages***

| Package Name | Package ID | Version | Support Dependent On |
|---|---|---|---|
| Address Reporting | adr | 1 | Extension to ipnapt package |
| End Point Statistics | epstat | 1 | — |
| Enhanced Root | eroot | N/A | Proprietary package |
| Enhanced Traffic Management | etman | 1 | — |
| Gate Information | ginfo | 1 | — |
| Gate Recovery Information | gri | 1 | — |
| Generic | g | 1 | — |
| IP NAPT Traversal | ipnapt | 1 | — |
| Media Gateway Overload Control | ocp | 1 | — |
| Segmentation | seg | 1 | Applicable for UDP transport where sufficiently large messages are required to be supported |
| Session Failure Reaction | sfr | 1 | — |
| Termination State Control | tsc | 1 | — |

CHAPTER 3

# DTMF Interworking on the Cisco Unified Border Element (SP Edition) Distributed Model

This chapter describes the importance and function of dual-tone multifrequency (DTMF) interworking between various signaling types and how DTMF is supported on Cisco Unified Border Element (SP Edition).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

## Contents

This chapter provides information about the following topics:

## Information About DTMF Interworking

One of the features of Cisco Unified Border Element (SP Edition) is the ability to interwork between the various dual-tone multifrequency (DTMF) signaling types. DTMF interworking is used when the two endpoints do not use the same type for relaying DTMF tones.

DTMF dialing consists of simultaneous voice-band tones generated when a button is pressed on a telephone. The challenge comes from a scenario where one side uses Real-time Transport Protocol (RTP) and the other uses Session Initiation Protocol (SIP) signaling to enable advanced telephony services. Examples of the types of services and platforms that are supported by DTMF interworking are various voice web browser services, Centrex switches or business service platforms, calling card services, and unified message servers. All of these applications require DTMF interworking for the user to communicate with the application outside of the media connection.

The Cisco ASR 1000 Series Aggregation Services Routers only support DTMF interworking between RTP and SIP DTMF indication types. This type of DTMF interworking provides for DTMF signals generated by SIP to be inserted into an RTP stream and RTP DTMF tones to be extracted and to generate a SIP message.

The following are ways of generating a DTMF tone:

- SIP digit detection and generation package—A SIP message is sent from the endpoint to the SIP proxy indicating that there has been a DTMF event, the type and the duration of the event.
- RTP DTMF insertion—The RTP packets contain information in their headers indicating that a DTMF is being generated. The endpoints interpret these messages and play the DTMF locally.
- In-band waveform—The DTMF is sent as part of the voice waveform.

# RTP-to-SIP Interworking

In the case where the RTP packet is marked as DTMF, the RTP packet is removed from the stream and the DBE sends an H.248 message to the SBE indicating that a DTMF event has occurred and that this should be converted into a SIP DTMF event.

# SIP-to-RTP Interworking

In the case of an endpoint generating a SIP signal, the SIP DTMF signals arrive completely out of band. An endpoint that supports SIP DTMF generates the signals to the SBE. The SBE recognizes that this is a DTMF message and sends an H.248 message to the DBE that a DTMF tone is required to be inserted into the RTP stream. The DBE then inserts the RTP DTMF packets into the audio stream.

# Configuring the Default Duration of a DTMF Event

For a complete description of commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

*http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html.*

Use the **dtmf-duration** command in VDBE configuration mode to configure a default duration of a DTMF event. If there is no DTMF duration configured, the system default is 200 milliseconds.

## Prerequisites

Before implementing interworking DTMF, the DBE must be created.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sbc** {*sbc-name*} **dbe**
4. **vdbe** [**global**]
5. **dtmf-duration** {*duration*}
6. **exit**
7. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables the privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **sbc** {*sbc-name*} **dbe**<br>**Example:**<br>`Router(config)# sbc global dbe` | Enters the mode of a DBE service and enters into SBC-DBE configuration mode. Use the *sbc-name* argument to specify the name of the DBE service. |
| **Step 4** | **vdbe** [**global**]<br>**Example:**<br>`Router(config-sbc-dbe)# vdbe global` | Enters into the VDBE configuration mode with a default DBE named “global”.<br>Only one DBE is supported and its name must be “global”. |
| **Step 5** | **dtmf-duration** {*duration*}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# dtmf-duration 250` | Configures the default duration of a DTMF event in milliseconds. |
| **Step 6** | **exit**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# exit` | Exits the VDBE configuration mode. |
| **Step 7** | **end**<br>**Example:**<br>`Router(config-sbc-dbe)# end` | Exits SBC-DBE configuration mode and returns to the privileged EXEC mode. |

CHAPTER 4

# Media Address Pools

You can configure the distributed model of the Cisco Unified Border Element (SP Edition) with a single media address or a range of sequential media addresses. In addition, you can define one or more permissible port ranges for the configured addresses. This feature allows the administrator to configure or restrict the data border element (DBE) address by address pool with or without port range, and define class of service (CoS) affinity for each port range.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

## Contents

This chapter provides information about the following topics:

## Prerequisites for Implementing Media Address Pools

Before implementing media address pools, the Cisco Unified Border Element (SP Edition) must already be created. See the procedures described in the "Configuring the Cisco Unified Border Element (SP Edition) DBE Deployment" section on page 2-2.

## Restrictions for Configuring Media Address Pools

- The ending address must be greater than or equal to the starting address.
- The minimum port must be numerically lower than the maximum port.

- Port ranges may not overlap.
- Address ranges may not overlap.
- Address ranges and single addresses may not overlap.
- Where a range of addresses is defined in a single command, the addresses will share any port ranges assigned. If there is a requirement to have different port ranges for different media addresses, then the addresses must be configured separately.
- Media addresses and port ranges may only be deleted before the DBE is activated. After DBE activation, the DBE must be deactivated in order to delete addresses and port ranges.

# Information About Media Address Pools

A media address is one of a pool of IP addresses on the DBE that is used for media relay functionality. Addresses assigned by the media pool are the destination addresses used by packets that arrive at the DBE.

After you have configured a local media address or port range, the media address or port range cannot be modified while the DBE service is active. Deactivate the DBE with the **no activate** command before modifying the IPv4 or IPv6 media addresses or port ranges.

If you do not specify a port range, all possible VoIP port numbers are valid. The full VoIP port range extends from 1 to 65535 (inclusive).

You can define a class of service (CoS) affinity for each port range. The set of classes of service is consistent with those used for QoS packet marking, and consists of voice, video, signaling, fax, or any. If you do not define an associated CoS affinity, then the affinity is for all call types.

You can modify the extent of existing port ranges or the CoS affinities of existing port ranges or delete an existing port range. Any configuration changes do not apply to existing calls but apply to calls being set up after the configuration has been committed.

# Configuring Media Address Pools

This section contains steps for configuring media address pools on a DBE.

### SUMMARY STEPS

1. **configure terminal**
2. **interface sbc**
3. **sbc** {*sbc-name*} **dbe**
4. **media-address pool ipv4** {*A.B.C.D*} {*E.F.G.H*}
5. **port-range** {*min-port*} {*max-port*} [**any** | **voice** | **video** | **signaling** | **fax**]
6. **exit**
7. **end**
8. **show sbc** {*sbc-name*} **dbe addresses**
9. **show sbc** {*sbc-name*} **dbe media-flow-stats ipv4** *A.B.C.D* **port** *port-number*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 2 | **interface sbc**<br>**Example:**<br>`Router(config)# interface sbc 1` | Enters into interface configuration mode.<br>In the example, an SBC virtual interface called "1" is configured. |
| Step 3 | **sbc** {*sbc-name*} **dbe**<br>**Example:**<br>`Router(config)# sbc mySbc dbe` | Enters into SBC-DBE configuration mode. |
| Step 4 | **media-address pool ipv4** {*A.B.C.D*} {*E.F.G.H*}<br>**Example:**<br>`Router(config-sbc-dbe)# media-address pool ipv4 10.0.2.1 10.0.2.10` | Creates a pool of sequential IPv4 media addresses that can be used by the DBE as local media addresses. Enters into SBC-DBE media address configuration mode. |
| Step 5 | **port-range** {*min-port*} {*max-port*} [**any** \| **voice** \| **video** \| **signaling** \| **fax**]<br>**Example:**<br>`Router(config-sbc-dbe-media-address)# port-range 16384 30000 any` | Creates a port range for the configured media addresses in the pool and specifies a class of service such as any, voice, video, signaling, and fax for the port range.<br>In the example, a port range of 16384 to 30000 is created where the class of service for the port range is any class of service. |
| Step 6 | **exit**<br>**Example:**<br>`Router(config-sbc-dbe-media-address)# exit` | Exits SBC-DBE media address configuration mode. |
| Step 7 | **end**<br>**Example:**<br>`Router(config-sbc-dbe)# end` | Exits SBC-DBE configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **show sbc** {*sbc-name*} **dbe addresses**<br>**Example:**<br>`Router#` **`show sbc mySbc dbe addresses`** | Lists the media addresses and H.248 control addresses configured on DBEs. |
| **Step 9** | **show sbc** {*sbc-name*} **dbe media-flow-stats ipv4** *A.B.C.D* **port** *port-number*<br>**Example:**<br>`Router#` **`show sbc mySbc dbe media-flow-stats ipv4 10.0.1.1 port 20000`** | Displays the statistics about one or more media flows collected on the DBE and shows, as an example, the following reported fields:<br>• *A.B.C.D*—(Optional) Only displays media flows to and from this IPv4 media address.<br>• *port-number*—(Optional) Only displays media flows to and from this port.<br>The RTCP packet statistics are collected from RTCP packets transmitted by endpoints and are updated when the RTCP packets are received. |

# Configuring Media Address Pools Example

This section provides a sample configuration for media address pools.

The following sample script adds a single address (10.10.10.1), and two ranges of addresses (10.10.11.1 through 10.10.11.10 and 10.10.11.21 through 10.10.11.30) to the default media address pool.

Two port ranges are configured on the single address. The first port range is for voice traffic, and runs from port 16384 to 20000 inclusively. The second one is for video traffic, and runs from port 20001 to 65535 inclusively.

The first range of addresses also has two similar port ranges configured that apply to all ten addresses within the range.

The second range of addresses has a single port range defined, and no service class associated with it.

```
Router(config)# interface sbc 1
Router(config)# sbc mySBC dbe
Router(config-sbc-dbe)# media-address ipv4 10.10.10.1
Router(config-sbc-dbe-media-address)# port-range 16384 20000 voice
Router(config-sbc-dbe-media-address)# port-range 20001 65535 video
Router(config-sbc-dbe-media-address)# exit
Router(config-sbc-dbe)# media-address pool ipv4 10.10.11.1 10.10.11.10
Router(config-sbc-dbe-media-address)# port-range 16384 30000 voice
Router(config-sbc-dbe-media-address)# port-range 30001 40000 video
Router(config-sbc-dbe-media-address)# exit
Router(config-sbc-dbe)# media-address pool ipv4 10.10.11.21 10.10.11.30
Router(config-sbc-dbe-media-address)# port-range 20000 40000 any
```

CHAPTER 5

# Quality of Service and Bandwidth Management

Cisco Unified Border Element (SP Edition) distributed model for the Cisco ASR 1000 Series Routers provides Quality of Service (QoS) and bandwidth management features to assure quality end-to-end connection for real-time voice, video, and multimedia traffic. The packet marked for higher priority is delivered faster than non-prioritized packets. The data border element (DBE) supports statistics collection and saves all QoS statistics, including packets transmitted per second and packets dropped for exceeding allocated bandwidth on a per-call or per-interface basis. The Cisco ASR 1000 Series Routers support QoS functions such as Low Latency Queueing (LLQ), Class-Based Weighted Fair Queueing (CBWFQ), and shaping at the subinterface level.

The DBE has different packages to enhance QoS and these packages are described in this chapter.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

For information about all Cisco IOS commands, use the Command Lookup Tool at:

http://tools.cisco.com/Support/CLILookup or a Cisco IOS master commands list.

#### Feature History for the QoS and Bandwidth Management Features

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.1 | These features were introduced on the Cisco ASR 1000 Series Aggregation Services Routers for the distributed model. See Table 1-1 in Chapter 1 for a list of supported features by release. |
| Cisco IOS XE Release 2.6 | The Optional Tman Bandwidth Parameter Policing feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |

# Contents

This chapter provides information about the following topics:

# H.248 Traffic Management Package Support

The DBE supports the sustained data rate (tman/sdr), maximum burst size (tman/mbs), and policing (tman/pol) properties of the ETSI TS 102 333 Traffic Management (Tman) package.[1] Support of these Tman properties allows additional pinhole programming in the Tman package to inform the DBE how to police media and signaling flows. These Tman properties can be assigned to both media and signaling flows.

The DBE performs asymmetric policing. Asymmetric policing allows the MGC to impose different flow policing on traffic traveling in each direction on the same stream. For example, traffic traveling from the subscriber side to the DBE can be policed independently of traffic from the network core to the DBE.

Asymmetric policing is accomplished by allowing the tman/pol property to be specified separately for the two sides of a gate, which typically might be the access (subscriber) side and the backbone side. The tman/pol property can be specified as ON, OFF, or Absent on either the access side or the backbone side for either a media flow or signaling flow. Once tman/pol is specified as ON and both the tman/sdr and tman/mbs properties are present, the DBE polices traffic based on the values of the tman/sdr and tman/mbs parameters.

The supported Tman properties have the following functions:

- The tman/sdr property defines the sustainable data rate in bytes per second that is permitted for the stream. It has a numerical value.
- The tman/mbs property defines maximum burst size in bytes for the stream. It has a numerical value.
- The tman/pol (policing) property can be set to ON or OFF or Absent.
  - When the tman/pol property is set to ON, policing is applied at the point of entry for traffic entering the media gateway (MG).

    When both the tman/sdr and tman/mbs properties are present (and the tm/pol property is ON), the DBE polices traffic based on the sdr and mbs Tman parameters.

    However, the absence of both tman/sdr and tman/mbs properties is permissible. In this case, the DBE polices traffic based on the Session Description Protocol (SDP).

**Note** For releases prior to Cisco IOS XE Release 2.6, if either the tman/sdr or tman/mbs property is present, then the other property must be present; that is, *both* the tman/sdr and tman/mbs properties must be present. In this case, the DBE polices traffic based on the sdr and mbs parameters.

[1] ETSI TS 102 333 version 1.1.2 Traffic Management Package

- When the tman/pol property is set to OFF, no policing is applied to traffic entering the media gateway.
- If the tman/pol property is Absent, policing is done based on the SDP for the stream for a media flow. No policing is done for a signaling flow.

**Note** Absent means that the property has not been defined. If no Tman properties (tman/pol, tman/sdr, and tman/mbs) have been defined, then the behavior for a media flow is to calculate the required bandwidth from the Session Description Protocol (SDP) in the local descriptor. For a signaling flow, the behavior is to perform no policing.

The Tman properties (tman/pol, tman/sdr, and tman/mbs) are defined using Add and Modify requests, and they are returned on subsequent responses to Audit requests.

**Note** For additional information on RTP and RTCP streams and RTCP policing based on the Tman Package, see the "RTCP Policing" section on page 5-6.

The Tman properties have the following caveat:

For releases prior to Cisco IOS XE Release 2.6, the DBE issues error 421 indicating "Unknown action or illegal combination of actions" for any programming containing other fields and programming that sets the tman/pol flag, but only specifies one of the tman/sdr or tman/mbs values.

For releases prior to Cisco IOS XE Release 2.6, Table 5-1 describes the asymmetric flow policing behavior of the two sides of a gate based on whether the tman/pol property is specified as ON, OFF, or Absent. Each side of the gate behaves independently of the other side. The Access Side might be the subscriber side to the DBE, and the backbone side might be the network core to the DBE.

*Table 5-1 Asymmetric Flow Policing—Independent Behavior of Signaling and Media Flows on Two Sides of a Media Gateway*

| | | Access Side (AC) | | |
|---|---|---|---|---|
| | **tman/pol Property** | **Absent** | **ON** | **OFF** |
| **Back Bone Side (BB)** | **Absent** | Signaling: No policing<br>Media: Policing per SDP | Signaling: Policing per Tman parameters on AC and no policing on BB<br>Media: Policing per Tman parameters on AC and per SDP on BB | Signaling: No policing on AC and BB<br>Media: No policing on AC and policing per SDP on BB |
| | **ON** | Signaling: Policing per Tman parameters on BB and no policing on AC<br>Media: Policing per Tman parameters on BB and per SDP on AC | Signaling: Policing per Tman parameters on AC and on BB independently<br>Media: Policing per Tman parameters on AC and on BB independently | Signaling: No policing on AC and policing per Tman parameters on BB<br>Media: No policing on AC and policing per Tman parameters on BB |
| | **OFF** | Signaling: No policing on BB and AC<br>Media: No policing on BB and policing per SDP on AC | Signaling: No policing on BB and policing per Tman parameters on AC<br>Media: No policing on BB and policing per Tman parameters on AC | Signaling: No policing on BB and AC<br>Media: No policing on BB and AC |

# Optional Tman Bandwidth Parameter Policing

In Cisco IOS XE Release 2.6, the Optional Tman Bandwidth Parameter Policing feature improves H.248 interworking capability with the Traffic Management (Tman) package. The usefulness of the feature is to disable bandwidth policing from using bandwidth (b-) line information when Tman parameters are missing in order to comply 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.

The Optional Tman Bandwidth Parameter Policing feature uses CLI to configure the data border element (DBE) to perform no traffic policing unless Traffic Management (Tman) properties, tman/pdr or tman/sdr, 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.

Prior to Cisco IOS XE Release 2.6, *both* tman/pdr and tman/sdr were required to be present before the DBE policed traffic. This feature improves interworking capability with the media gateway controller (MGC). The behavior prior to Cisco IOS XE Release 2.6 was that the DBE performed bandwidth policing based either on Tman parameters or on the SDP bandwidth (b-) line information, with Tman parameters taking precedence over b-line information in the SDP. Therefore if *both* tman/pdr and tman/sdr are missing, the DBE would do bandwidth policing based on information from the b-line.

For behavior prior to Cisco IOS XE Release 2.6, see the "H.248 Traffic Management Package Support" section on page 5-2.

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

## Configuration Examples of an Optional Tman Bandwidth Parameter Policing feature

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, then policing is performed using tman/pdr or tman/sdr.

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

The following example shows how to set 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 dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# no bandwidth-police tman
```

# DSCP Marking and IP Precedence Marking

The DBE supports marking of differentiated services code point (DSCP) bits and IP precedence marking for egress traffic and media relay. Using standard Router features, these markings can be used to prioritize packets for faster delivery or for lower risk of drop under congestion.

## DSCP Re-Markings

For every media stream, the DBE receives a DSCP value to use in the Real-Time Transport Protocol (RTP) and RTP Control Protocol (RTCP) packets. The DBE receives these values at the call setup time on a per-flow basis and maintains the values as a part of the connection table entry. The DBE modifies the type of service (TOS) bits in the IP header for every outgoing packet and updates the checksum accordingly.

# QoS Bandwidth Allocation

The DBE supports QoS bandwidth allocation. The DBE has the ability to limit excess traffic beyond the allocated bandwidth by performing session-based policing. For information on the different types of policing performed by the DBE, see the "H.248 Traffic Management Package Support" section on page 5-2, the "RTCP Policing" section on page 5-6, and the "Two-Rate Three-Color Policing and Marking" section on page 5-7.

# RTCP Policing

An SBC session may be of two types, media or signaling. The media portion of the call comprises the Real-Time Transport Protocol (RTP) stream and, optionally, a RTP Control Protocol (RTCP) stream. Calls typically have both a RTP and RTCP stream.

Each session may be subject to policing. RTCP streams are not explicitly configured using the H.248 protocol and therefore cannot have their policing parameters set. Instead, the policing parameters for RTCP sessions are derived from the corresponding RTP flows based on the usage of the ETSI TS 102 333 Traffic Management (Tman) package.

For more information on the Tman package, see the "H.248 Traffic Management Package Support" section on page 5-2.

## RTCP Policing Using the Tman Package

The H.248 Tman package is used to set the sustained data rate (tman/sdr) and maximum burst size (tman/mbs) properties, and the policing type (tman/pol), on the RTP session. The tman/pol property can be specified as one of the following:

- ON—Policing is enabled on the RTP session.
- OFF—No policing is applied to incoming traffic.
- Absent—Property is not defined, but policing is enabled on the RTP session.

When tman/pol is ON, then tman/sdr and tman/mbs set the policing parameters for the RTP session. When tman/pol is OFF, then there is no policing of either RTP or RTCP sessions. When tman/pol is Absent or undefined, then default policing parameters for RTP sessions are derived from the codec embedded in the SDP string.

When policing is enabled on the RTP session, RTCP policing parameters for setting rate limits (sustained data rate) and maximum burst size are derived from RTP parameters by calculating 5 percent of the RTP sdr and 5 percent of the RTP mbs, with a minimum RTCP sdr and mbs. See Table 5-2 for details on how policing parameters for RTP and RTCP sessions are derived.

*Table 5-2 Policing Parameters for RTP and RTCP Sessions*

| | If tman/pol = ON, policing parameters are derived as follows | If tman/pol = Absent (undefined), policing parameters are derived as follows | If tman/pol = OFF, policing parameters are derived as follows |
|---|---|---|---|
| **For the RTP session** | tman/sdr and tman/mbs set the policing parameters. | Default policing parameters are derived from the codec embedded in the SDP string. | There is no policing of RTP sessions. |
| **For the RTCP session** | • The sustained data rate for RTCP policing is 5 percent of the sustained data rate for the RTP session, or a minimum rate of 208 bytes per second, whichever is the greater.<br>• The maximum burst size for RTCP policing is 5 percent of the RTP maximum burst size, or a minimum value of 1500 bytes, whichever is the greater. | • The sustained data rate for RTCP policing is 5 percent of the sustained data rate for the RTP session, or 208 bytes per second, whichever is the greater.<br>• The maximum burst size for RTCP policing is 5 percent of the RTP maximum burst size, or 1500 bytes, whichever is the greater. | There is no policing of RTCP sessions. |

## RTCP Policing Without Using the Tman Package

RTCP policing can be implemented by not setting any of the properties of the H.248 Tman package.

When the tman/sdr and tman/mbs properties are not specified, the RTCP rate limiting and maximum burst size are set at 5 percent of the codec (embedded in the SDP string) for the RTP stream.

# Two-Rate Three-Color Policing and Marking

Traffic policing is a traffic regulation mechanism that is used to limit the rate of traffic streams. Policing allows you to control the maximum rate of traffic sent or received on an interface. When the traffic rate exceeds the configured maximum rate, policing drops or re-marks the excess traffic.

The ETSI TS 102 333 Traffic Management (Tman) package defined a number of properties to allow traffic policing to be explicitly enabled. However, because the current H.248 standard only supported specifying one rate with a traffic flow, the only action available in the H.248 standard for non-conforming packets had been to discard them. (See the "Enhanced Event Notification and Auditing" section on page 12-4).

The Two-Rate Three-Color Policing and Marking feature is an enhancement to how the DBE polices traffic flow by introducing two-rate policing and three-color marking.

The DBE previously supported three tman properties—policing type (pol), sustainable data rate (sdr), and maximum burst size (mbs). In supporting the Two-Rate Three-Color Policing and Marking feature, the DBE uses one additional property of the ETSI TS 102 333 Traffic Management (Tman) package:

peak data rate (pdr)—Defines the peak data rate in bytes per second that is permitted for the stream.

See "H.248 Traffic Management Package Support" section on page 5-2 for more information on the tman properties.

# Enabling Two-Rate Three-Color Policing and Marking

All of the following conditions must occur to enable the Two-Rate Three-Color Policing and Marking feature for a specific flow:

- The DSCP value is provisioned via diffserv package during call setup.
- The sdr and mbs are provisioned via the Tman package during call setup. (The mbs property is used for pdr policing as well and has an assumed minimal value of 1500 bytes.)
- Two DSCP values (control and marker DSCPs) and the pdr coefficient are configured via the **control-dscp marker-dscp pdr-coefficient** CLI.
- The **control-dscp** value configured must match the diffserv DSCP value for a specific flow to enable the Two-Rate Three-Color Policing and Marking feature.

If any one of the conditions is not met, this feature is not enabled for the flow.

# Implementing Two-Rate Three-Color Policing and Marking

In the Two-Rate Three-Color Policing and Marking feature, only two rates—sdr and pdr—allow traffic to be policed into three categories of traffic, which are handled as follows:

- Traffic conforming to both sdr and pdr.

  These packets are colored using the DSCP value provisioned via the H.248 diffserv package; that is, H.248 passes the DSCP value. These packets are forwarded and the DSCP value comes from the H.248 diffserv package.

- Traffic not conforming to the lower sdr rate, but conforming to the higher pdr rate.

  These packets are colored with the marker DSCP value and pdr configured with the **control-dscp** *value1* **marker-dscp** *value2* **pdr-coefficient** *value3* command.

  - The **control-dscp** *value1* keyword enables the Two-Rate Three-Color Policing and Marking feature for a specific flow if *value1* matches the DSCP value for the flow in the diffserv package transmitted via H.248.
  - The **marker-dscp** *value2* keyword colors traffic packets with a DSCP *value2*. This traffic conforms to the peak data rate (pdr), but does not conform to the sustainable data rate (sdr).
  - The **pdr-coefficient** *value3* keyword applies the following formula to calculate the pdr value (which is not passed from H.248).

    The pdr-coefficient value is calculated as pdr = sdr * *value3* /100 (and pdr must be greater than sdr).

- Traffic not conforming to either of the sdr or pdr rates.

  These packets are dropped.

**Note** The Two-Rate Three-Color Policing and Marking feature is not enabled for a particular flow if the DSCP value set by H.248 for that flow does not match the configured **control-dscp** *value1*.

Traffic flows must have the Two-Rate Three-Color Policing and Marking feature enabled to use the three parameters configurable with the Two-Rate Three-Color CLI. Traffic flows that do not have the Two-Rate Three-Color Policing and Marking feature enabled are subject to normal Tman-based policing with pdr, sdr, and mbs parameters configured via H.248, regardless of the pdr coefficient configured via the Two-Rate Three-Color CLI.

The DBE supports dual token bucket policing to support this feature. The DBE uses a "token bucket algorithm" to manage the maximum rate of traffic. This algorithm is used to define the maximum rate of traffic allowed on an interface at a given moment in time. The token bucket algorithm processes as follows—each arriving packet's size (frame's size) is subtracted from the contents of the bucket. If the bucket does not have enough tokens for the arriving packet, the packet is dropped and no tokens are removed. The passage of time fills the bucket with tokens and the dispatching of a packet depletes the bucket.

## DBE Restrictions

The following are DBE restrictions pertaining to the Two-Rate Three-Color Policing and Marking feature:

- The DSCP values configured via CLI are global. Specifically, the DSCP values are shared among all the terminations when this feature is enabled.
- The Two-Rate Three-Color CLI is only applicable to future new call flows and do not trigger any backtrack to established terminations.
- A media gateway controller (MGC), also called the SBE, is only able to use the Tman fields if the DBE supports the various features which make up Tman support.

## Related Commands

The **control-dscp marker-dscp pdr-coefficient** command enables the Two-Rate Three-Color Policing and Marking feature, and configures differentiated services code point (DSCP) values and the peak data rate (pdr) coefficient for the feature on the data border element (DBE) for each affected flow.

The **show sbc dbe forwarder-stats** command output entries are added to report statistics of colored traffic.

For a description of the commands used, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

CHAPTER 6

# H.248 Services—Signaling and Control

The data border element (DBE) of the Cisco Unified Border Element (SP Edition) distributed model manages media packets, but it also takes part in forwarding signaling packets to the signaling border element (SBE). In this way, the DBE helps in signaling interworking.

The SBE generates controlling packets and, through the H.248 interface, informs the DBE on management of media packets, as well as signaling packets. After the DBE creates media pinholes and defines the policy, the DBE manages the media packets based on that policy. The features in this chapter describe different H.248 services and controlling functions of the DBE.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

For information about all Cisco IOS commands, use the Command Lookup Tool at:

http://tools.cisco.com/Support/CLILookup or a Cisco IOS master commands list.

**Feature History for H.248 Services—Signaling and Control Features**

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.1 | These features were introduced on the Cisco ASR 1000 Series Aggregation Services Routers for the distributed model. See Table 1-1 for a list of supported features by release. |
| Cisco IOS XE Release 2.6 | The following features were introduced on the Cisco ASR 1000 Series Aggregation Services Routers:<br>• The Return Local and Remote Descriptors in H.248 Reply.<br>• End-Point Switching. |
| Cisco IOS XE Release 2.6.2 | The H.248 Timers feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |

# Contents

This chapter provides information about the following topics:

# DBE Signaling Pinhole Support

DBE Signaling Pinhole Support allows the media gateway controller (MGC) to directly control policing of signaling flows through the SBC interfaces on the DBE. The policing is at a per signaling flow level, via the H.248 association between the MGC and the DBE. The feature removes the need to have a separate firewall device to protect the MGC.

Without this feature, signaling packets are addressed to the SBE, and the DBE acts as a router, forwarding the packets to the SBE. With this feature enabled, the DBE can police signaling packets using the ETSI TS 102 333 Traffic Management (Tman) package. The DBE has application-level pinholes created to allow those packets to be forwarded to the SBE. Normal IP forwarding is disabled on the SBC interfaces of the DBE.

DBE Signaling Pinhole Support includes the following functionality:

- DBE only forwards traffic that is received on a configured pinhole. The packet must be addressed to a VPN, address, or port on an SBC interface on the DBE.
- Signaling pinholes are configured in the same way as media pinholes over H.248. They can be differentiated from media pinholes by session descriptions as defined in the Session Description Protocol (SDP) in the local and remote descriptors. The "m=application" line indicates that the termination is a signaling pinhole.
- Data rate through a signaling pinhole can be unlimited.
- MGC can specify the VPN, address, and port of the pinhole on the DBE when it is created. This must be selected from the address and port range available on the DBE, and must not already have been allocated for another use. This function is intended to be used for signaling pinholes, but it can be used for any pinhole. The address and port range available must be separately configured on both the MGC and the DBE.
- Each endpoint must have a signaling pinhole associated with it for it to communicate with the Session Initiation Protocol (SIP) server.
- Signaling pinholes are forwarded in the same way as media pinholes; that is, packets are forwarded after the policing bandwidth usage is checked and the IP header is re-written. The only exception is that signaling pinholes do not time out if the flow of signaling packets stops.
- Signaling pinholes can be used for traffic other than just SIP, such as for non-RTP media streams of any kind. However, you need to specify a bandwidth limit using the Tman package if you want policing.

## Restrictions for DBE Signaling Pinhole Support

The following are DBE restrictions pertaining to the DBE Signaling Pinhole Support feature:

- Endpoint still needs to be sending its signaling to a local address owned by the DBE configured as a media address.
- If a signaling port range is not configured, then by default the range is the same as that for media ports (16384 to 32767). For this reason, it is recommended that a signaling port range is explicitly configured. The configured range must not clash with the address and port used by the media gateway for its connection to the MGC. You need to ensure this configuration is entered consistently.

# Extension to H.248 Audit Support

Extension to H.248 Audit Support adds support for DBE auditing of the Signals, ObservedEvents, and EventBuffer descriptors in any of the **Add**, **Modify**, **Subtract**, or **AuditValue** commands at any time on both sides of a media flow.

## Restrictions for the DBE Extension to H.258 Audit Support

The following are restrictions pertaining to the DBE Extension to H.248 Audit Support feature:

- When a termination endpoint has latched, the Signals, ObservedEvents, and EventBuffer descriptors are empty.

For information on latching, see the "IP NAPT Traversal Package and Latch and Relatch Support" section on page 9-9.

- When a termination has not yet latched, the Signals, ObservedEvents, and EventBuffer descriptors contain other descriptors; for example, the Signals descriptor can contain the descriptor for the ipnapt/latch signal.
- DBE only supports the Dual Tone Multifrequency (DTMF) injection and the ipnapt/latch signals. However, the DTMF injection signal is defined as a brief signal and thus is not present in the Signals descriptor.
- DBE does not support the lockstep mode of event reporting. Therefore, the ObservedEvents and EventBuffer descriptors never contain events.

# Extension to H.248 Termination Wildcarding Support

Extension to H.248 Termination Wildcarding Support adds support for partially wildcarded termination names, which allows a single command to replace one or more elements of a termination name with the wildcard character "*".

The MGC can issue H.248 commands using wildcarding at any level of the Nine-Tier Termination Name Hierarchy.

For example, any of the following wildcarded termination names would be valid:

```
operator/sip/*/0/1023/0/*/*/*
operator/sip/*/0/1023/0/4094/*/*
*/*/*/0/1023/0/*/*/*
```

For more information on the Nine-Tier Termination Name Hierarchy feature, see the "Nine-Tier Termination Name Hierarchy" section on page 6-18.

## Restrictions for the DBE H.248 Termination Wildcarding Support

The following are restrictions pertaining to DBE Extension to H.248 Termination Wildcarding Support feature:

- H.248 commands supporting wildcarded termination names are limited to the **AuditValue**, **Modify** (of ServiceState), and **Subtract** commands.
- In the event that both the Termination ID and Context ID are wildcarded, then the Modify and Subtract commands must include an empty Audit descriptor, and must request a wildcarded response.
- Partial wildcards, which omit one or more tiers of the termination name, are not supported. For example, "operator/sip/*" is not supported, but "operator/sip/*/*/*/*/*/*/*" is. The exception is the full wildcard, which is simply "*".
- You can construct transactions with multiple overlapping wildcarded commands, and when a single transaction contains multiple commands referencing the same terminations, the commands operate in order. However, when a termination is subtracted, any other commands affecting it are ignored.

  For example, suppose a media gateway (MG) has a single termination a/b/1. The following are examples of overlapping wildcarded commands and their returns:

  - "audit value a/*/*, audit value */b/*" returns a/b/1 in the response twice.

- "modify a/*/*, modify */b/*" modifies termination a/b/1, with the second modify overwriting the first, and return success to both commands.
- "subtract a/*/*, subtract */b/*" subtracts a/b/1 as part of the first subtract and ignores the second subtract.
- "subtract a/*/*, modify */b/*" subtracts termination a/b/1 and ignores the modify.
- "modify a/*/*, subtract */b/*" does the same as above.

When a wildcard command is ignored under these circumstances, the response to that command is error 431 "No Termination ID matched a wildcard".

When a non-wildcarded command is ignored, the response is error 430 "Unknown Termination ID".

# Flexible Address Prefix Provisioning

When the Remote Source Address Mask (rsam) property of the ETSI TS 102 333 Gate Management (GM) package is not involved in the flow entry hash key construction, there are no limits to the network mask length, because the mask specific to each flow is used to validate the SBC packets after the flow entry is retrieved (that is, the expected gm/rsam information is obtained from the flow entry that is stored during the signaling/call setup process). However, when features such as Local Source Properties (Address and Port) or Remote Source Address Mask Filtering are used, where flows from various source IPs can connect to the same service destination IP address and port, the source IP network mask (gm/rsam network mask) must be used in the hash key construction in addition to the destination IP and port to identify and retrieve a unique flow entry.

Because there is no way to know about the existence of the multiple terminations when the DBE tries to construct the hash key for retrieving the flow entry, support has been added for the Flexible Address Prefix Provisioning feature. This feature creates a dummy entry using the service IP and port to construct a hash key when the first termination with this service IP and port combination is established. This dummy entry is shared among all the terminations sharing the same service IP and port for storing network masks, and supports three different lengths of network masks on a given shared address at one time or different shared addresses. Any length of network masks is allowed.

This feature is applicable to both IPv4 and IPv6 flows.

If there is only one network mask in a dummy entry, the DBE uses this network mask to mask out the source IP of the incoming packet and, together with the destination IP/port, constructs a new hash key to locate the corresponding termination flow entry from the flow table.

If multiple network masks are configured in the dummy entry, the DBE masks the source IP of the incoming packets using the multiple network masks stored in the dummy entry sequentially from longest to shortest. If a flow entry is located, the DBE stops the flow retrieval operation and continues the rest of SBC processing. When a termination is subtracted, its network mask length is removed from the dummy entry if the termination is the last one with that gm/sam network mask length.

## Restrictions for DBE Flexible Address Prefix Provisioning

The following are restrictions pertaining to the DBE Flexible Address Prefix Provisioning feature:

- Only three different lengths of network masks can be in use on a given shared address at one time.
- When multiple mask lengths are used on a shared local address, there is extra overhead of hash key construction and flow entry lookup.

# Full Support for Wildcard Response

Previously Cisco Unified Border Element (SP Edition) distributed model supported H.248 wildcard operations that were restricted to W-Modify or W-Subtract requests, which yielded summary wildcard responses. This feature introduces support for a complete wildcard response. A wildcard H.248 Subtract or Modify operation now returns a complete response with per-termination statistics.

With this enhancement, the MGC is not required to request a summary wildcard response when sending an H.248 Subtract or Modify command with a wildcard context ID and wildcarded termination ID. However, the MGC can request a summary wildcard response if it chooses. The Subtract or Modify command is not rejected if the MGC does not make a summary wildcard request.

Table 6-1 lists the commands and context IDs for the wildcard response.

*Table 6-1 List of Commands and Context IDs*

| Command | Context ID |
|---|---|
| **subtract** | All |
| **auditvalue** | All |
| **modify** | All |

If the resulting responses to these commands get very large, you are advised to turn on the H.248 Segmentation Package Support feature. For more information, see the "H.248 Segmentation Package Support" section on page 7-3. However, if segmentation is not supported and the maximum PDU size is met, the response generates error 533 "Response exceeds maximum transport PDU size".

## Restriction for the DBE Full Support for Wildcard Response

Commands that have wildcard (All) context can occur only once in a request.

## Complete Wildcard Response Example

The following example shows a sample H.248 wildcard Subtract request that yields per-termination statistics:

```
T = 63 {
C = * {
S = */*/*/*/*/*/*/*/*
}}
```

The above wildcard Subtract request produces the following example of a complete wildcard subtract response with segmentation on:

```
P=63/1{
C=25{
S=xyzcompany/sip4/gn/0/1/0/1/ac/13{
SA{EMP/PD=0,NT/OS=0,NT/OR=0,EMP/OD=0,GM/DP=0,EPSTAT/EPJIT=0,EPSTAT/EPPS=0,
EPSTAT/EPPR=0,EPSTAT/EPOS=0,EPSTAT/EPPL=0,EPSTAT/EPDELAY=0,NT/DUR=1628429},
M{ ST=1{ SA{EMP/PD=0,NT/OS=0,NT/OR=0,EMP/OD=0,GM/DP=0,EPSTAT/EPJIT=0,EPSTAT/EPPS=0,
EPSTAT/EPPR=0,EPSTAT/EPOS=0,EPSTAT/EPPL=0,EPSTAT/EPDELAY=0,NT/DUR=1628429}}}}}}

P=63/2{
C=25{
```

```
S=xyzcompany/sip4/gn/0/1/0/1/bb/14{
SA{EMP/PD=0,NT/OS=0,NT/OR=0,EMP/OD=0,GM/DP=0,EPSTAT/EPJIT=0,EPSTAT/EPPS=0,
EPSTAT/EPPR=0,EPSTAT/EPOS=0,EPSTAT/EPPL=0,EPSTAT/EPDELAY=0,NT/DUR=1628429},
M{ ST=1{ SA{EMP/PD=0,NT/OS=0,NT/OR=0,EMP/OD=0,GM/DP=0,EPSTAT/EPJIT=0,EPSTAT/EPPS=0,
EPSTAT/EPPR=0,EPSTAT/EPOS=0,EPSTAT/EPPL=0,EPSTAT/EPDELAY=0,NT/DUR=1628429}}}}}}
```

# H.248 ServiceChange Handoff

The ServiceChange Handoff functionality on Cisco Unified Border Element (SP Edition) distributed model conforms to section 7.2.8, ServiceChange, and section 7.2.8.1.1, ServiceChangeMethod, of the H.248.1v3 Gateway Control Protocol: Version 3. The ServiceChange Handoff functionality allows an MGC to hand over control of an MG to another MGC. The MGC sends a ServiceChange message to the MG with which it is currently associated to request that the MG terminate that association and the MG form a new association with a MGC identified in the ServiceChange message.

The ServiceChangeMethod identifies the type of ServiceChange that occurs. The ServiceChangeMethod used in this functionality is Handoff. A ServiceChange Handoff message is sent from the MGC to the MG to signify that the MGC is being taken out of service, and that the MG needs to establish a new association with another MGC. Then, the next Handoff message is sent from the MG to the MGC to show that the MG is trying to form the new association.

A ServiceChange Handoff is useful when a MGC goes down for maintenance purposes or when a MGC decides to share load with another MGC.

If the MG is not able to connect to the selected MGC because of an access denial or network failure, the MG tries to connect to another MGC by using the ServiceChangeMethod of Failover. The MG sends a ServiceChange Failover message to alternate MGCs that are described in the MGC list and tries to connect with an MGC from the list.

## Debugging Example

You can use the **show sbc dbe controller** command to verify that the ServiceChange Handoff was successful. The command output shows the address of the new MGC and the status of the new MGC association is *Attached*.

The following is an example showing the H.248 controller address of the new MGC that is now associated with the MG and the status of the association:

```
Router# show sbc global dbe controller
SBC Service "global"
  vDBE in default DBE location (4294967295)

   DBE Admin Status:    Active
   DBE Transaction Long Timer  10500 (ms)
   DBE TMAX Timeout            10000 (ms)

    Media gateway controller in use:
      H.248 controller address                    <========= Address of new MGC
        200.40.1.254:2948
      Status:   Attached, since 2008/09/09 12:40:37   <====== Status of the association
```

# In-Service Provisioning of H.248 Controllers

Introduced in Cisco IOS XE Release 2.3, the In-Service Provisioning of H.248 Controllers feature allows you to configure a new MGC or make configuration changes to an existing MGC on the DBE while the SBC is active. The SBC is still in service while controller changes are being made. The in-service provisioning capability ensures that existing pinholes and active calls are not lost.

For example, you can add a new controller to your configuration so it can be used later when the active MGC goes down for maintenance. In that event, the active MGC attached to the DBE sends a ServiceChange message to the DBE to request that the DBE detach from the MGC and attach to the new MGC. The in-service provisioning feature ensures the new controller can be configured and added easily without tearing down existing pinholes and losing calls.

Other examples of configuration changes to a controller include changes to the Interim Authentication Header parameters or to the control address.

If you are running Cisco IOS XE Release 2.2 or earlier, see the "Without the In-Service Provisioning Capability" section on page 6-9 for information on making configuration changes to a controller.

## Restrictions for In-Service Provisioning of H.248 Controllers

You cannot modify the existing controller that is associated with the MGC. You can only modify other controllers in the configuration.

## Configuring a New Controller: Examples

The following **show run** command shows an existing SBC configuration with configured controller 2:

```
Router# show run | be sbc
sbc global dbe
  vdbe global
   h248-version 3
   h248-napt-package napt
   local-port 2974
   control-address h248 ipv4 200.50.1.4
   controller h248 2
    remote-address ipv4 200.50.1.254
    remote-port 2974
   attach-controllers
  deactivation-mode abort
  location-id 1
  media-address ipv4 202.50.2.1
   port-range 10000 60000 any
  media-address ipv4 202.50.3.1
   port-range 10000 60000 any
  media-timeout 1000
  activate
```

The following example shows how to configure a new controller 99 with the **controller h248 99** command:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# controller h248 99
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 99.0.0.1
Router(config-sbc-dbe-vdbe-h248)# remote-port
Router(config-sbc-dbe-vdbe-h248)# remote-port 2799
Router(config-sbc-dbe-vdbe-h248)# ^Z
Router#
```

## Error When Configuring an Attached Controller: Examples

If you try to modify the existing controller that is associated with the MGC, you receive an error message because you can only modify other controllers in the configuration. The following example shows an existing SBC configuration with configured controller 2:

```
Router# show run
*Nov 25 23:53:00.400: %SYS-5-CONFIG_I: Configured from console by console run
| be sbc
sbc global dbe
  vdbe global
   h248-version 3
   h248-napt-package napt
   local-port 2974
   control-address h248 ipv4 200.50.1.4
   controller h248 2
    remote-address ipv4 200.50.1.254
    remote-port 2974
   attach-controllers
  deactivation-mode abort
  location-id 1
  media-address ipv4 202.50.2.1
   port-range 10000 60000 any
  media-address ipv4 202.50.3.1
   port-range 10000 60000 any
  media-timeout 1000
  activate
```

The following example shows the error message received when you try to configure the attached controller 2:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# sbc global dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# controller h248 2
SBC: SBC: Specified controller cannot be changed while it is currently attached
```

## Without the In-Service Provisioning Capability

Without the in-service provisioning capability in releases before Cisco IOS XE Release 2.3, any configuration changes to the MGC require deactivating the DBE (with the **no activate** command), detaching the MGC (with the **no attach-controllers** command), re-attaching the MGC (with the **attach-controllers** command) after making the change, and then reactivating the DBE (with the **activate** command).

If you run a release before Cisco IOS XE Release 2.3, read the following examples for the recommended steps for making global changes to controllers and making changes to individual controller settings.

## Making Global Changes to Controllers: Examples

You have configured H.248 controllers for the DBE and want to make a global change that affects all controllers. Global changes are configured on the DBE and consist of changing any one of the following:

- Control address
- Local port
- Use-any-local-port

**Note** You cannot make global changes to controllers while controllers are configured. You cannot delete a controller while the controller is attached.

To change the control address and local port that globally affect configured controllers, we recommend the following steps:

1. Deactivate the DBE with the **no activate** command.
2. Enter into VDBE configuration mode with the **vdbe** command.
3. Detach the controller with the **no attach-controllers** command.
4. Delete any configured controllers with the **no controller h248** command.
5. Make the change to the control address or local port.
6. Add the controllers back with the **controller h248** command.
7. Reconfigure the individual settings configured on each controller, such as the remote address, remote port, and transport configuration, that were removed with the **no controller h248** command.
8. Exit the Controller H.248 configuration mode with the **exit** command.
9. Re-attach each controller with the **attach-controllers** command.
10. Exit the VDBE configuration mode with the **exit** command.
11. Reactive the DBE with the **activate** command.

The following example shows the initial SBC configuration:

```
sbc mySbc dbe
 vdbe global
  use-any-local-port
  control-address h248 ipv4 172.25.2.26
  controller h248 1
   remote-address ipv4 172.25.2.243
   remote-port 2946
   transport udp
  attach-controllers
 activate
 location-id 1
 media-address ipv4 20.20.20.20
 media-address ipv4 21.21.21.21
```

The following example illustrates a user trying to change the local port number while the controllers are configured and receiving an error message:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# sbc mySbc dbe
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# local-port 2946
```

```
SBC: local-port cannot be changed while controllers are configured.
```

The following example illustrates the user following the recommended steps to change the local port:

```
Router(config-sbc-dbe-vdbe)# exit
Router(config-sbc-dbe)# no activate
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# no attach-controllers
Router(config-sbc-dbe-vdbe)# no controller h248 1
Router(config-sbc-dbe-vdbe)# local-port 2946      <== Make change to local port
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 172.25.2.243 <== Reconfigure
Router(config-sbc-dbe-vdbe-h248)# remote-port 2946                 <== Reconfigure
Router(config-sbc-dbe-vdbe-h248)# transport udp                    <== Reconfigure
Router(config-sbc-dbe-vdbe-h248)# exit
Router(config-sbc-dbe-vdbe)# attach-controllers       <== Re-attach controller
Router(config-sbc-dbe-vdbe)# exit
Router(config-sbc-dbe)# activate                      <== Reactivate the DBE
Router(config-sbc-dbe)# end
```

The following example shows the modified running SBC configuration:

```
sbc mySbc dbe
 vdbe global
  local-port 2946
  control-address h248 ipv4 172.25.2.26
  controller h248 1
   remote-address ipv4 172.25.2.243
   remote-port 2946
   transport udp
  attach-controllers
 activate
 location-id 1
 media-address ipv4 20.20.20.20
 media-address ipv4 21.21.21.21
```

## Making Changes to Individual Controller Settings: Examples

You can change an individual setting on a controller that is already configured. Individual controller-specific settings include any one of the following:

- Remote address
- Remote port
- Transport type

**Note** You cannot change an individual controller setting (remote address, remote port, or transport type) unless you detach the controller first.

To change the remote address, remote port, or transport type setting on a controller, we recommend the following steps:

1. Deactivate the DBE with the **no activate** command.
2. Enter into VDBE configuration mode with the **vdbe** command.
3. Detach the controller with the **no attach-controllers** command.
4. Enter into Controller H.248 configuration mode with the **controller h248** command.

5. Make the change to the remote address, remote port, or transport type.
6. Exit the Controller H.248 configuration mode with the **exit** command.
7. Re-attach the controller with the **attach-controllers** command.
8. Exit the VDBE configuration mode with the **exit** command.
9. Reactivate the DBE with the **activate** command.

The following example shows the initial configuration:

```
sbc mySbc dbe
 vdbe global
  use-any-local-port
  control-address h248 ipv4 172.25.2.26
  controller h248 1
   remote-address ipv4 172.25.2.243
  attach-controllers
 activate
 location-id 1
 media-address ipv4 20.20.20.20
 media-address ipv4 21.21.21.21
```

The following example illustrates a user trying to change the remote address and receiving an error message:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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-address ipv4 210.229.108.253
SBC: remote-address cannot be changed while controllers are attached.
```

The following example illustrates the user following the recommended steps to change the remote address:

```
Router(config-sbc-dbe-vdbe-h248)# exit
Router(config-sbc-dbe-vdbe)# exit
Router(config-sbc-dbe)# no activate
Router(config-sbc-dbe)# vdbe
Router(config-sbc-dbe-vdbe)# no attach-controllers
Router(config-sbc-dbe-vdbe)# controller h248 1
Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 210.229.108.253<= change remote addr
Router(config-sbc-dbe-vdbe-h248)# exit
Router(config-sbc-dbe-vdbe)# attach-controllers
Router(config-sbc-dbe-vdbe)# exit
Router(config-sbc-dbe)# activate
Router(config-sbc-dbe)# end
```

The following example shows the modified running SBC configuration:

```
sbc mySbc dbe
 vdbe global
  use-any-local-port
  control-address h248 ipv4 172.25.2.26
  controller h248 1
   remote-address ipv4 210.229.108.253
  attach-controllers
 activate
 location-id 1
 media-address ipv4 20.20.20.20
 media-address ipv4 21.21.21.21
```

# IPsec Pinhole Support—Twice NAT for IPv4 and No NAT for IPv6

This enhancement adds support for voice calls over IP Security (IPSec) tunnels and adds support for IPsec address-only pinholes. This support enables the DBE to forward IPsec packets when the port cannot be determined because the port is within the encrypted portion of the frame. Thus, IPsec support handles the IPsec requirement that does not allow use of port numbers for session lookup or translation. Currently, single IPsec pinholes are supported.

IPsec support introduces a new port type of Encapsulating Security Payload (ESP) to indicate IPsec ESP pinholes. The new port type allows ESP address-only pinholes to be configured. ESP pinholes are identified by the transport identifier "ESP" and a port equal to zero.

IPsec support enables the flow of IPsec traffic through an address-only pinhole and supports ESP tunnel mode, where the IP header and payload of the IP packet is encrypted. The ESP data operates directly on top of IP, using IP protocol number 50.

Cisco Unified Border Element (SP Edition) does not encrypt or decrypt any IPsec traffic.
Cisco Unified Border Element (SP Edition) merely passes the encrypted packets after applying SBC policies, such as policing and latching. Because packets flowing through the IPsec pinholes are encrypted, the DBE is unable to read the endpoint statistics from a RTP Control Protocol (RTCP) stream or generation and detection of in-band dual-tone multifrequency (DTMF) tones.

The Session Description Protocol (SDP) to create an IPsec NAT mode pinhole using the ESP identifier is as follows:

m=<*media*> 0 ESP <fmt-list>, where media is audio, video, or application.

Both media and signaling IPsec address-only pinholes are supported. When the media is audio or video, the pinholes are created as media flow pairs. When the media is an application, the pinholes are created as signaling flow pairs.

If the port is not zero when the ESP tag is applied or the <*media*> tag is not audio, video, or application, the SDP is rejected with error 515, "Unsupported media type".

An Internet Key Exchange (IKE) session can be established for IPsec pinholes. An IKE session is a session in which IPsec endpoints commonly establish the security association between peers using the IKE protocol. An IKE session is typically a UDP session with port number 500. However, when a single pinhole is used for both an IKE session and ESP media, only the ESP pinhole is created and the IKE pinhole is not created.

The following models of IPsec address-only pinholes are supported on the DBE:

- IPv4 single Twice-NAT pinhole

  In this model, the IPv4 IKE session and ESP data packets use a single Twice-NAT pinhole. Twice-NAT IPsec pinholes need additional configuration on the DBE. Two addresses are needed on the DBE for every Twice-NAT IPsec pinhole. See the "Related Commands and Command Examples" section on page 6-14 for CLI information.

  The MGC requests that the DBE choose the local address for both terminations A and B. However, the MGC can also select the local address.

- IPv6 single No-NAT pinhole

  In this model, the IPv6 IKE session and ESP data use a single No-NAT pinhole. The MGC allocates the local address.

## Related Commands and Command Examples

The **nat-mode twice-nat** keywords have been added to the **media-address ipv4**, **media-address ipv6**, **media-address pool ipv4**, and **media-address pool ipv6** commands to allow the user to configure media addresses in the **nat-mode twice-nat** mode. The NAT mode allows local addresses to be reserved for Twice-NAT pinholes.

For more information on these commands, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

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 IPsec 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)# end
```

The following example configures IPv6 address 5::1:1 as the local address, and it is reserved for Twice-NAT IPsec 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 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 IPsec 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 adds IPv6 addresses from 5::1:1 to 5::1:10 to the media address pool as local addresses, reserved for Twice-NAT IPsec 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
```

## Restrictions for DBE IPsec Pinhole Support

The following are restrictions pertaining to the DBE support for this feature:

- 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.
- DBE functionality is only applied to the Layer 3 IP header. RTCP endpoint statistics, DTMF detection and generation, and other media-related query capabilities are lost when IPsec pinholes are created.
- IPsec address-only pinholes do not support sharing of local address and port between multiple pinholes.
- When a specific bandwidth has not been supplied, either through an SDP b line or H.248 Tman properties, the DBE does not rate limit IPsec pinhole traffic.

## Restrictions for ISSU Downgrade

The ISSU Downgrade restrictions pertaining to this feature are as follows:

- Pinholes that use IPsec address-only pinholes cannot be supported on software releases earlier than Cisco IOS XE Release 2.2.
- While in a downgrade process during an In-Service Software Upgrade (ISSU), IPsec address-only pinholes are lost.

## Debugging Tips

The debugging tips for the ISSU downgrade feature are as follows:

- Debug IPsec pinholes by using the **show sbc dbe signaling-flow-stats** or **show sbc dbe media-flow-stats** commands. Note that RTCP statistics are not available because RTCP packets are encrypted.
- If the pinhole creation for IPv4 Twice NAT fails, check whether there are sufficient addresses in the media address pools.

# Local Source Properties (Address and Port)

The Local Source Properties (Address and Port) feature is described in the "Local Source Properties (Address and Port)" section on page 9-11.

# Locally Hairpinned Sessions

The DBE supports hairpinning of calls between subscribers connected to the same DBE for IPv4 and IPv6 packets. A hairpin consists of two pinholes or two pairs of terminations on the DBE that the MGC has provisioned with local and remote addresses whereby media from one pinhole should travel directly (loops back) to the other pinhole. The MGC (also known as an SBE) does not differentiate whether Add requests are sent to the same or different DBEs for a flow setup.

In a hairpin media call flow setup, two pairs of terminations internally connect the backbone (BB) side to logically merge two separate DBEs into one DBE. The flow resembles a hairpin.

This feature is useful for interoperation with SBEs that provision two pinholes, even in the case in which the SBE does not require media to be sent further into the network.

**Note** *Pinhole* is an informal term for a pair of terminations in the same stream and same context.

## Twice NAPT Pinhole Hairpinning

The DBE successfully forwards media through Twice Network Address and Port Translation (NAPT) pinholes that form a hairpin. For Twice NAPT hairpinning, the DBE forwards media on demand. The SBE sees no differences between Twice NAPT hairpins and Twice NAPT non-hairpins.

When forwarding media, a hairpin behaves the way two separate pinholes behave, except that a packet going through a coupled pair has its IP Time-to-Live (TTL) counter decremented only once, not twice.

**Note** Twice NAPT is only supported on IPv4.

## No NAPT Pinhole Hairpinning

The No NAPT pinholes can form hairpins only under the following circumstances:

- Both pinholes are No NAPT.
- Each “internal termination” has local and remote addresses that are identical to those of the external termination on the associated pinhole.

  **Note** The two terminations between which media loops back are called the “internal terminations” of their respective pinholes. Only external terminations directly receive packets from the network.

- Any remote source address masks (rsams) are duplicated. For example, if a termination with remote address A in one pinhole has an rsam of 1111:2222:3333:4444::/48, the termination with remote address A in the other pinhole also has an rsam of 1111:2222:3333:4444::/48.

## Restrictions for DBE No NAPT Pinhole Hairpinning

The following are DBE restrictions pertaining to the Locally Hairpinned Sessions feature:

- For No NAPT pinholes, the DBE chooses the internal terminations as follows:
  - First specified termination is chosen to be internal.
  - Other termination is chosen accordingly from the other pinhole. If the termination with remote address A on one pinhole is internal, the termination with local address A on the other pinhole is also internal.
  - DBE does not support choosing internal terminations based on termination names.
- For No NAPT hairpins, any Network Address Translation (NAT) latching requests are duplicated. For example, if a termination with remote address A in one pinhole requests NAT latching, the termination with remote address A in the other pinhole must also request NAT latching. The “request NAT latching” can be done using the ipnapt/latch H.248 signal.
- Hairpin in which both external terminations are provisioned with the NAT latching instruction cannot latch and cannot forward media. No NAPT pinholes are not allowed to (re)latch to the remote addresses on both sides.
- IPv6 hairpins are supported on UDP and TCP.
- Single NAPT pinhole hairpins are not supported.

# MGC-Specified Local Addresses or Ports

This feature allows an MGC to specify a local address or port for media and signaling flows through the DBE. The MGC specifies a specific address or port for terminations in H.248 Add and Modify requests, instead of using the CHOOSE wildcard.

If either address or port is not specified, it is selected by the DBE from one of the DBE-managed address ranges.

The following error messages describe how the functionality has failed:

- Requested address and port do not belong to a range that has been configured on the DBE with the appropriate class of service for the flow.

  Megaco error 421 “Unknown action or illegal combination of actions”.
- Media port number requested is an odd number.
  Megaco error 500 “Internal Software Failure”.
- Request attempted to change the local address and port for an existing flow.
  Megaco error 501 “Not Implemented”.
- Requested address or port is already in use by another flow, or was in use by a recently deleted flow.
  Megaco error 510 “Insufficient Resources”.

## Restrictions for DBE MGC-Specified Local Addresses or Ports

The following are restrictions pertaining to the DBE support for this feature:

- Addresses and ports specified must fall within a valid address or port range configured on the DBE, and not marked as “MGC-managed”.
- Class of service of the port range must match the type of flow being allocated.
- Real-time Transport Protocol (RTP) flows cannot be set up to use odd-numbered ports.

# MultiStream Terminations

This enhancement allows a single H.248 termination to contain multiple streams. Previously, only a single stream for each termination was allowed, which meant that multi-stream calls needed to be signaled using multiple pairs of terminations. This enhancement supports the new H.248.1v3 syntax in which several streams can occupy the same termination.

## Restrictions for DBE MultiStream Terminations

Auditing of per-stream statistics is only supported when using H.248.1v3. This is a restriction of the H.248 protocol.

# Nine-Tier Termination Name Hierarchy

The Nine-Tier Termination Name Hierarchy feature adds support for a nine-tier termination name schema, where the multi-tier prefix is supplied by the MGC, and the final element, the channel ID, is generated by the media gateway (MG). All MGCs that the MG is configured to contact must use the same termination name schema. A termination is the point of entry or exit of media flows relative to the MG. The MG understands how the flows entering and leaving each termination are related to each other.

This feature plays an important role in identifying the company, transaction service (such as voice or video), and termination attributes (such as access and backbone).

## Restrictions for Nine-Tier Termination Name Hierarchy

The following are restrictions pertaining to the Nine-Tier Termination Name Hierarchy feature:

- Only the final element may contain the CHOOSE wildcard ($). The DBE will not extract any meaning from any elements of the termination ID, except " * " is reserved for wildcard notation.
- Multitier prefixes can be less than nine tiers, but must have the same depth.

## Information About the Nine-Tier Termination Name Hierarchy

The MG assigns a *channel ID* that is unique across all terminations realized on the DBE. Using a unique channel ID ensures that the termination ID, as a whole, is unique across all terminations on the DBE. If a multi-tier prefix is not desired, the MGC may use a CHOOSE wildcard ($) for the termination ID, in which case the MG allocates a prefix in the form: **ip/**<*flow-id*>.

The only element within the hierarchy that may contain the CHOOSE attribute in an ADD request from the MGC is the channel element, which is the final element. The full termination name is stored persistently.

The termination naming hierarchy is extended to include nine tiers and is defined as follows:

```
<operator> / <service> / <subscriber-class> / <Reserved1> / <physical-interface-id> /
<Reserved2> / <sub-interface-id> / <termination-attribute> / <channel>

<operator> : "yourcompanyname", "com", "others"
<service> : "sip", "voice", "video", "vphone" (video-phone),"mon" (monitor), "others"
<subscriber-class> : "gn" (public), "ur" (priority), "ur1" (emergency)
<Reserved1> : digit (0-15)
<physical-interface-id> : digit (0-1023)
<Reserved2> : digit (0-4095)
<sub-interface-id> : digit (0-4095)
<termination-attribute> : "dc" (d.c.), "ac" (access), "bb" (backbone),"mon" (monitor)
<channel> : digit (0-4294967295)
```

## Displaying the Nine-Tier Termination Name Hierarchy

The **show sbc dbe media-flow-stats** command is extended to include the full-termination ID in the response.

For a description of this command, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

# Displaying the Nine-Tier Termination Name Hierarchy: Example

This section provides an example of the reported fields for the **show** command displaying the nine-tier termination name hierarchy: abc/voice/gn/0/1/0/1/ac/3

The entry `Media flowing = Yes` 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 Cisco Unified Border Element (SP Edition) distributed model has not yet had a chance to observe whether media is flowing or not.

The statistics starting with `RTCP` are maintained and collected in real time when the **show sbc dbe media-flow-stats detail** command is issued.

The following example shows detailed statistics from an IPv4 media flow collected on the DBE:

```
Router# show sbc mySbc dbe media-flow-stats detail

SBC Service "mySbc"
  Media Flow:
    Context ID:          1
    Stream ID:           2
    State of Media Flow: Active
    Call Established Time: 23:50:20 UTC Jun 21 2007
    Flow Priority:       Routine
    Side A:
      Name                        abc/voice/gn/0/1/0/1/ac/3
      Reserved Bandwidth:         12 (bytes/second)
      Status                      InService
      VRF Name:                   Global
      VLAN Tags(Priorities):      0(0), 0(0)
      Local Address:              202.50.255.113
      Local Port:                 20000
      Remote Address:             100.50.255.110
      Remote Port:                20000
      Remote Source Address Mask: 100.50.255.0/24
      Packets Received:           2272
      Packets Sent:               1784
      Packets Discarded:          0
      Data Received:              266 (bytes)
      Data Sent:                  209 (bytes)
      Data Discarded:             0 (bytes)
      GM Discarded Packets:       0
      Time To Recovery:           Not known
      RTCP Packets Sent:       Not known
      RTCP Packets Received:   Not known
      RTCP Packets Lost:       Not known
      DTMF Interworking:          No
      Media Flowing:              Yes
      Unexpected SrcAddr Packets: No
      Billing ID:                 000000000000000000000000000000000000000000000000
      Media directions allowed:  sendrecv
    Side B:
      Name                        abc/voice/gn/0/1/0/1/bb/4
      Reserved Bandwidth:         23 (bytes/second)
      Status                      InService
      VRF Name:                   Global
      VLAN Tags(Priorities):      0(0), 0(0)
      Local Address:              202.50.255.113
      Local Port:                 20002
      Remote Address:             200.50.255.110
      Remote Port:                30000
      Packets Received:           2249
      Packets Sent:               2272
Packets Discarded:          465
Data Received:              263 (bytes)
Data Sent:                  266 (bytes)
Data Discarded:             54 (bytes)
GM Discarded Packets:       0
Time To Recovery:           Not known
RTCP Packets Sent:       Not known
RTCP Packets Received:   Not known
RTCP Packets Lost:       Not known
DTMF Interworking:          No
Media Flowing:              Yes
Unexpected SrcAddr Packets: No
Billing ID:                 000000000000000000000000000000000000000000000000
Media directions allowed:  sendrecv
```

# Optional Local and Remote Descriptors

The MGC can specify one or more local and remote descriptors in a **Modify** command because the MGC does not always specify the descriptors in a single **Add** command. A descriptor might be an address or port allocation or bandwidth reservation.

The DBE process for adding or modifying local and remote descriptors is as follows:

- DBE accepts **Add** or **Modify** commands for a termination with zero or one local descriptor and zero or one remote descriptor for each stream.
- DBE reserves resources for a pinhole when the first local descriptor for either side of the pinhole is specified. This includes, but is not necessarily limited to, address and port allocation and bandwidth reservation. If the DBE resource reservation fails, one of the following may occur:
  - If the Ginfo package is in use and the Ginfo or gate_state is provisional, then the gate is deleted and the Add or Modify request is returned with error 510 “failure response code of insufficient resources”.
  - Gate reverts to its previous state and the Add or Modify request is returned with error 510 “failure response code of insufficient resources”. MGC deletes the gate if required.

**Note** If both local SDP and remote SDP are included in an H.248 message, the codec mentioned in both descriptors must be the same. Otherwise, the DBE rejects the message because the DBE does not support codec selection across the local and remote descriptors. You can use the **symmetric-payload-types** command to disable checking for asymmetric payload types in the local and remote descriptors for a call flow. After you run the **symmetric-payload-types** command, the local and remote descriptors can contain different codecs. You can use the **no** form of this command to enable checking for asymmetric payload types.

## Restrictions for DBE Optional Local and Remote Descriptors

The following are restrictions pertaining to DBE support for this feature:

- DBE rejects attempts to change the addresses and ports in the local descriptor after they have been selected.

- Partially specified terminations (those without both a local and remote descriptor) must have a termination state of OutOfService. If an attempt is made to place a partially specified termination InService, then the request is rejected with error 421, "Unknown action or illegal combination of actions response."

# Remote Source Address Mask Filtering

The Remote Source Address Mask Filtering feature is described in the "Remote Source Address Mask Filtering" section on page 9-12.

# Return Local and Remote Descriptors in H.248 Reply

Before Cisco IOS XE Release 2.6, the DBE behavior was to return a local or remote descriptor in an H.248 Reply only if the descriptor was either under-specified or over-specified in the associated request. Under-specified means the SBE includes "$" 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.

However, some H.248 interworking cases between the DBE and signaling border element (SBE) required the ability and flexibility of the DBE to always return the local and remote descriptors in an H.248 Reply. In Cisco IOS XE Release 2.6, the Return Local and Remote Descriptors in the H.248 Reply feature provides that capability.

This feature uses the **local-remote-desc always** command to configure the DBE to always return the local and remote descriptors in an H.248 Reply if the descriptors were present in the H.248 request. This function enhances H.248 interoperability with the SBE.

## Configuration Examples

The following example shows how to configure the DBE to always include the local and remote descriptor in an H.248 Reply, if those descriptors were present in the H.248 request:

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

In the following example, use 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)# vdbe global
Router(config-sbc-dbe-vdbe)# no local-remote-desc always
```

# RTP-Specific Behavior Support

This feature adds support for the RTP Specific Behavior (rsb) property of the ETSI TS 102 333 version 1.1.2 Gate Management (GM) package. This support allows the MGC to disable RTP-specific behavior for a given termination. In this case, the MGC overrides the default DBE behavior for RTP flows.

Terminations representing gates for RTP traffic typically require two streams per media (one for RTP packets, one for RTCP packets). Mono media sessions require two bidirectional streams, whereas a multimedia session with voice and video traffic would require four streams.

Setting the property value to OFF overrides the default DBE behavior in the following ways:

- DBE does not open the RTCP port for the given RTP flow. However, the RTCP port is not available for use by other flows.
- DBE does not reserve additional resources (equal to 5 percent of those required for the RTP flow) for processing the RTCP stream.

## Restrictions for DBE RTP-Specific Behavior Support

Enabling or disabling the property value is valid only for RTP flows. It is ignored for other types of flows.

# ServiceChange Notification for Interface Status Change

This feature enables the media gateway (MG) to generate a ServiceChange H.248 notification to the MGC containing the termination ID of the physical interface on the DBE when the interface experiences status changes. The termination ID is a nine-tier name string associated with a pinhole or pair of terminations and it contains a physical-interface-id supplied by the user. For example, the MG notifies the MGC when a group of terminations is taken out of service (link down) or returned to service (link up).

Although notification of interface status changes can be obtained via SNMP, this feature provides a more reliable transport than SNMP and consolidates the information on the MGC for simpler management.

The MGC is also referred to as SBE.

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 MG is able to report a service change with that particular termination ID to the SBE.

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 name string such as “xyzcompany”. In this case, the MG reports “xyzcompany/*/*/*/<*interface-id*>/*/*/*/*” to the MGC with the ServiceChange notification. The default value of the termination ID rootidname is “Cisco”.

**Note** For more details on the **sbc interface-id** and **termination-id rootidname** commands, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at: http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

The ServiceChange H.248 notification is generated by any of the following events:

- Link up and link down.

  For link up—MG Service Restoration event. The ServiceChangeMethod is Restart and the ServiceChangeReason is 900 (Service Restored).

For link down—MG Service Cancellation event. The ServiceChangeMethod is Forced and the ServiceChangeReason is 905 (Term taken Out Of Service).

- Interface shutdown or interface online insertion and removal (OIR).

The ServiceChange Notification for Interface Status Change feature has the following restrictions and conditions:

- It is only supported on EtherChannel (gigabit EtherChannel and fast EtherChannel) and on all Ethernet interfaces. EtherChannel may also be called port channel.
- The **sbc interface-id** command 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.
- If an interface configured with the **sbc interface-id** command goes down, the affected terminations are marked “Out Of Service”. If the DBE then receives an H.248 ADD or MODIFY request that moves one of these affected terminations to “in-service,” although the interface is marked “down,” the ADD or MODIFY request is not rejected. The request can move the termination state to “in-service,” even though the interface cannot accept any packets until it goes up. When the interface changes status to either up or down, the MG reports a service change with the affected termination IDs to the SBE.

**Note** The ServiceChange procedure is described in H.248.1v3 Annex F.

# Configuring the ServiceChange Notification for Interface Status Change

This section contains steps to configure the ServiceChange Notification for Interface Status Change feature on the Cisco ASR 1000 Series Routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **sbc interface-id** {*value*}
5. **end**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **`interface`** *`type number`*<br>Example:<br>`Router(config)# interface port-channel 99` | Configures an interface type and enters into interface configuration mode. |
| **Step 4** | **`sbc interface-id`** `{`*`value`*`}`<br>**Example:**<br>`Router(config-if)# sbc interface-id 2` | Maps the physical-interface-id contained in the termination ID for the pinhole to the port channel interface. |
| **Step 5** | **`end`**<br>**Example:**<br>`Router(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |

### Example

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/*/*/*/*
```

# SBC End-Point Switching

The SBC End-Point Switching feature enhances the user experience for a caller while the call is in setup mode.

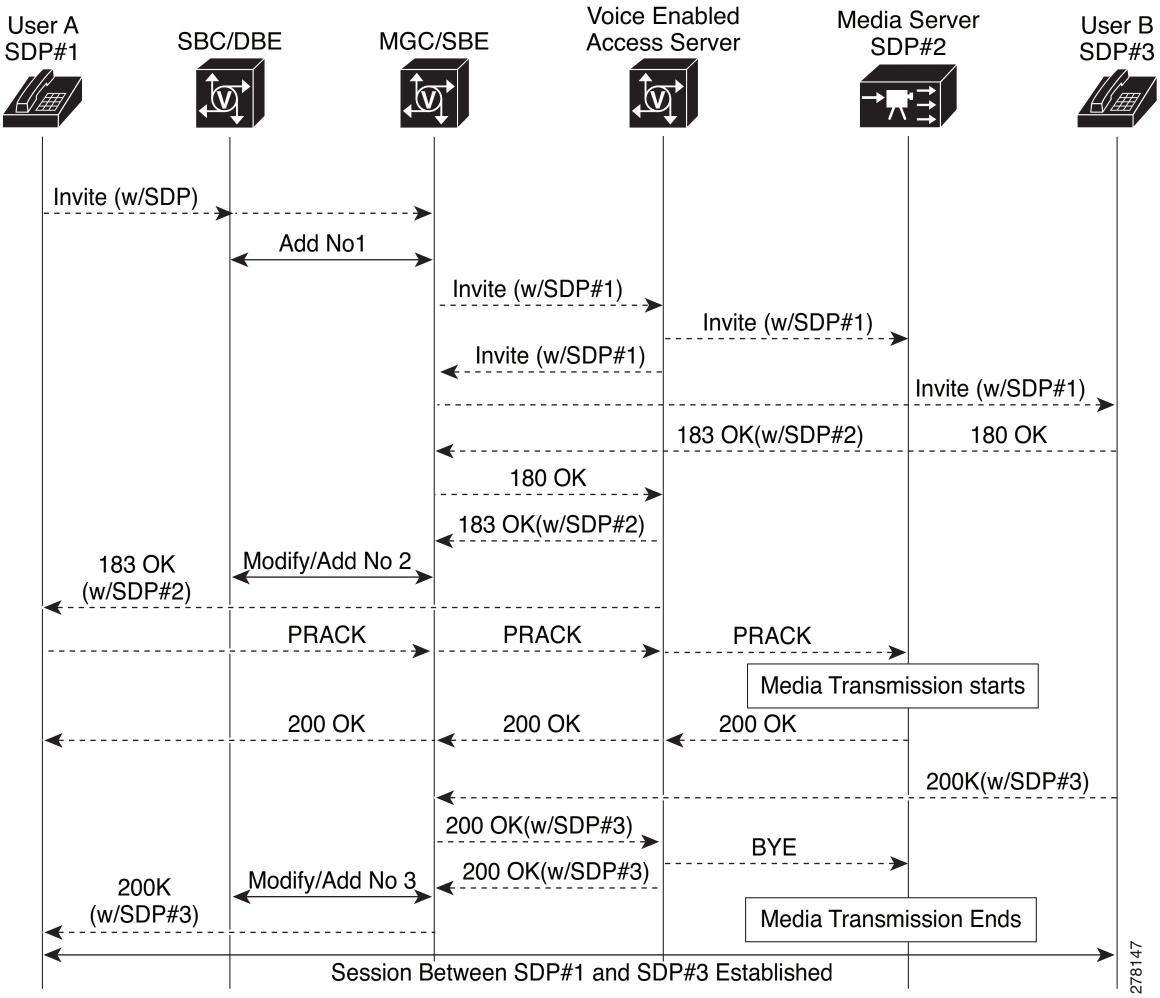
Currently, when a call originates, during the call setup mode, there would be a silence at the other end or the caller hear various tones—such as waiting tone. With End-Point Switching, calls are redirected to a media server. Media server then plays a music instead of a tone until the callee picks up the call. As soon as the callee picks up the call, the redirection to the Media Server is removed and the two End-Points are connected.

End-Point switching feature is available for the following types of calls:

- Basic regular Calls (IPv4 - Twice NAPT [Network Address and Port Translation], IPv6 - No NAPT)
- Single and Double Hairpininng Calls (IPv4 - Twice NAPT, IPv6 - No NAPT)

Figure 6-1 shows the message flow between User A and User B in an IPv4 environment:

*Figure 6-1 End-Point Switching — Message Flow*



# T-MAX Timer

The T-MAX timer is a timer that limits the maximum delay of retransmissions by the H.248 stack on a DBE when sending messages to the MGC.

## Related Command

The **tmax-timer** command configures the value of the T-MAX timer.

# H.248 Timers

The Version 2 of H.248 BaseRoot package, as defined in H.248.1v3, allows the MGC to indicate the following timers:

- normalMGCExecutionTime—Interval within which the MG expects to receive a transaction response from the MGC (excluding any network delay).
- MGCProvisionalResponseTimerValue—Interval within which the MG expects to receive a pending response from the MGC if the transaction cannot be completed. This interval includes the normalMGCExecutionTime timer and any network delay.

The T-MAX timer has an upper limit on the interval between the initial transmission of a transaction request and the receipt of any response. A device considers a transaction as a failure if no response is received within this interval.

Conditions that lead to H.248 association failures are as follows:

- If a ServiceChange request for the ROOT termination times out, the DBE treats the H.248 association as a failure.
- If an event notification for the Inactivity Timer (**IT/ITO**) event times out, the maximum retransmission number is hit, or normalMGCExecutionTime or T-MAX timer expires, DBE treats the H.248 association as a failure.
- If other event notifications time out, behavior of the SBC depends on the configuration of the **h248-association-timeout** command. If the command is configured, time out of any event notifications causes failure of H.248 association.

**Note** The **h248-inactivity-duration** command configures the Inactivity timer. The duration of the Inactivity timer is the time the DBE waits to hear from the MGC before generating an **IT/ITO** event notification request. This timer does not affect how long it takes for an **IT/ITO** event to time out and fail.

Prior to Cisco IOS Release 2.6.2, the T-MAX timer would use the lower values of the normalMGCExecutionTime and MGCProvisionalResponseTimerValue timers, if specified by the MGC in the baseroot package, replacing the configured T-MAX timer value. From Cisco IOS Release 2.6.2 onwards, the default behavior is to use the locally configured T-MAX timer value. The T-MAX timer value can be configured using the **tmax-timer** command.

Apart from T-MAX, normalMGCExecutionTime, and MGCProvisionalResponseTimerValue timers, there are following related H.248 timers:

- normalMGExecutionTime—Interval within which the MGC expects to receive a transaction final response from the MG (excluding any network delay).
- MGProvisionalResponseTimerValue—Interval within which the MGC expects to receive a pending response from the MG if the transaction cannot be completed. This interval includes the normalMGExecutionTime timer and any network delay.
- Maximum inactivity timer—This timer specifies the period of H.248 messaging silence that the MG applies to the process of monitoring incoming H.248 messages. Whenever the period of silence is exceeded, the MG generates a Notify Request with the **IT/ITO** ObservedEvent.
- LONG-TIMER—This timer is the period of time that H.248 responses should be stored by a device before receiving its response acknowledgement. LONG-TIMER duration is defined by the protocol to be equal to the T-MAX timer and the expected network delay.

## Configuring an H.248 Timer

This section contains steps to configure a T-MAX timer. By default, the T-MAX timer uses the value configured by the **tmax-timer** command. However, you can also configure the T-MAX timer to use the MGC specified value, the smaller value of normalMGCExecutionTime or MGCProvisionalResponseTimerValue timer by using the **tmax baseroot** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sbc** {*sbc-name*} **dbe**
4. **vdbe** [**global**]
5. **tmax-timer** {*timer-value*}
6. **tmax baseroot**
7. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **sbc** {*sbc-name*} **dbe**<br>**Example:**<br>`Router(config)# sbc global dbe` | Creates the DBE service on the SBC and enters into SBC-DBE configuration mode. |
| **Step 4** | **vdbe** [**global**]<br>**Example:**<br>`Router(config-sbc-dbe)# vdbe global` | Enters into VDBE configuration mode with a default DBE named “global”.<br>Only one DBE is supported, and its name must be “global”. |
| **Step 5** | **tmax-timer** {*timer-value*}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# tmax-timer 20` | Defines the value of the T-MAX timer, which limits the maximum delay of retransmissions by the H.248 stack on a DBE when sending messages to the MGC. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **tmax baseroot**<br><br>**Example:**<br>Router(config-sbc-dbe-vdbe)# tmax baseroot | (Optional) Configures T-MAX timer to use the baseroot package value.<br>The T-MAX timer chooses the smaller value of either the normalMGCExecutionTime or MGCProvisionalResponseTimerValue timer that is specified by the MGC root package.<br>If the T-MAX timer is not configured to use the baseroot package value, by default, the T-MAX timer uses the value configured by the **tmax-timer** command. |
| **Step 7** | **exit**<br><br>**Example:**<br>Router(config-sbc-dbe-vdbe)# exit | Exits VDBE configuration mode. |

## Examples

The following example shows how to configure the value of the T-MAX timer that is the default behavior of the H.248 Timers feature:

```
Router# configure terminal
Router# sbc sbc dbe
Router(config-sbc-dbe)# vdbe global
Router(config-sbc-dbe-vdbe)# tmax-timer 20
```

The following example shows how to configure the T-MAX timer to use the MGC specified value, the smaller value of the normalMGCExecutionTime or MGCProvisionalResponseTimerValue timer:

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

# tsc-Delay Timer

The tsc-delay timer is a timer used to delay entry into the tsc-quiesce state. Delaying entry into the tsc-quiesce state delays closing all the signaling pinholes gracefully and delaying a TerminationState of OutOfService, where the tsc/gtd property is set to ON.

The tsc-delay timer is started when an H.248 Subtract command deletes the final termination from a context that does not have the tsc/gtd property set to ON. This delay provides a window during which closing SIP messages can flow to the endpoints before the signaling pinhole is closed by the media gateway (MG) and the context enters the tsc-quiesce state. After the tsc-delay timer expires, the context enters the tsc-quiesce state, the signaling pinhole is closed, and (if subscribed) the MG generates H.248 event notifications for the tsc/dc event.

The tsc-delay timer is set to a value of 2 seconds.

For more information on the tsc-quiesce state, see the "H.248 Termination State Control Package" section on page 7-5.

## Restrictions for DBE tsc-Delay Timer

The following are restrictions pertaining to DBE support for the tsc-delay timer:

- If an H.248 Modify command explicitly changes the tsc/gtd property so that all terminations within the context have the tsc/gtd property set to ON, the tsc-delay timer is not started and the tsc-quiesce state occurs immediately.
- Duration of the tsc-delay timer cannot be modified.
- While the tsc-delay timer is running for a context, the MG can accept further programming for that context. If, because of this interim programming, the context is no longer in the tsc-quiesce state (for example, if new streams are added without the tsc/gtd property set or the tsc/gtd property is changed for existing streams), the tsc-delay timer stops and no further action is taken unless the context re-enters the tsc-quiesce state at a later time.

# Video on Demand Support

Cisco Unified Border Element (SP Edition) distributed model supports Video on Demand (VoD) systems, enabling users to select and watch or listen to video and audio content over a network as part of an interactive television system. VoD systems can either stream content through a set-top box that allows the user to view in real time, such as pay-per-view, or download content to a delivery device for future viewing. Delivery devices include computers, digital video recorders, personal video recorders, portable media players, mobile phones, and any system that can receive on-demand audio-visual content over a network.

Cisco Unified Border Element (SP Edition) distributed model supports different methods for delivering VoD packets over the Internet.

One method assumes that all flows of Real-Time Streaming Protocol (RTSP), RTP, RTCP, and Forward Error Correction (FEC) are delivered over one TCP connection that is started by the client side.

This method includes the following features:

- TCP connection is always initiated by the client side.
- Local address and port number on the client or user side are specifically assigned by the SBE.
- Local address and port number on the backbone or server side are “any,” based on the media flow being supported by IPv6 No NAPT TCP with latching.

Another method assumes that all flows of RTSP are delivered over TCP connections that are started by the client side. Each flow of RTP for video, RTCP for video, and RTP for FEC is delivered over each corresponding User Datagram Protocol (UDP) connection. In addition, when RTCP for FEC is used, it is delivered over a separate UDP connection.

This method includes the following features:

- RTCP port number is always RTP port + 1. This is done by the SBE instructing the DBE to set the Real-Time Transport Protocol (RTP) Specific Behavior (rsb) property of the Gate Management package to rsb=ON at assignment of the RTCP port number.
- SBE assigns the RTP and FEC port numbers because the media flow support is IPv6 No NAPT.

CHAPTER 7

# H.248 Packages—Signaling and Control

The data border element (DBE) deployment of Cisco Unified Border Element (SP Edition) distributed model supports standard H.248 packages that are used to make the Cisco ASR 1000 Series Router function as the DBE in distributed mode. H.248 packages are described or cross-referenced in this chapter.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:
http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

## Contents

This chapter provides information about the following topics:

# Enabling the Optional H.248 Packages

H.248 profiles define option values, sets of packages, naming conventions, and other details for an entire set of applications. The Cisco Unified Border Element (SP Edition) DBE deployment for the Cisco ASR 1000 Series Routers currently supports only one such profile, SBC_GateControl. The SBC_GateControl profile, a Cisco internal profile based on ITU-T Recommendation H.248.1 Version 2, defines functionality between the DBE and the MGC.

While all mandatory items in the profile are supported automatically by the DBE, it is possible to configure the optional Enhanced Root (eroot) package to interoperate with the MGC/SBE. The eroot package is a proprietary package for the transport of the location ID and media gateway (MG) ID from the signaling border element (SBE).

For more information on the Cisco H.248 profile, see the "Cisco H.248 Profile" section on page 2-12.

## Related Command

The **package** command enables the DBE to use the optional eroot package.

# H.248 Address Reporting Package

The H.248 Address Reporting Package is described in the "H.248 Address Reporting Package" section on page 9-2.

# H.248 Gate Information (Ginfo) Package Becomes Optional

This enhancement removes the stipulation that the Gate Information (Ginfo) package properties are required in the DBE H.248 profile. The DBE continues to support the Ginfo package properties as optional properties and supplies default values if values are not specified.

The Ginfo package properties are the following:

- bill_corr property is defaulted to a value of 24 zero bytes.
- gate_state property is defaulted to COMMITTED. The termination is maintained across system failover and H.248 association loss at all times after the initial termination add. Changes to committed gates are replicated to the redundant card immediately. Therefore omitting this property has a minor performance overhead on redundant systems.
- gate_side property is defaulted to SIDE_A for the first termination in a stream and to SIDE_B for the second termination in a stream.

## Restrictions for DBE H.248 Gate Information Package Becomes Optional

The following is a restriction pertaining to DBE support for the H.248 Gate Information Package Becomes Optional feature:

If one of the Ginfo properties is omitted when adding a termination, you cannot later specify a value for that property value on an Add termination request. An attempt to do fails with error 421 indicating "Unknown action or illegal combination of actions".

# H.248 Protocol—Acknowledgment Support for Three-Way Handshake

The data border element (DBE) supports a three-way handshake for H.248 messages. The DBE supports sending of an acknowledgement (Ack) for a three-way handshake after receiving the transaction response from the media gateway controller (MGC), as described in Annex D.1.2 and Annex D.1.2.2 of H.248.1v3 Gateway Control Protocol: Version 3.

The TransactionResponseAcknowledgement parameter is part of an H.248 message. The acknowledgement is composed of a set of transactions, each of which is made up of a request and a response. The entity receiving the Ack (DBE or MGC) knows that its response has reached the other side. It can delete the response message stored in its memory for handling retransmissions.

The DBE understands and acts upon acknowledgment responses from the MGC.

From the H.248 protocol, the transaction response acknowledgment looks like the following:

```
transactionResponseAck = ResponseAckToken LBRKT transactionAck
*(COMMA transactionAck) RBRKT
transactionAck = TransactionID / (TransactionID "-" TransactionID)
ResponseAckToken = ("TransactionResponseAck" / "K")
```

An example of a response part of the acknowledgment looks like the following:

```
K { 1, 2, 4-6 }
```

# H.248 Segmentation Package Support

When an H.248 association is established over the User Datagram Protocol (UDP), the H.248 message can be too big to fit inside one UDP packet, and as a result, H.248-based segmentation is required. The H.248 Segmentation (seg) package, defined in H.248.1v3 Annex E, defines the following four properties to use when performing this segmentation:

- MGSegmentationTimerValue
- MGCSegmentationTimerValue
- MGMaxPDUSize
- MGCMaxPDUSize

Segmentation package support includes the following functionality:

- If the media gateway controller (MGC) does not receive all the message segments or expected segmented responses, it sends error 459.
- If the MGC receives all the segmented responses, but the DBE does not receive a TransactionResponseAcknowledgement, then the DBE cannot send an error message because this behavior is not defined in the H.248 specification.

## Restrictions for DBE H.248 Segmentation Package Support

The following are restrictions pertaining to DBE support for the Segmentation package:

- The DBE must support H.248 segmentation in addition to this package to negotiate the segmentation properties with MGC.
- The DBE only supports sending of segmented messages; the DBE does not support receiving of segmented messages from the MGC.
- The DBE can send segmented messages only over UDP and can send segmented messages to H.248.1v3 MGCs only. The DBE generates an error message when it receives segmented messages over Transmission Control Protocol (TCP) connections from MGCs. The DBE sends unsegmented messages over TCP or UDP.
- The maximum segment size is subject to the segmentation configuration and the maximum buffer size.

## Related Commands

The **package segment max-pdu-size** command is used to enable the Segmentation package and specify the maximum PDU size that UDP should use for H.248 control signaling. The package is enabled by configuring the maximum PDU size to a value other than 0. A value of 0 disables the package. By default, the Segmentation package is disabled.

The **show sbc dbe controllers** command has been modified to include H.248 Segmentation statistics on the DBE.

# H.248 Session Failure Reaction Package

The Session Failure Reaction (SFR) package enables a media gateway controller (MGC) to instruct a media gateway (MG) to put a specified termination in the OutOfService state (either gracefully or forcefully) at the point where the H.248 association between them is lost. Putting a termination in an OutOfService state is used to prevent signaling messages from reaching the call agent in case of failure or administrative shutdown of MGC and MG communication.

The SFR package includes the following functionality:

- The specifications on signaling pinholes, termination ID structure, and validation of termination name from the Termination State Control (TSC) package also apply to the SFR package.
- The deactivation timer is started when the H.248 association between the MGC and MG is lost. The deactivation timer is cancelled if an association is regained.
- Media timeout is always enabled when the H.248 association is down.
- The values of the SFR/TD, SFR/DB, SFR/AA, and SFR/DT properties are reported to the MGC in Audit responses.

## Restrictions for DBE H.248 Session Failure Reaction Package

The following are restrictions pertaining to DBE support for the SFR package:

- Terminations can be associated by context, but not by VLAN because the VLAN value of the SFR/AA property is not supported. If a request includes the VLAN value, the request is rejected with error 501, "Not Implemented".
- Properties in the SFR package cannot be manipulated by a wildcard Modify command.
- If a termination belongs to multiple streams, the SFR properties must be set consistently in all streams.

**Note** See the MultiService Forum Contribution document, Contribution Number: msf2006.117.03 for more information about the SFR package.

# H.248 Termination State Control Package

The Termination State Control (TSC) package enhances the capabilities of the media gateway controller (MGC) to support the following two features:

- tsc-quiesce

  The MGC can instruct the media gateway (MG) to set the ServiceState property of a signaling pinhole to OutOfService state at the point where all associated (media) terminations are subtracted. The MG informs the MGC when this has occurred. This feature is known as tsc-quiesce.
- tsc-suspend

  The MGC can put a signaling pinhole out of action for a given period of time. The MG informs the MGC when the signaling pinhole becomes operational again, and the MGC can query the time remaining until the suspension ends. This feature is known as tsc-suspend.

  A signaling pinhole is composed of two terminations. If either termination is out of service, the entire pinhole is out of service. It is up to the MGC whether to provision one or both terminations with the relevant properties. If the MGC chooses to provision only one termination, the MG does not impact the other termination.

## The tsc-quiesce Feature

The tsc-quiesce feature includes the following functionality:

- Quiesce is not symmetrical. Adding a media termination does not cause a quiesced OutOfService signaling pinhole to automatically move to InService. The MGC must explicitly set the termination to InService.
- When tsc-quiesce takes effect, the gtd property is left as is, which means that the termination requiesces the next time all associated terminations are subtracted.
- Wildcard Subtracts on media terminations in multiple contexts result in multiple Deactivation Completed events to the MGC.
- The tsc/gtd and tsc/ata properties and the tsc/dc event (if subscribed for) are reported to the MGC in Audit responses.

# The tsc-suspend Feature

The tsc-suspend feature includes the following functionality:

- Termination association (by context or VLAN) is not relevant to tsc-suspend.
- The trt property may be set to ON only when changing a termination to OutOfService. Modification of trt can cause the following error cases:
  - trt set to ON and ServiceState set to InService.
  - trt set to ON and ServiceState is not supplied (in which case it defaults to InService).

  In each case, the transaction is failed with error 421, “Unknown action or illegal combination of actions”. This policing occurs before any other processing or checking.
- The MG ignores cases where the termination is already OutOfService when trt is set to ON.
- If the recovery timer is running and LocalControl is modified:
  - If trt is ON and the recovery timer (rt) is non-zero, the recovery timer will be cancelled and restarted with the new rt value.
  - If trt is OFF or rt is zero, the timer is stopped.
- If the MGC manually changes a suspended termination from OutOfService to InService, the recovery timer is stopped. However, if the MGC re-applies OutOfService state to an already suspended termination, this has no effect on the recovery timer and does not cancel recovery.
- The tsc/trt and tsc/rt properties and the tsc/rc event (if subscribed for) are reported to the MGC in Audit responses.

# Restrictions for DBE tsc-suspend Feature

The following is a restriction pertaining to DBE support for the tsc package:

Terminations can be associated by context, but not by VLAN. This means that the VLAN value of the tsc/ata property is not supported. If a request includes the VLAN value, the request is rejected with error 501, “Not Implemented”.

**Note** See the MultiService Forum Contribution document, Contribution Number: msf2006.117.03 for more information about the tsc package.

# Related Command

The tsc/ttr statistic is reported in the **show sbc dbe media-flow-stats** and **show sbc dbe signaling-flow-stats** command outputs. The tsc/trt property is reported as ON if the termination is OutOfService with the recovery timer running, and OFF otherwise.

# H.248 Traffic Management Package Support

The DBE supports the sustained data rate (tman/sdr), maximum burst size (tman/mbs), and policing (tman/pol) properties of the ETSI TS 102 333 Traffic Management (Tman) package.[1] Support of these tman properties allows additional pinhole programming in the Tman package to inform the DBE how to police media and signaling flows. These tman properties can be assigned to both media and signaling flows. The DBE performs asymmetric flow policing.

The Traffic Management package is described in the "H.248 Traffic Management Package Support" section on page 5-2.

# H.248.1v3 Support

H.248.1v3 Support allows the DBE to interoperate with an SBE, which requires H.248.1v3 or Media Gateway Controller (MGC) version 3. The DBE can only accept version 3 once it is configured to support version 3.

On contacting an SBE, the DBE advertises for H.248.1 version 3 and confirms the version received in the response from the SBE. If the SBE supports a lower version than was advertised, the DBE logs the event, disconnects from the SBE, and tries an alternative SBE until an SBE with H.248.1v3 is found. A new field, bcaGalEntMegacoVersion, is added to the MG-Abstraction Layer entity MIB.

## Restrictions for DBE H.248.1v3 Support

The following is a restriction pertaining to H.248.1v3 Support:

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

## Related Command

The **h248-version** command defines the version of the H.248 protocol which the DBE uses when forming associations with an H.248 controller.

# Syntax-Level Support for H.248 VLAN Package

The DBE provides syntax-level support for the H.248 VLAN package. The media gateway controller (MGC) can program up to two VLAN tags and associated Ethernet priorities, as defined in the H.248 VLAN package. The DBE can accept, store, and return VLAN tag and priority information, at the syntax level, for media streams.

## Restrictions for DBE Syntax-Level Support for H.248 VLAN Package

The following is a restriction pertaining to DBE support for the H.248 VLAN package:

The DBE does not use the VLAN tag and priority information.

[1] ETSI TS 102 333 version 1.1.2 Traffic Management Package

## Related Command

The VLAN tag and priority information is returned in the **show sbc dbe media-flow-stats** and **show sbc dbe signaling-flow-stats** command outputs.

# MGC-Controlled Gateway-Wide Properties

This feature adds support for all of the properties in Version 2 of the H.248 Base Root package as defined in H.248.1v3.

The following properties of the Base Root Version 2 package can be modified and audited by the media gateway controller (MGC):

- normalMGExecutionTime
- normalMGCExecutionTime
- MGProvisionalResponseTimerValue
- MGCProvisionalResponseTimerValue
- MGOriginatedPendingLimit
- MGCOriginatedPendingLimit

In addition, the following read-only properties can be audited:

- maxNrOfContexts
- maxTerminationsPerContext

## Restrictions for DBE MGC-Controlled Gateway-Wide Properties

The following is a restriction pertaining to DBE support for this feature:

The property field values are stored where set by H.248 and returned on subsequent audits. However, the property values are not used by the DBE and do not affect the behavior of the DBE.

CHAPTER 8

# ETSI Ia Profile on SBC

The Ia profile is a part of the H.248 functionality that is required for communication on the data border element (DBE). The Ia profile is an H.248 profile for the reference point between the Service Policy Decision Function (SPDF) and the DBE, using the Border Gateway Function (BGF).

The ETSI Ia Profile (ETSI ES 283 018 V2.4.1 (2008-09)) makes the Bandwidth Description (b= line) of Session Description Protocol (SDP) mandatory. However, as per SDP RFC 2327 and SDP RFC 4566, Bandwidth Description is optional. To improve interoperability, the ETSI Ia Profile on SBC feature permits SBC to accept SDP without a Bandwidth Description, even when using the Ia Profile.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller, and may be commonly referred to as the session border controller (SBC) in this document.

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

## Contents

This chapter provides information about the following topics:

# Information About ETSI Ia Profile on SBC

During registration, the DBE includes the ServiceChangeProfile parameter in the ServiceChange message to indicate support for Ia profile.

To improve interoperability, the SBC is configured to permit the Bandwidth Description parameter to be optional when using the ETSI Ia profile.

The SDP that is presented, permits bandwidth requirements to be determined through a full parse of the SDP. Although Bandwidth Description is configured as optional, it is not ignored. When present, the Bandwidth Description continues to take precedence over any other bandwidth information inferred from the SDP.

Any SDP that does not provide a Bandwidth Description provides sufficient codec information to permit bandwidth requirements to be determined. Omitted codec type information is not permitted and is rejected with the H.248 ErrorCode 421, as “Unknown action or illegal combination of actions”.

The following SDP information is acceptable since it uses static codec, and bandwidth requirements can also be determined:

```
v=0
c=IN4 192.168.0.1
m=audio $ RTP/AVP 4 8 18
a=ptime:30
```

By default, the Traffic Management (TMAN) or maximum burst size (MBS) parameter is optional. This ensures that the SBC does not reject the call if TMAN or MBS parameter is missing from the H.248 message.

## Differences Between ETSI Ia Profile Version 1 (ES 283 018 V1.1.4) and Ia Profile Version 2 (ES 283 018 V2.7.1)

Table 8-1 provides an overview of the differences between ETSI Ia Profile Version 1 (ES 283 018 V1.1.4) and Ia Profile Version 2 (ES 283 018 V2.7.1).

*Table 8-1 Differences Between ETSI Ia Profile Version 1 (ES 283 018 V1.1.4) and Ia Profile Version 2 (ES 283 018 V2.7.1*

| Topic | ES 283 018 [19] V1.1.4 (Ia Profile Version 1) | ES 283 018 V2.7.1 (Ia Profile Version 2) |
|---|---|---|
| QoS monitoring | Not Supported | Basic support via H.248 statistics (see clause 5.17.1.6) |
| TerminationID structure | ip/<group>/<interface>/<id> | ip/<group>/<interface>/<id> Field element "interface" is off-loaded from the semantic of "IP realm/domain" indication. |
| SDP Usage: "s=", "t=" and "o=" lines | Provides no guidance on this | Guidance provided in clause 5.16. |
| SDP Usage "b=" line | The bandwidth-value value defines the required protocol layer 2 (e.g. Ethernet) bandwidth for the specific H.248 Stream. | The bandwidth-value value defines the IP layer bandwidth for the specific H.248 Stream. |
| Semantic for ignoring SDP information. | Usage of "ignore" | Replacement of "ignore" by text describing the handling of received SDP at the BGF for both media aware and media agnostic cases. |
| **Packages** | | |

*Table 8-1 Differences Between ETSI Ia Profile Version 1 (ES 283 018 V1.1.4) and Ia Profile Version 2 (ES 283 018 V2.7.1*

| Topic | ES 283 018 [19] V1.1.4 (Ia Profile Version 1) | ES 283 018 V2.7.1 (Ia Profile Version 2) |
|---|---|---|
| RTP Package | Not Supported | Optional Version 1 |
| IP Domain Connection Package | Not Supported | Version 1 |
| Media Gateway Overload Control Package | Not Supported | Optional Version 1 |
| Application Data Inactivity Package | Not Supported | Optional Version 1 |
| Hanging Termination Package | Not Supported | Optional Version 1 |
| Statistics Conditional Reporting | Not Supported | Optional Version 1 |
| **Procedures** | | |
| Session Independent Procedures (also known as Call Independent Procedures or Non-Call Related Procedures) | Implicit[1] link to TR 183 025 [i.2]. | Explicit link to TR 183 025 [i.2] by clause 5.17.2. Additional details in clause 5.19. |
| | Call-independent procedures for ES 283 018 [19] are defined in a separate document (TR 183 025 [i.2]), which is an overall description for all ETSI defined H.248 profile specifications, i.e. TR 183 025 [i.2] complements each profile specification. The set of profile-applicable call-independent procedures is primarily given by the supported H.248 Command API capabilities for AuditValue (see clause 5.8.5), AuditCapabilities (see clause 5.8.6) and ServiceChange (see clause 5.8.8), and supported packages (for example, for overload control), by each profile. | |
| IP Domain/Realm Indication | Via semantical overloading of the TerminationID [2] | Explicit protocol element: via ipdc/realm property (ITU-T Recommendation H.248.41 [15]; see clause 5.17.1.10). |
| BGF Resource Reservation | One-stage mechanism | Additional support of a two-stage resource reservation (see clause 5.17.1.11) |
| RTCP Handling | High-level description in clause 5.17.1.1. | Additional information by clause 5.17.1.7. |

[1] The TR was work in progress when Ia profile version 1 was published.

[2] ITU-T Recommendation H.248.41 [15] was work in progress when Ia profile version 1 was published.

## Gate Controller Profile

The Gate Controller (GC) is a logical entity that controls gates and associated resources in a Multimedia Border Gateway (MBG). By default, the GC profile is enabled on the SBC, and the Bandwidth Description parameter is optional. Table 8-2 lists the packages supported by GC profiles. The supported GC profile versions are 1, 2, and 3.

*Table 8-2 Packages Supported by the GC Profile*

| Package Name | ID | Version |
|---|---|---|
| Network | nt | 1 |
| DTMF Detection | dd | 1 |
| DTMF Generation | dg | 1 |

*Table 8-2 Packages Supported by the GC Profile (continued)*

| | | |
|---|---|---|
| RTP | rtp | 1 |
| Congestion Handling | chp | 1 |
| Inactivity Timer | it | 1 |
| NAT Traversal | ntr | 1 |
| Middlebox | emp | 1 |
| Diffserv | ds | 1 |
| Extended VPN Discrimination | evpnd | 1 |
| Gate Information | ginfo | 1 |
| Enhanced base root package | eroot | 2 |
| Gate recovery information | gri | 1 |
| Traffic Management | tman | 1 |
| Enhanced Traffic Management | etman | 1 |
| End-point Statistics | epstat | 1 |
| Media gateway overload control | ocp | 1 |
| IP NAPT Traversal Package | ipnapt | 1 |
| Address Reportýng Package | adr | 1 |
| Gate Management | gm | 1 |
| Base root | root | 2 |
| VLAN | vlan | 1 |
| MGC Information Package | mgcinfo | 1 |
| Segmentation | seg | 1 |
| Application Inactivity Detection | adid | 1 |
| IP Domain Connectivity | ipdc | 1 |
| IP Realm Availability | ipra | 1 |

## Restrictions for ETSI Ia Profile on SBC

The ETSI Ia Profile on SBC feature has the following restrictions:

- TMAN package function is not implemented on the dataplane module.
- Remote port filter is not supported.

## Memory and Performance Impact

In the absence of a Bandwidth Description, the SBC has to perform an extensive parse of the SDP to calculate bandwidth requirements. This results in a slight degradation of performance that is relative to an Ia Profile compliant call. However, the degradation is less than 1%.

# Configuring ETSI Ia Profile on SBC

This section contains steps to configure the ETSI Ia Profile on SBC feature on the Cisco ASR 1000 Series Routers.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sbc** {*sbc-name*} **dbe**
4. **vdbe** [**global**]
5. **no bandwidth-fields**
6. **h248-profile etsi-bgf** *version*
7. **exit**
8. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **`enable`**<br>**Example:**<br>`Router>` **`enable`** | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **`configure terminal`**<br>**Example:**<br>`Router#` **`configure terminal`** | Enters global configuration mode. |
| **Step 3** | **`sbc`** `{`*`sbc-name`*`}` **`dbe`**<br>**Example:**<br>`Router(config)#` **`sbc global dbe`** | Creates the DBE service on the SBC, and enters into SBC-DBE configuration mode. |
| **Step 4** | **`vdbe`** `[`**`global`**`]`<br>**Example:**<br>`Router(config-sbc-dbe)#` **`vdbe global`** | Enters into Virtual Data Border Element (VDBE) configuration mode with a default DBE named “global”.<br>Only one DBE is supported, and its name must be “global”. |
| **Step 5** | **`bandwidth-fields mandatory`**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# no bandwidth-fields` | Sets the Bandwidth Description of the SDP as mandatory. The **no** form of the **bandwidth-fields mandatory** command sets the bandwidth as optional.<br>**Note** By default, the Bandwidth Description is set as optional. |
| **Step 6** | **`h248-profile etsi-bgf`** *`version`*<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)#` **`h248-profile etsi-bgf version 2`** | Configures the VDBE H.248 profile name to interoperate with the DBE.<br>Version 2 is the default version number for the Ia ETSI BGF profile.<br>When the H.248 profile is configured with the **h248-profile etsi-bgf version 2** command, the ServiceChange message that the DBE sends to SBE (MGC) during startup is as follows:<br>`T=1{`<br>`C=-{`<br>`SC=ROOT{`<br>`SV{MT=RS,DL=0,RE="901 Cold Boot",V=3,PF=ETSI_BGF/02,20091229T01364500}}}}` |
| **Step 7** | **`exit`**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)#` **`exit`** | Exits VDBE configuration mode. |
| **Step 8** | **`end`**<br>**Example:**<br>`Router(config-sbc-dbe)#` **`end`** | Exits SBC-DBE configuration mode and returns to privileged EXEC mode. |

# Configuration Example of ETSI Ia Profile on SBC

The following example shows how to configure the ETSI Ia Profile on SBC feature on a Cisco ASR 1000 series router:

```
config terminal
 sbc mySBC dbe
  vdbe global
   no bandwidth-fields
   h248-profile etsi-bgf version 2
```

CHAPTER 9

# Security in Cisco Unified Border Element (SP Edition) Distributed Model

The Cisco Unified Border Element (SP Edition) distributed model for the Cisco ASR 1000 Series Routers offers high security functions. Enterprise users want to protect their network and service providers want to protect their core or backbone network. Because service providers allow direct users to come into their network to access different services, it is critical to have high security. Customers also want to police the data coming into their networks and require notification if any unwanted user tries to access the network. The data border element (DBE) implementation supports various security features and policing of incoming data.

For example, the DBE supports the ETSI TS 102 333 Gate Management (GM) package to control addressing for the local as well as the remote party. The DBE uses the source address mask and remote source address filtering to specify a range of addresses rather than a specific address and port for the source or remote address of the arriving packet. Data coming from other defined addresses are dropped and reported to the Signaling Border Element (SBE) for security reasons. Local Source Properties (Address and Port) and Remote Source Address Mask Filtering, described in this chapter, are supported features of the GM package.

This chapter describes or cross-references supported security features.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

## Contents

This chapter provides information about the following topics:

- NAPT and NAT Traversal, page 9-11
- Remote Source Address Mask Filtering, page 9-12
- Topology Hiding, page 9-12
- Traffic Management Policing, page 9-13
- Two-Rate Three-Color Policing and Marking, page 9-13

# Firewall (Media Pinhole Control)

The SBE Call Admission Control (CAC) function inspects the signaling message and instructs the firewall in the DBE to open and close pinholes as needed for the media streams and signaling.

# H.248 Address Reporting Package

The data border element (DBE) supports the H.248 Address Reporting (ADR) package, defined in "Draft New H.248.37 Amendment 1", ITU-T document TD-27. The adr package extends the existing IP NAPT Traversal (IPNAPT) package, and adds a new Remote Source Address Change (RSAC) event with two parameters: New Remote Source Address (NRSA), and New Remote Source Port (NRSP).

The rsac event is generated by the media gateway (MG) when the remote source address for the termination changes (that is, when a stream latches), and is used to report the newly detected remote source address and port to which the stream has been latched.

The event is generated in both the LATCH and RELATCH scenarios. The DBE reports the event subscription with the audit response when the media gateway controller (MGC) audits the packages.

For further information on support for the H.248 IP NAPT Traversal package, see the "IP NAPT Traversal Package and Latch and Relatch Support" section on page 9-9.

## Restrictions for DBE H.248 Address Reporting Package

The following are restrictions pertaining to ADR package support:

- The MGC must explicitly subscribe for the rsac event.
- The adr package can be used only in conjunction with the IP NAPT Traversal package.

# H.248 Session Failure Reaction Package

The data border element (DBE) supports the H.248 Session Failure Reaction (SFR) package. From a security point of view, the media gateway controller (MGC) can put a termination out of service when the H.248 connection between the MGC and media gateway (MG) is lost.

For more information on the SFR package, see the "H.248 Session Failure Reaction Package" section on page 7-4.

# H.248 Termination State Control Package

The data border element (DBE) supports the Termination State Control (TSC) package to monitor signaling pinholes.

The "tsc-quiesce" feature of the TSC package helps the media gateway controller (MGC) monitor a signaling pinhole and put the pinhole in "not-in-service" mode when all terminations are subtracted.

For more information on the TSC package, see the "H.248 Termination State Control Package" section on page 7-5.

# Full Support for Interim Authentication Header

The Cisco Unified Border Element (SP Edition) distributed model offers full support to the Interim Authentication Header (IAH) that conforms to section 10.2, Interim AH Scheme, of the H.248.1v3 Gateway Control Protocol: Version 3. An IAH is part of every H.248 message generated by the data border element (DBE) to the media gateway controller (MGC). Information in the IAH is used to authenticate and check the integrity of packets, thus ensuring packet security.

The DBE generates an IAH for outgoing H.248 messages sent to the MGC. The DBE calculates and then populates an IAH which is sent with the H.248 message. For all incoming H.248 messages received from the MGC, the DBE validates that the IAH received matches its calculation. The IAH scheme inserts the IAH within the H.248.1 protocol header. Note that for IPsec, the IAH is inserted immediately after the IP header for IPsec.

Figure 9-1 shows the IAH format consisting of the Security Parameters Index (SPI), Sequence Number, and Integrity Check Value (ICV):

- Security Parameters Index (SPI)—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.
- Sequence Number—A monotonically increasing number, used to prevent replay attacks.
- Integrity Check Value (ICV)—A variable-length field that contains the Integrity Check Value for the packet. The MGC computes the ICV over the appropriate fields of the packet, using the specified integrity algorithm, and verifies that it is the same as the ICV included in the ICV field of the packet. If the computed and received ICVs match, then the packet is valid.

***Figure 9-1 Interim Authentication Header Format***

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                Security Parameters Index (SPI)                |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                   Sequence Number Field                       |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 +               Integrity Check Value-ICV (variable)            |
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

To enable full support of IAH, you must configure the following:

- IAH hashing scheme – Configure one of the following:
  - HMAC-MD5: Hashing for Message Authentication-Message Digest 5 that produces a 128-bit hash value.
  - HMAC-SHA: Hashing for Message Authentication-Secure Hash Algorithm that produces a message digest that is 160 bits long.

  MD5 hashing is faster to calculate, but provides less secure authentication than SHA hashing. 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.
- Inbound (local) Security Parameter Index (SPI)
- Outbound (remote) SPI
- Hex-key argument, which 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.

**Note** IPv6 packets that support IPsec do not use the Interim Authentication Header scheme.

## Restrictions for DBE Interim Authentication Header Full Support

In some circumstances, the DBE uses zero authentication where the IAH is inserted in the packet and all fields in the IAH are set to zeroes. The DBE checks the packet syntactically, however, the DBE does not authenticate whether there is an IAH or if it is correct.

The following are restrictions pertaining to the IAH full support, where the DBE reverts back to zero authentication:

- If you enable authentication of call packets by specifying the **interim-auth-header** keyword in the **transport** command, but you do not specify either **ah-md5-hmac** or **ah-sha-hmac**, the authentication reverts back to zero authentication.
- For the MD5 or SHA hashing scheme to work, both the inbound and outbound SPI must be configured. If you configure only the inbound or outbound SPI key or neither inbound or outbound SPI key, 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”.

## Related Commands

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** keywords) using the **transport (session border controller)** command, you must configure incoming and outgoing call packets using both the **inbound** and **outbound** commands.

- **transport** command—**interim-auth-header** keyword was added to insert the IAH into H.248 messages. The **ah-md5-hmac** and **ah-sha-hmac** keywords are added to specify the type of hashing scheme for authentication.
- **inbound** and **outbound** commands—Configures inbound and outbound packets with the *spi* and *hex-key* arguments to use a specific Security Parameters Index (SPI) and hex key.

For more information on the **transport (session border controller)**, **inbound**, and **outbound** commands, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

# Configuring IAH Full Support

This section contains steps to configure the IAH full support functionality in a typical configuration scenario on the Cisco ASR 1000 Series Routers.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface sbc** {*interface-number*}
4. **ip address** *ip-address*
5. **exit**
6. **sbc** {*sbc-name*} **dbe**
7. **vdbe** [**global**]
8. **h248-version** *version*
9. **h248-napt-package** [**napt** | **ntr**]
10. **local-port** {*port-num*}
11. **control-address h248 ipv4** {*A.B.C.D*}
12. **controller h248** {*controller-index*}
13. **remote-address ipv4** {*A.B.C.D*}
14. **remote-port** {*port-num*}
15. **transport** {**udp** | **tcp**} [**interim-auth-header**] [**ah-md5-hmac** | **ah-sha-hmac**]
16. **inbound** {*spi*} {*hex-key*}
17. **outbound** {*spi*} {*hex-key*}
18. **exit**
19. **exit**
20. **attach-controllers**
21. **exit**
22. **location-id** {*location-id*}
23. **media-address ipv4** {*A.B.C.D*}
24. **activate**
25. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | `enable`<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | `configure terminal`<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | `interface sbc {interface-number}`<br>**Example:**<br>`Router(config)# interface sbc 1` | Creates an SBC virtual interface and enters into interface configuration mode. |
| **Step 4** | `ip address ip-address`<br>**Example:**<br>`Router(config-if)# ip address 1.1.1.1 255.0.0.0` | Configures an IP address on the SBC virtual interface. |
| **Step 5** | `exit`<br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode. |
| **Step 6** | `sbc {sbc-name} dbe`<br>**Example:**<br>`Router(config)# sbc global dbe` | Creates the DBE service on the SBC and enters into SBC-DBE configuration mode. |
| **Step 7** | `vdbe [global]`<br>**Example:**<br>`Router(config-sbc-dbe)# vdbe global` | Enters into VDBE configuration mode with a default DBE named “global”.<br>Only one DBE is supported and its name must be “global”. |
| **Step 8** | `h248-version version`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# h248-version 3` | Specifies that the DBE uses an H.248 version when it forms associations with an H.248 controller.<br>Version 2 is the default. |
| **Step 9** | `h248-napt-package [napt \| ntr]`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# h248-napt-package napt` | Defines whether the DBE uses the Network Address and Port Translation (NAPT) or NAT Traversal (NTR) H.248 package for signaling NAT features. NTR is the default.<br>The example shows how to configure the DBE to use NAPT. |
| **Step 10** | `local-port {port-num}`<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# local-port 2971` | Configures the DBE to use the specific local port number when connecting to the default media gateway controller (MGC). |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **control-address h248 ipv4** {*A.B.C.D*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe)# **control-address h248 ipv4 200.50.1.41** | Configures the DBE to use a specific IPv4 H.248 control address, which is the local IP address the DBE uses as its own address when connecting to the SBE. |
| **Step 12** | **controller h248** {*controller-index*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe)# **controller h248 2** | Configures the H.248 controller for the DBE and enters into Controller H.248 configuration mode.<br>In the example, the configured number 2 identifies the H.248 controller for the DBE. |
| **Step 13** | **remote-address ipv4** {*A.B.C.D*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248)# **remote-address ipv4 200.50.1.254** | Configures the IPv4 remote address of the H.248 controller for the SBE.<br>In the example, 200.50.1.254 is configured as the remote SBE IP address. |
| **Step 14** | **remote-port** {*port-num*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248)# **remote-port 2971** | Configures the port number of the H.248 controller that is used to connect to the SBE. |
| **Step 15** | **transport** {**udp** \| **tcp**} [**interim-auth-header**] [**ah-md5-hmac** \| **ah-sha-hmac**]<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248)# **transport udp interim-auth-header ah-sha-hmac** | Configures the DBE to use either UDP or TCP for H.248 control signaling, and configures the Interim Authentication Header (IAH) to authenticate and check the integrity of call packets by specifying either the MD5 or SHA hashing scheme. Enters into IAH Key configuration mode.<br>**ah-md5-hmac**—Hashing for Message Authentication-Message Digest 5, produces a 128-bit hash value.<br>**ah-sha-hmac**—Hashing for Message Authentication-Secure Hash Algorithm, produces a message digest that is 160-bits long. |
| **Step 16** | **inbound** {*spi*} {*hex-key*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248-iah)# **inbound 300 abcdef01234456** | Configures inbound call packets to use a specific Security Parameters Index (SPI) and hex key.<br>spi (Security Parameters Index)—An arbitrary 32-bit value that the MGC uses to identify the Security Association to which an incoming packet is bound, that is, which hashing key to use. Accepts a range of 256 through 2147483647.<br>hex-key—Maximum of 64 characters. It can be a text string, such as myOutboundKey89, or be in hexadecimal format, such as 012345678abcde. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 17** | **outbound** {*spi*} {*hex-key*}<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248-iah)# **outbound 400 012345678abcde** | Configures outbound call packets to use a specific Security Parameters Index (SPI) and hex key.<br>spi (Security Parameters Index)—An arbitrary 32-bit value that the MGC uses to identify the Security Association to which an outgoing packet is bound, that is, which hashing key to use. Accepts a range of 256 through 2147483647.<br>hex-key—Maximum of 64 characters. It can be a text string, such as myOutboundKey89, or be in hexadecimal format, such as 012345678abcde. |
| **Step 18** | **exit**<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248-iah)# **exit** | Exits IAH Key configuration mode and enters Controller H.248 configuration mode. |
| **Step 19** | **exit**<br>**Example:**<br>Router(config-sbc-dbe-vdbe-h248)# **exit** | Exits Controller H.248 configuration mode and enters VDBE configuration mode. |
| **Step 20** | **attach-controllers**<br>**Example:**<br>Router(config-sbc-dbe-vdbe)# **attach-controllers** | Attaches the DBE to an H.248 controller. |
| **Step 21** | **exit**<br>**Example:**<br>Router(config-sbc-dbe-vdbe)# **exit** | Exits VDBE configuration mode. |
| **Step 22** | **location-id** {*location-id*}<br>**Example:**<br>Router(config-sbc-dbe)# **location-id 1** | Configures a location ID for the DBE.<br>The location ID is used by the network to route calls. |
| **Step 23** | **media-address ipv4** {*A.B.C.D*}<br>**Example:**<br>Router(config-sbc-dbe)# **media-address ipv4 1.1.1.1 255.0.0.0** | Adds the IPv4 address to the set of addresses, which can be used by the DBE as a local media address. This address is the SBC virtual interface address.<br>Configure this command for each IP address that you specified under the SBC virtual interface in Step 4. |
| **Step 24** | **activate**<br>**Example:**<br>Router(config-sbc-dbe)# **activate** | Initiates the DBE service of the SBC. |
| **Step 25** | **end**<br>**Example:**<br>Router(config-sbc-dbe)# **end** | Exits SBC-DBE configuration mode and returns to privileged EXEC mode. |

## IAH Full Support Examples

The following configuration example shows how to configure the IAH to use the HMAC-SHA hashing scheme, set the inbound SPI to 300 and outbound SPI to 400, and the inbound and outbound hash keys to abcdef01234456 and 012345678abcde, respectively:

```
sbc global dbe
 vdbe global
  h248-version 3
  h248-napt-package napt
  local-port 2970
  control-address h248 ipv4 200.50.1.40
  controller h248 2
   remote-address ipv4 200.50.1.254
   remote-port 2970
   transport tcp interim-auth-header ah-sha-hmac
     inbound 300 abcdef01234456
     outbound 400 012345678abcde
 attach-controllers
```

The following example shows an H.248 message with the IAH:

```
AU=0x00000190:0x00000002:0x6E60A7DC58ECD631A5E13DCFC6E94DEB
!/3 [200.60.255.200]:2944
P=6{
C=1{
A=xyzcompany/sip/gn/0/1/0/1/ac/1,
A=xyzcompany/sip/gn/0/2/0/1/bb/2}}
```

## Debugging Tips

The debugging tips for IAH Full Support are as follows:

- If the MGC is rejecting the H.248 messages from the DBE, or the DBE is rejecting H.248 messages from the MGC, compare the IAH configuration on the DBE with that on the MGC. The inbound SPI key on the DBE should match the outbound SPI key on the MGC, and vice-versa.
- If the IAH header on H.248 messages from the DBE looks like all zeros, then it is likely that the IAH configuration is incomplete, for example, only the inbound or the outbound IAH configuration is specified. See also the "Restrictions for DBE Interim Authentication Header Full Support" section on page 9-4.

# IP NAPT Traversal Package and Latch and Relatch Support

The data border element (DBE) supports the IP NAPT Traversal (IP NAPT) package that is defined in H.248.37. IP NAPT traversal is an alternative method to the existing support of the NAT Traversal (NTR) package, defined in ETSI TS 102 333. IP Network Address and Port Translation (IP NAPT) defines two signals, Latch and Relatch, to control how the DBE learns remote addresses for endpoints behind a Network Address Translation (NAT).

The NAPT package is defined through a new field, napt_variant, in the bcaGalEntTable MIB table. If this field is set to "H.248.37," then NAPT support can be requested by the media gateway controller (MGC) using the H.248.37 IP NAPT Traversal package. In other words, the MGC can request that the DBE wait for the first inbound media packet and "latch" onto it. The DBE learns the remote address and port for the flow from that packet. The MGC can request latching or relatching using the H.248 signal.

# Latch and Relatch Support

The DBE supports Latch and full Relatch support. The Latch and Relatch signals control how the DBE learns remote addresses. Latch and Relatch are commands from the media gateway controller (MGC). Latch is an event that occurs on a flow when certain packets arrive and are matched to that flow. This event changes the admission criteria for a flow.

The ITU-T H.248.37 standard describes the ipnapt/latch signal with the napt parameter. The napt parameter has the values OFF, LATCH, and RELATCH.

When the LATCH value is set, the DBE ignores the addresses received in the RemoteDescriptor. Instead, the DBE uses the source address and source port from the incoming media streams to be the destination address and destination port of the outgoing streams.

The RELATCH value is similar to the LATCH value except that when the DBE detects a change of source IP address and port on the incoming media stream, then the new source IP address and port are used as the destination address and port for outgoing packets. After relatching, any packets received with the old source address and port are discarded.

When latching, the DBE uses the remote address and port of a source endpoint as the destination endpoint address and port if the source IP address is within a specified Gate Management/remote source address mask (gm/rsam). This means that within a subnet any packet can be latched within a gm/rsam. The Relatch event waits until a packet arrives that fails the latched admission criteria, but which meets the relatch criteria. The relatch may require stricter admission criteria than the original latching, such as packets may have to come from a specific remote address rather than from within the subnet. Or the relatch criteria might identify a different subnet. In relatching, one reason for the change in the source IP address and port could be a subscriber requiring a different service.

When the ntr package is in use, the DBE continues to attempt to relearn remote addresses and ports following any H.248 operation that modifies a termination whose endpoint is behind a NAT. Relearning continues to be timed out if no packets from a new remote source address and port are received within a suitable period.

When the ipnapt package is in use, the DBE does not attempt to relearn remote addresses and ports unless a Relatch is explicitly signaled by the MGC. Relatching is not timed out.

# Restrictions for DBE Latch and Relatch Support

The following are restrictions pertaining to DBE support for the IP NAPT Traversal (ipnapt) package and Latch and Relatch:

- The DBE only supports either the NTR package or the IP NAPT Traversal package for a termination. You can configure either package with the **h248-napt-package** command.
- The DBE does not generate the notifyComplete signal when the Latch or Relatch signal completes.
- With the IP NAPT Traversal package, the DBE does not automatically relatch on receipt of an H.248/Megaco request that modifies the gm/sam. If a Relatch is required, it must be explicitly signaled by the MGC. In addition, you cannot update the remote source address mask so that it no longer contains the previously latched remote address without signaling a Relatch.

# Related Command

The **h248-napt-package** command defines which H.248 package (either ipnapt or ntr) the DBE uses for signaling NAT features.

# Local Source Properties (Address and Port)

The data border element (DBE) is enhanced to support multiple terminations that share a single local address and port. The Gate Management/remote source address mask (gm/rsam) defines a remote subnet. The mask length is a property of the local address and port combination. Only multiple terminations that share the same local address and port are required to have the same gm/rsam length. Terminations with different local addresses or ports can have different gm/rsam lengths.

A gm/rsam having the same mask length allows multiple terminations to share a single local address and port combination, with the requirement that the terminations are configured with gm/rsams that are distinct. This enables the media gateway controller (MGC) to identify and match the terminations to the correct flow. For more information about Local Source Address and Local Source Port properties, see the ETSI TS 102 333 V1.1.2 Gate Management Package.

**Note** A termination can be described as a point of entry or exit of media flows relative to the DBE.

Terminations may share a single local address and port under one or the other of the following conditions:

- Terminations have an MGC-managed local address, in which case they must be specified with a proper gm/sam.
- Terminations are specified with a gm/sam and the address is “non-local”; that is, the pinhole is No NAPT or the termination is the one that is the unwritten flow of a Single NAPT pinhole.

This enhancement supports the following functionality:

- Call signaling can be routed to the MGC through the DBE.
- Call signaling from different subscribers can be routed through different pinholes on the DBE.

  These different pinholes can share the same IP address and port on the subscriber side on the DBE. This is a typical scenario on the User-Network Interface, where it is simpler to publish a single IP and port to many subscribers.

## Restrictions for DBE Local Source Properties (Address and Port)

The following is a restriction pertaining to DBE support for this feature:

Only three different lengths of network masks can be in use at the same time on a given local address and port combination. Otherwise, the DBE issues error 510 “Insufficient Resources”.

# NAPT and NAT Traversal

The data border element (DBE) performs translation of IP addresses and port numbers via Network Address and Port Translation (NAPT) and Network Address Translation (NAT) Traversal functions in both directions.

NAT converts an IP address from a private address to a public address in real time. It allows multiple users to share a single public IP address. The DBE can learn the NAT’s public address and latch onto it for that flow.

# Remote Source Address Mask Filtering

This feature adds support for the Remote Source Address Filtering (saf) and Remote Source Address Mask (rsam) properties of the ETSI TS 102 333 Gate Management (GM) package.[1]

The media gateway controller (MGC) can specify the gm/saf and gm/rsam properties of terminations in Add and Modify requests. Cisco Unified Border Element (SP Edition) reports them in Audit responses.

This feature allows the MGC to program multiple terminations with the same local address and port, VPN ID, and transport protocol, as long as the multiple terminations are distinguished by their remote source address mask, and the local address is taken from an MGC-managed address range.

This feature supports a single local address for each phone where each phone transmits media using a single pinhole. This means several signaling flows or pinholes can have the same address and port.

Packets arriving at the SBC are classified into flows using the following data: VPN ID, destination address, destination port, protocol type, and source address. The source address is only required to match a remote source address mask rather than a specific remote address.

## Restrictions for DBE Remote Source Address Mask Filtering

The following are restrictions pertaining to data border element (DBE) support for this feature:

- If the remote source address mask is specified for a termination, then it must contain the address in the remote descriptor, unless NAT latching techniques are used. However if you want more than one flow on the same local address or port, then the local address must be MGC-managed.
- A prefix length of 0 for the remote source address mask is invalid.
- The MGC is only allowed to specify local addresses and ports that lie within configured address and port ranges.

## Related Commands

The related commands for Remote Source Address Mask Filtering feature include:

- The **media-address ipv4** command has **dbe** and **mgc** options that indicate whether an address pool is provided from which the DBE or MGC can allocate addresses.
- The new **media-address pool ipv4** command creates a pool of sequential IPv4 media addresses that can be used by the DBE as local media addresses; the command also has **dbe** and **mgc** options.

# Topology Hiding

Topology hiding is an important function of security because it protects the identity of the users and their network addresses. See Chapter 13, "Topology Hiding" for more information.

[1] ETSI TS 102 333 version 1.1.2 Gate Management Package

# Traffic Management Policing

The data border element (DBE) supports the H.248 Traffic Management (Tman) package to police signaling and media streams. The DBE can also monitor packets coming from the access (customer) side and from the backbone (network core) side.

For more information on the Tman package, see the "H.248 Traffic Management Package Support" section on page 7-7.

# Two-Rate Three-Color Policing and Marking

The data border element (DBE) supports Two-Rate Three-Color Policing and Marking to control the traffic coming from the user.

For more information on the Two-Rate Three-Color Policing and Marking feature, see the "Two-Rate Three-Color Policing and Marking" section on page 5-7.

CHAPTER 10

# Cisco Unified Border Element (SP Edition)—SPA DSP Services

The shared port adapter (SPA) digital signal processor (DSP) is a single-width, half-height, high-power, SPA module that can be used across multiple Cisco platforms. The SPA DSP is designed for DSP-based voice and video solutions in the SPAs on the Cisco mid-range and high-end routers.

In Cisco IOS XE Release 3.2S, the following SPA DSP features have been deployed on the Cisco ASR 1000 Series Router for the session border controller (SBC):

- Associating SBC configuration with a DSP farm profile.
- Voice transcoding and transrating support using onboard DSP services.
- Dual tone multifrequency (DTMF) interworking using onboard DSP services.
- VoIPv4 and VoIPv6 transcoding and transrating support.
- Transcoding, transrating, and DTMF interworking call control and signaling control.

Cisco Unified Border Element (SP Edition) was earlier known as Integrated Session Border Controller, and is referred to as SBC in this document.

For a complete description of the commands used in this chapter, refer to the *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* document at: http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

For information about all the Cisco IOS commands, use the Command Lookup Tool at: http://tools.cisco.com/Support/CLILookup or the Cisco IOS master commands list.

### Feature History of SPA DSP on the Cisco Unified Border Element (SP Edition)

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.2S | The SPA DSP onboard services were introduced on the Cisco ASR 1000 Aggregation Series Routers. |
| Cisco IOS XE Release 3.3S | The Call Recovery feature was added. |
| Cisco IOS XE Release 3.8S | The AMR-WB feature was supported on the SBC on the Cisco ASR 1000 Aggregation Series Routers. |

# Contents

# Restrictions

The following restrictions are applicable to a SPA DSP:

- Voice, audio, and video conferencing are not supported.
- HA, system-level In-Service Software Upgrade (ISSU), and Nonstop Forwarding (NSF) are not supported.
- Video codecs are not supported.
- Although Online Insertion and Removal (OIR) is supported, the sessions going through a SPA at the time of removal are lost.
- The Cisco Unified Communications Manager is not supported.

# Prerequisites for the SPA DSP Services

The DSP farm definition and SBC configuration and activation must be completed before transcoding the SBC calls. For more information about SPA configuration, see the "Configuring the Cisco DSP SPA for the ASR 1000 Series" chapter in *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide* at:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ASR1000/asrcfgdsp.html

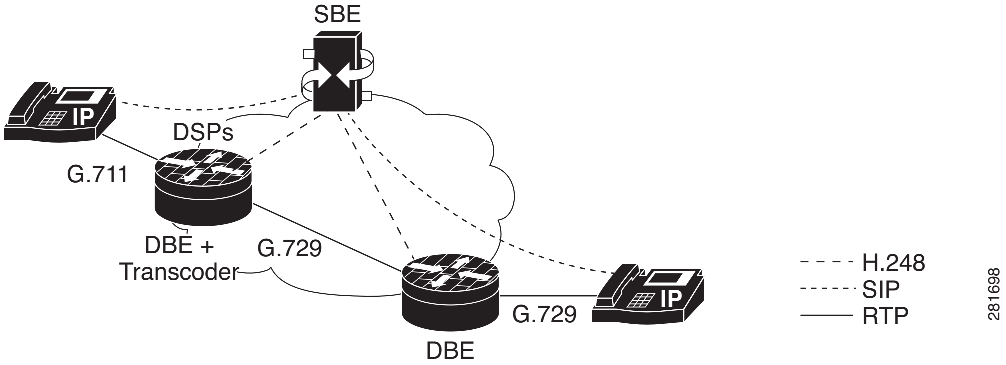
# Information About the SPA DSP Services

A SPA DSP contains digital signal processors and related hardware to provide voice transcoding capability for the SBC. In addition, Cisco Unified Border Element, Enterprise Edition can use a SPA DSP for simple voice transcoding services.

# Transcoding the SBC

SBC transcoding is used for codec translation between two VoIP networks as part of the Data Border Element (DBE) functions. Figure 10-1 shows how a SPA DSP performs codec transcoding for distributed SBC.

*Figure 10-1 SPA DSP Transcoding for Distributed SBC*



The SPA DSP allows the translation of one type of media stream or codec to another type of media stream that uses different media encoding and decoding technologies. Other translation activities include:

- Translation between different codecs
- Translation between different packetization settings (transrating)
- DTMF interworking

## Transcoding the Distributed SBC

Transcoding is inferred from a Session Description Protocol (SDP) that is used to program a call. Programming terminations in the same call containing different codecs implicitly instruct the distributed SBC to perform transcoding.

## Transrating the Distributed SBC

Transrating is inferred from the SDP that is used to program a call. Programming terminations in the same call with different ptime implicitly instruct the distributed SBC to perform transrating.

**Note** Transrating is supported only for the different rates using the same codec, not across codecs. Therefore, transrating and transcoding cannot be performed simultaneously.

# In-Band DTMF Interworking

The Cisco ASR 1000 Series Aggregation Services Routers support DTMF interworking between Real-Time Transport Protocol (RTP) in-band waveform, RTP telephone-event codec (RFC2833), and SIP DTMF indication types.

A DTMF tone can be generated using the following methods:

- SIP digit detection and generation package—A SIP message is sent from an endpoint to a SIP proxy, indicating that there has been a DTMF event, along with information about the type and duration of the event.
- RTP payload for DTMF (telephone-event codec)—The RTP packets contain information in their headers, indicating that a DTMF is being generated. The endpoints interpret these messages and play the DTMF locally.
- RTP in-band waveform—The DTMF is sent as part of the voice waveform.

For more information about DTMF interworking, see the "Implementing Interworking DTMF" chapter in the *Cisco Unified Border Element (SP Edition) Configuration Guide: Distributed Model* at:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/sbc_dtmf.html

## RTP Telephone-Event Codec-to-SIP Interworking

When an RTP packet is marked as DTMF using the telephone-event codec, the RTP packet is removed from the stream. The DBE sends an H.248 message to the signaling border element (SBE), indicating that a DTMF event has occurred, and that the RTP packet should be converted into a SIP DTMF event.

The call must meet the following conditions:

- The telephone-event codec (for RFC 2833) is present in side A of the SDP, but not in side B.
- The dd/etd event is subscribed for side A, but not for side B.

## SIP-to-RTP Telephone-Event Codec Interworking

When an endpoint generates a SIP signal, the SIP DTMF signals arrive completely out of band. An endpoint that supports SIP DTMF generates the signals to be sent to the SBE. In turn, the SBE recognizes that this is a DTMF message and sends an H.248 message to the DBE, indicating that a DTMF tone is required to be inserted into the RTP stream. The DBE then inserts the RTP DTMF packets into the audio stream using telephone-event codec.

The call must meet the following conditions:

- The telephone-event codec (for RFC 2833) is present in side B of the SDP, but not in side A.
- The dd/etd event is subscribed for side B, but not for side A.

## RTP Telephone-Event Codec-to-RTP In-Band Waveform

After the RTP packet is marked as DTMF using the telephone-event codec, the RTP packet is removed from the stream, and an RTP stream containing the DTMF waveform is sent to the other endpoint.

The call must meet the following conditions:

- The telephone-event codec (for RFC 2833) is present in side A of SDP, but not in side B.
- The dd/etd event is subscribed for side A and side B.

## RTP In-Band Waveform-to-RTP Telephone-Event Codec

After the DTMF is sent as part of the voice waveform, the RTP packets are removed from the stream, and the DBE inserts the a new RTP packet with the payload-type telephone event into the audio stream.

The call must meet the following conditions:

- The telephone-event codec (for RFC 2833) is present in side B of the SDP, but not in side A.

- The dd/etd event is subscribed for side A and side B

### SIP-to-RTP In-Band Waveform

After an endpoint generates a SIP signal, the SIP DTMF signals arrive completely out of band. The endpoint that supports SIP DTMF generates the signals to be sent to the SBE. In turn, the SBE recognizes that this is a DTMF message, and sends an H.248 message to the DBE, indicating that a DTMF tone is required to be inserted into the RTP stream. The DBE then inserts a stream containing the DTMF waveform.

The call must meet the following conditions:

- The telephone-event codec (for RFC 2833) is not present on either side A or side B.
- The dd/etd event is subscribed for side B.

### RTP In-Band Waveform-to-SIP

When the DTMF is sent as part of the voice waveform, the RTP packets are removed from the stream, and the DBE sends an H.248 message to the SBE, indicating that a DTMF event has occurred, and that the RTP packets should be converted into a SIP DTMF event.

The call must meet the following conditions:

- The telephone-event codec (for RFC 2833) is not present on either side A or side B.
- The dd/etd event is subscribed for side A.

## Call Recovery

From Cisco IOS XE Release 3.3S, calls on a partially crashed SPA DSP can be recovered within the call outage time of 2.5s.

When part of a SPA DSP crashes, a crash recovery process runs, and then the RP reprograms the crashed part of the SPA DSP with all calls that were previously on it. For example, a simple transcoding scenario, a-law to u-law transcoding, can represent up to 129 calls that require reprogramming.

Depending on the part of the SPA DSP that crashes, the total recovery time may be longer because it might have to recover more components and also reprogram more calls. However, the entire media path outage time for all the recovered calls is less than 2.5s.

In all cases of the SPA DSP call recovery, the call recovery occurs on the same SPA DSP where the call existed prior to the crash. The calls are not moved to another SPA DSP.

The SPA DSP failure call recovery can be disabled  or rendered ineffective if the SPA DSP crash dumps are enabled. It can push the call outage time beyond 2.5s.

The **show voice dsp group all** command indicates when a SPA DSP is undergoing call recovery.

```
Router# show voice dsp group all

Show DSP group all

DSP groups on slot 0 bay 0:
dsp 1:
  State: UP
  HA State : DSP_HA_STATE_PENDING1
  Max signal/voice channel: 43/43
  Max credits: 645
```

```
num_of_sig_chnls_allocated: 43
Transcoding channels allocated: 43
Group: FLEX_GROUP_XCODE, complexity: LOW
  Shared credits: 0, reserved credits: 645
  Transcoding channels allocated: 24
  Credits used (rounded-up): 360
```

**Note** The **show voice dsp group all** command displays the output `HA State : DSP_HA_STATE_PENDING1` only during the recovery process which can be upto a few milliseconds.

## AMR-WB Transcoding Support

Adaptive Multi-Rate Wideband (AMR-WB) is a patented speech coding standard based on Adaptive Multi-Rate encoding, using a methodology that is similar to the Algebraic code-excited linear prediction (ACELP). AMR-WB, which was specified by 3GPP, provides improved speech quality due to a wider speech bandwidth of 50 to 7000Hz compared to narrowband speech coders what are in general optimized for Plain old telephone service (POTS) wireline quality of 300 to 3400 Hz.

AMR-WB is codified as G.722.2, an ITU-T standard speech codec, formally known as Wideband coding of speech at around 16 kbps using AMR-WB. G.722.2 AMR-WB is the same codec as the 3GPP AMR-WB.

AMR-WB operates like AMR with nine different bit rates. The lowest bit rate providing excellent speech quality in a clean environment is 12.65 kbps. Higher bit rates are useful in background noise conditions and for music. Also, lower bit rates of 6.60 and 8.85 kbps provide reasonable quality, especially compared to narrowband codecs.

**Note** The AMR-WB feature requires DSP firmware with AMR-WB codec support.

shows the relationship between the AMR rate mode and bit-rate.

*Table 10-1 Relationship Between the AMR Rate Mode and Bit-Rate*

| Rate Mode | AMR Bit-Rate (kbps) | AMR-WB/G.722.2 Bit-Rate (kbps) |
|---|---|---|
| 0 | 4.75 | 6.60 |
| 1 | 5.15 | 8.85 |
| 2 | 5.90 | 12.65 |
| 3 | 6.70 | 14.25 |
| 4 | 7.40 | 15.85 |
| 5 | 7.95 | 18.25 |
| 6 | 10.20 | 19.85 |
| 7 | 12.20 | 23.05 |
| 8 | SID[1] | 23.85 |
| 9 | — | SID |

[1] SID: Silence Indicator

# Configuring the SPA DSP Services for the SBC

This section describes the tasks involved in configuring the SPA DSP services for the SBC:

- Configuring a DSP Farm Profile on DBE, page 10-7
- Configuring the SBC to Deactivate the SDP Analysis, page 10-8
- Configuring the SBC to Support AMR-WB on DBE, page 10-11

## Configuring a DSP Farm Profile on DBE

This section explains how to configure a DSP farm profile on DBE.

### SUMMARY STEPS

1. **show dspfarm** {**all** | **dsp** | **profile**}
2. **configure terminal**
3. **sbc** *sbc-name* **dbe**
4. **associate dspfarm profile** {*profile-number* | **all**}
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **show dspfarm** {**all** \| **dsp** \| **profile** *profile-identifier*}<br>**Example:**<br>`Router# show dspfarm profile all` | (Optional) Displays the DSP farm configuration information:<br>• **all**—Displays the DSP farm global information.<br>• **dsp**—Displays information pertaining to all the DSPs.<br>• **profile**—Displays the DSP farm profiles. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **sbc** *sbc-name* **dbe**<br>**Example:**<br>`Router(config)# sbc mySBC dbe` | Creates the DBE service on the SBC, and enters into the SBC-DBE configuration mode. |
| Step 4 | **associate dspfarm profile** {*profile-number* \| **all**}<br>**Example:**<br>`Router(config-sbc-dbe)# associate dspfarm profile 1` | Associates the SBC with a DSP farm profile:<br>• *profile-number*—Specifies the profile number to be associated.<br>• **all**—Allows the SBC to pick the most appropriate DSP farm profile from the profiles associated to the SBC for the transcoding session. |
| Step 5 | **end**<br>**Example:**<br>`Router(config-sbc-dbe)# end` | Exits SBC-DBE configuration mode and returns to privileged EXEC mode. |

# Configuring the SBC to Deactivate the SDP Analysis

This section explains how to configure the SBC to deactivate the SDP analysis that sets up a transcoded call.

### SUMMARY STEPS

1. **show dspfarm** {**all** | **dsp** | **profile**}
2. **configure terminal**
3. **sbc** *sbc-name* **dbe**
4. **no activate**
5. **vdbe**
6. **no attach-controllers**
7. **transcoding check** *{***match** | **none** | **overlap***}*
8. **controller h248** *controller-index*

9. **no transrating check**
10. **exit**
11. **attach-controllers**
12. **exit**
13. **activate**
14. **end**
15. **show sbc** *sbc-name* **dbe media-stats**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show dspfarm** {**all** \| **dsp** \| **profile** *profile-identifier*}<br>**Example:**<br>`Router# show dspfarm profile all` | (Optional) Displays the DSP farm configuration information:<br>• **all**—Displays the DSP farm global information.<br>• **dsp**—Displays information pertaining to all the DSPs.<br>• **profile**—Displays the DSP farm profiles. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **sbc** *sbc-name* **dbe**<br>**Example:**<br>`Router(config)# sbc mySBC dbe` | Creates the DBE service on the SBC, and enters SBC-DBE configuration mode. |
| **Step 4** | **no activate**<br>**Example:**<br>`Router(config-sbc-dbe)# no activate` | Deactivates the DBE. |
| **Step 5** | **vdbe**<br>**Example:**<br>`Router(config-sbc-dbe)# vdbe` | Enters the virtual data border element (vDBE) function mode of the SBC. |
| **Step 6** | **no attach-controllers**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# no attach-controllers` | Detaches the controllers with the **no attach-controllers** command. |
| **Step 7** | **transcoding check** {**match** \| **none** \| **overlap**}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# transcoding check none` | Configures the transcoding options:<br>• **check**—Enables transcoding checking.<br>• **match**—Specifies exact codec matching check.<br>• **none**—Specifies no codec matching check.<br>• **overlap**—Specifies overlapping codec matching check. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **`controller h248`** {*`controller-index`*}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# controller h248 1` | Configures the H.248 controller for the DBE, and enters into the H.248 controller configuration mode.<br>In the example provided here, the configured number 1 identifies the H.248 controller for the DBE. |
| **Step 9** | **`no transrating check`**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe-h248)# no transrating check` | Disables the transrating option:<br>**check**—Enables transrating checking. |
| **Step 10** | **`exit`**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe-h248)# exit` | Exits the H.248 controller configuration mode. |
| **Step 11** | **`attach-controllers`**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# attach-controllers` | Attaches the DBE to the H.248 controllers. |
| **Step 12** | **`exit`**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# exit` | Exits the vDBE configuration mode. |
| **Step 13** | **`activate`**<br>**Example:**<br>`Router(config-sbc-dbe)# activate` | Activates the DBE service of the SBC. |
| **Step 14** | **`end`**<br>**Example:**<br>`Router(config-sbc-dbe)# end` | Exits the SBC-DBE configuration mode and returns to the privileged EXEC mode. |
| **Step 15** | **`show sbc`** *`sbc-name`* **`dbe media-stats`**<br>**Example:**<br>`Router# show sbc MySBC dbe media-stats` | Lists the general DBE statistics. |

The following example shows an output of the **show sbc dbe media-stats** command that lists the count of the transcoded calls:

```
Router# show sbc MySBC dbe 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
```

# Configuring the SBC to Support AMR-WB on DBE

This section explains how to configure the SBC to support the AMR-WB on DBE.

## SUMMARY STEPS

1. **configure terminal**
2. **dspfarm profile** *profile-identifier* **transcode**
3. **codec amr-wb**
4. **sbc** *sbc-name* **dbe**
5. **associate dspfarm profile** *profile-identifier*
6. **activate**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters the global configuration mode. |
| Step 2 | **dspfarm profile** *profile-identifier* **transcode**<br>**Example:**<br>`Router(config)# dspfarm profile 20 transcode` | Enters the DSP farm profile configuration mode, and defines a profile for DSP farm services. |
| Step 3 | **codec amr-wb**<br>**Example:**<br>`Router(config-dspfarm-profile)#codec amr-wb` | Specifies the AMR-WB codec in the DSP farm profile. |
| Step 4 | **sbc** *sbc-name* **dbe**<br>**Example:**<br>`Router(config)# sbc mySBC dbe` | Creates the DBE service on the SBC, and enters the SBC-DBE configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **associate dspfarm profile** *profile-identifier*<br>**Example:**<br>`Router(config-sbc-dbe))# associate profile 20` | Associates a DSP farm profile to a Cisco Call Manager group. |
| **Step 6** | **activate**<br>**Example:**<br>`Router(config-sbc-dbe)# activate` | Initiates the DBE service of the SBC. |

# Configuration Examples of the SPA DSP Services for the SBC

This section contains the following examples:

- Example: Configuring a DSP Farm Profile on DBE, page 10-12
- Example: Configuring the SBC to Deactivate the SDP Analysis, page 10-12
- Example: Viewing DSP Farm Profile Configuration and Status, page 10-13
- Example: Configuring the SBC to Support AMR-WB on DBE, page 10-14

## Example: Configuring a DSP Farm Profile on DBE

The following example shows how to configure a DSP farm profile on DBE:

```
enable
configure terminal
 sbc MySBC dbe
  associate dspfarm profile 1
  end
```

## Example: Configuring the SBC to Deactivate the SDP Analysis

The following example shows how to configure SBC to deactivate the SDP analysis that sets up a transcoded call.

```
enable
configure terminal
 sbc mySBC dbe
  no activate
  vdbe
   no attach-controllers
    transcoding check none
   controller h248 1
   no transrating check
   exit
  attach-controllers
  exit
 activate
end
```

# Example: Viewing DSP Farm Profile Configuration and Status

After a DSP farm profile is created, use the **show** command to display the DSP farm profile configuration and status. The following examples show the output of the **show** commands:

```
Router# show running-config
!
voice-card 2/0
no dspfarm
dsp services dspfarm
!
dspfarm profile 20 transcode
codec g711ulaw
codec g711alaw
codec g729r8
codec g729ar8
codec g729br8
codec g729abr8
rsvp
maximum sessions 5
associate application SBC
!

Router# show dspfarm profile 20

Dspfarm Profile Configuration
Profile ID = 20, Service = TRANSCODING, Resource ID = 1
Profile Description :
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : SBC Status : ASSOCIATED
Resource Provider : FLEX_DSPRM Status : UP
Number of Resource Configured : 5
Number of Resource Available : 5
Codec Configuration
Codec : g729abr8, Maximum Packetization Period : 60
Codec : g711alaw, Maximum Packetization Period : 30
Codec : g711ulaw, Maximum Packetization Period : 30
Codec : g729r8, Maximum Packetization Period : 60
Codec : g729ar8, Maximum Packetization Period : 60
Codec : g729br8, Maximum Packetization Period : 60
RSVP : ENABLED
!

Router# show dspfarm all

DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 0(Avail: 0), Conferencing Sessions: 2 (Avail: 2)
Trans sessions for mixed-mode conf: 0 (Avail: 0), RTP Timeout: 600
Connection check interval 600 Codec G729 VAD: ENABLED
Total number of active session(s) 0, and connection(s) 0
SLOT DSP CHNL STATUS USE   TYPE SESS-ID CONN-ID PKTS-RXED PKTS-TXED
0   0   1   UP  FREE conf - -   -   -
0   0   2   UP  FREE conf- -   -   -
0   0   3   UP  FREE conf - -   -   -
0   0   4   UP  FREE conf - -   -   -
0   0   5   UP  FREE conf - -   -   -
0   0   6   UP  FREE conf - -   -   -
```

# Example: Configuring the SBC to Support AMR-WB on DBE

The following example shows how to configure the SBC to support the AMR-WB on DBE:

```
sbc system dbe
vdbe global
  h248-version 3
  h248-napt-package napt
  h248-profile gate-ctrl version 0
  local-port 2964
  control-address h248 ipv4 20.21.28.144
  controller h248 1
   remote-address ipv4 20.21.28.52
   remote-port 2984
   transrating check remote
  attach-controllers
media-address ipv4 20.24.26.144 managed-by mgc
  port-range 5000 40000 any
media-address ipv4 172.26.3.1 managed-by mgc
  port-range 5000 40000 any
media-address ipv4 172.26.3.2 managed-by mgc
  port-range 5000 40000 any
media-timeout 290
associate dspfarm profile 20
activate
```

CHAPTER 11

# High-Availability Support

This chapter describes high-availability support for the Cisco Unified Border Element (SP Edition) distributed model on the Cisco ASR 1000 Series Aggregation Services Routers.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at: http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

## Contents

This chapter provides information about the following topics:

## Cisco Unified Border Element (SP Edition) High Availability

The Cisco ASR 1000 Series Routers include the Cisco ASR 1002, Cisco ASR 1004, and Cisco ASR 1006 Routers. The different models support different types of redundancy. Cisco Unified Border Element (SP Edition) distributed model supports the redundancy available on each model.

On the Cisco ASR 1002 and Cisco ASR 1004 Routers, only software redundancy is available. These models have dual Cisco IOS software modules running on the same Route Processor, with one active and the other in standby mode.

The Cisco ASR 1006 Routers offer dual hardware redundancy and software redundancy.

Cisco Unified Border Element (SP Edition) high availability is provided in the standard image for the Cisco ASR 1000 Series Routers. There is no special configuration required.

For additional information, see “High Availability Overview” section in the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide* at *http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/asrswcfg.html*. Also see the *Cisco IOS High Availability Configuration Guide* at http://www.cisco.com/en/US/products/ps6922/products_installation_and_configuration_guides_list.html for information on high availability features that are on other Cisco platforms and that work identically on the Cisco ASR 1000 Series Aggregation Services Routers.

# Hardware Redundancy

Cisco Unified Border Element (SP Edition) distributed model supports use of a redundant or standby Route Processor (RP) and redundant Embedded Services Processor (ESP) on the Cisco ASR 1006 Router. The Cisco ASR 1006 Router has an ESP as well as an RP for dual hardware redundancy. If the active RP or active ESP hardware fails, the system performs a switchover to the standby RP or standby ESP. RP and ESP hardware redundancy support is independent. An RP failure does not require a switchover of the ESP hardware and an ESP failure does not require an RP switchover.

Hardware redundancy is available only on the Cisco ASR 1006 Router.

# Software Redundancy

On the Cisco ASR 1000 Series Routers, Cisco IOS runs as one of many processes within the Cisco IOS XE operating system. This architecture is different than on traditional Cisco IOS, where all processes are run within Cisco IOS. The Cisco ASR 1000 Series Router architecture allows for software redundancy opportunities not available on other Cisco IOS platforms.

Cisco Unified Border Element (SP Edition) distributed model supports software redundancy by running a standby peer SBC module within the IOS process that resides in an active RP. If the SBC module fails, then Cisco Unified Border Element (SP Edition) switches over to the standby SBC module in the standby IOS process. The standby IOS process may reside on the same Route Processor as the active IOS process (Cisco ASR 1002 and Cisco ASR 1004 Routers) or it may be on a redundant, standby RP (Cisco ASR 1006 Router).

On the Cisco ASR 1002 and Cisco ASR 1004 Routers, a standby Cisco IOS process is running on the same Route Processor as the active Cisco IOS process. In the event of a Cisco IOS failure, the Router switches to the standby Cisco IOS process. No redundant Route Processor or redundant ESP is available on the Cisco ASR 1002 Series and Cisco ASR 1004 Series Routers.

On the Cisco ASR 1006 Routers, the data border element (DBE) can have a redundant Route Processor and a redundant ESP. In the event of failure of the active Cisco IOS process, the Router switches to the standby Cisco IOS process, running on a separate standby Route Processor. SBC redundancy at the ESP level is provided only if a standby, redundant ESP is used. SBC components running on the active ESP have identical peer components running on the standby ESP. In this case, if the SBC components running on the active ESP fail, then a switchover to the backup ESP occurs.

The following types of software redundancy are supported on Cisco Unified Border Element (SP Edition) distributed model:

- Route Processor Redundancy (RPR)
- Stateful Switchover (SSO)
- In-Service Software Upgrade (ISSU)

# Route Processor Redundancy (RPR)

RPR allows you to run with a standby RP without state synchronization. In the event of a fatal error on the active RP, the system switches to the standby RP, which then completes its initialization. Because all the state information held by the formerly active RP is lost, the newly active RP has to configure itself and relearn all the state information.

Upon an RPR-based RP switchover event, all SBC calls already established (in a steady state) at the time of the switchover are lost. Some SBC calls in the process of being established at the time of the switchover are dropped as gracefully as possible. No new calls can be established briefly after the initial switchover event. An SBC call reconciliation takes place after an RPR-based RP switchover to ensure that both RP and Embedded Services Processor (ESP) are in sync.

RPR redundancy can allow for IOS fast software upgrades when ISSU is unavailable. In RPR mode, no Cisco IOS SBC state information is synchronized to the standby RP. Therefore, all calls are dropped upon an RPR-based switchover.

**Note** RPR is supported on the Cisco ASR 1000 Series Routers while RPR+ is not. You can use Stateful Switchover (SSO) instead of RPR+.

# SSO Support

Cisco Unified Border Element (SP Edition) support for Stateful Switchover (SSO) allows for stateful IOS process switchovers where critical state information is synchronized between one Route Processor used as the active processor and the other RP used as the standby processor. When Cisco IOS is configured for SSO, the SBC module running on the active IOS process constantly “replicates” its internal state to its standby peer SBC module on the standby IOS process. In this way, the standby SBC module is kept in sync with the active IOS process and has all the state information necessary to retain active calls and resume call processing in the event the active IOS process fails and an SSO occurs.

For information on SSO, see *Cisco IOS High Availability Configuration Guide* at:

http://www.cisco.com/en/US/products/ps6922/products_installation_and_configuration_guides_list.html

# ISSU Support

The Cisco Unified Border Element (SP Edition) distributed model supports In-Service Software Upgrade (ISSU) with a redundant RP or redundant IOS process. The ISSU process allows software to be updated or otherwise modified on a standby RP or standby IOS process while packet forwarding on the active RP or active IOS process continues. For the Cisco ASR 1000 Series Routers, ISSU compatibility depends on the software package being upgraded and the hardware configuration.

see “High Availability Overview” section in *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide* at:

*http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/asrswcfg.html* for more information on ISSU compatibility.

For information on the ISSU process, see *Cisco IOS In Service Software Upgrade and Enhanced Fast Software Upgrade Process* document at:

*http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/sb_issu.html*

CHAPTER 12

# Quality Monitoring and Statistics Gathering

The Data Border Element (DBE) deployment of the Cisco Unified Border Element (SP Edition) distributed model has a main objective in supporting quality monitoring and statistics reporting. The DBE supports generation of event messages detailing significant events that occur on each call. In addition, the DBE supports generation of correct billing, call usage and detail records.

Some of the monitoring events that the DBE tracks and reports are as follows:

- Checking on occurrence of hung calls using the H.248 Network Quality Alert event.
- Reporting on congestion events and critical status changes, such as a resource shortage or performance degradation, quality degradations of media streams, and service level agreement (SLA) violations.
- Reporting media timeout while the association with the controller is down.
- Enabling H.248 event storage and reporting.
- Detecting media gateway controller (MGC) failure.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

# Contents

This chapter provides information about the following topics:

- ServiceChange Notification for Interface Status Change, page 12-12

# Billing and Call Detail Records

One main function of Cisco Unified Border Element (SP Edition) is to generate correct billing, call detail and usage records. The DBE supports collecting statistics data and sending the data to the Signaling Border Element (SBE).

## Prerequisites for Implementing Billing

The following prerequisite is required to implement Cisco Unified Border Element (SP Edition) billing:

- Before implementing interworking billing, Cisco Unified Border Element (SP Edition) must already be configured. See the procedures described in Chapter 2, "Configuring the Cisco Unified Border Element (SP Edition) Distributed Model."

## Information About Billing

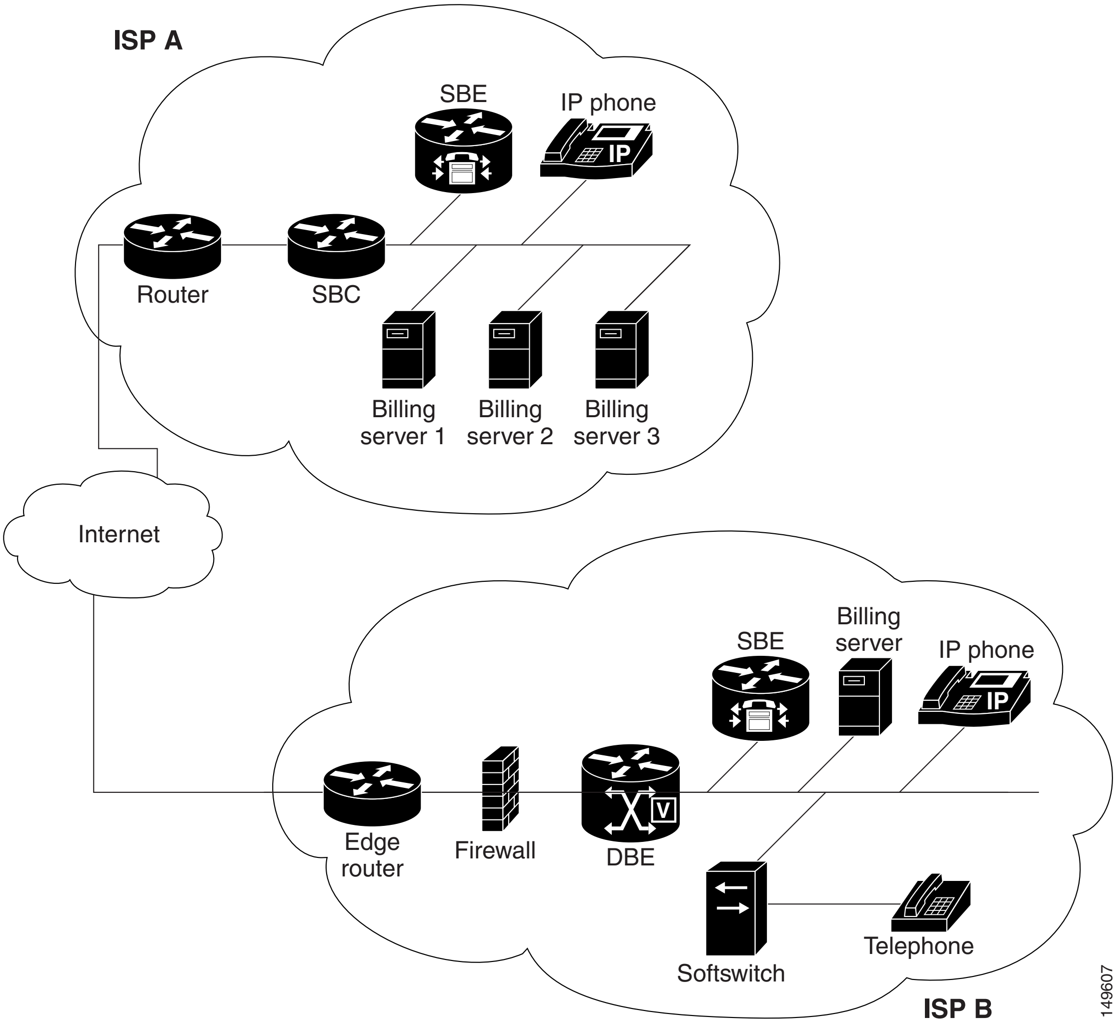
Integrated billing is achieved through the PacketCable Event Messages architecture (see the *PacketCable 1.5 Event Messages Specification*; PKT-SP-EM1.5-I01-050128) as shown in Figure 12-1 where the Cisco Unified Border Element (SP Edition) is integrated into this architecture. As shown, the billing server and softswitch both support PacketCable Event Messages.

ISP-B in Figure 12-1 shows Cisco Unified Border Element (SP Edition) operating in a distributed model where the billing system is being deployed using a single billing server and a softswitch. Note that ISP-A operates in the unified model.

In the distributed model, the system operates as follows:

- Only the SBE communicates with the billing server. That is, no event messages are generated by the DBE. All media-specific information (for example: gate request information and media statistics) is sent by the DBE to the SBE, which then generates event messages as required to send to the billing servers.
- The billing server collates billing information both from the SBE and the softswitch to provide the ISP with a single billing point. The softswitch only interface to the billing service is one of the ways service providers could use to get billing information. It is outside the scope of Cisco Unified Border Element (SP Edition) billing.

*Figure 12-1 Integrated Billing Deployment*



# Tracking Statistics

The following are some of the methods by which the DBE keeps track of statistics:

- Call statistics

  The DBE generates statistics for a given call by collecting information such as packet count and packets dropped. The DBE also snoops into the RTCP packets and reports back to the SBE at the end of the call. The DBE tracks and reports other statistics, such as call duration, media up event, media down event, and invalid source alert, to the SBE for billing and security purposes.

- H.248 Network Quality Alert (nt/qualert) event

  The H.248 nt/qualert event offers another method to check whether there are any hung calls. A voice call is considered a hung call when media packets are not present on the active stream and the call is not on hold nor has the hold timer expired. The H.248 nt/qualert feature generates a middlebox pinhole timer expired event when it detects this type of media loss. This feature is enabled by default.

- Discarded Packets Statistics

  The DBE tracks dropped packets when incoming packets fail to match the address and port mask specified using the H.248 Gate Management package. With this type of reporting, the DBE collects accurate packet information for a given user and also enhances network security.

# congestion-threshold Command

The **congestion-threshold** command configures the DBE to signal a congestion event to the SBE when a maximum percentage has been reached. 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.

# DBE Status Notification

The DBE notifies the SBE about critical status changes (for example, resource shortage or performance degradation).

# Enhanced Event Notification and Auditing

The Enhanced Event Notification and Auditing features address some of the limitations of H.248 event notification.

Previously, event notification was subject to the following limitations:

- If an H.248 event notification request from the DBE went unacknowledged by the MGC, then details of that event were lost, and the MG and MGC states could diverge as a result. (There is no current H.248 mechanism by which historical event information can be relearned by the MGC.)
- If the DBE switched to a new MGC for some reason, the new MGC had no means to learn what events had occurred on the streams and terminations programmed on the DBE. This behavior was particularly problematic for the nt/qualert and emp/phtoexp events, which are used to indicate that media has ceased flowing on a particular stream and can trigger the MGC to delete the context once all streams within the context reported either of these events.
- If an event notification failed, and the event being notified was not the inactivity timer event (it/ito), then the DBE did not reset the H.248 association with the MGC. As a result, the MGC could be unaware that it had failed to process some events.
- Silent gate deletion could occur because the DBE would delete contexts when all streams within the context had received media-down indications and there was no current H.248 association with an MGC.

With Enhanced Event Notification and Auditing, these limitations have been minimized with the following features:

- Retention and Returning of H.248 Event Information
- Association Reset
- Silent Gate Deletion
- Resetting the Media Timeout Timers

# Retention and Returning of H.248 Event Information

The storage of H.248 events is always turned on by default. A configuration option (the **h248-event-storage** command) enables two modes of H.248 events storage—permanent H.248 events storage and H.248 events storage until the events are acknowledged by the media gateway controller (MGC).

## Permanent H.248 Event Storage

The **h248-event-storage** command enables permanent events storage. In this mode, all H.248 events are retained until the stream on which they occurred is deleted.

These events are stored internally and reported to the SBE using a Notify command. A subsequent audit of the ObservedEvents descriptor for the stream can be used to return any events that are stored, with timestamp information indicating when the event actually occurred.

To reduce the memory required to store event information, the DBE only stores the most recent event of each type for each stream. The only exception is the dd/etd event, which indicates that the end of a dual-tone multifrequency (DTMF) tone has been detected, and also indicates which tone was detected. All instances of this event are stored because the entire sequence of tones is likely to be significant.

## H.248 Events Storage Until Event Acknowledgment

The system default is the mode where H.248 events are stored only until the events are acknowledged by the media gateway controller (MGC). This can also be enabled by the **no h248-event-storage** command.

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.

# Association Reset

A configuration option (the **h248-association-timeout** command) has been added that allows an alternative association reset behavior. The possible options are:

- The it/ito event is the only event where failure to notify the SBE about it causes the H.248 association with the SBE to be reset. (This behavior is the default and the standard H.248 protocol behavior.)
- Failure of any event notification causes an H.248 association with the SBE to be reset.

## Silent Gate Deletion

To prevent silent gate deletion, a configuration option (the **h248-preserve-gates** command) has been added that allows you to block this behavior. When silent gate deletion is blocked, all gates (media terminations and contexts) remain on the device until they are deleted by the SBE or the DBE service is deactivated.

## Resetting the Media Timeout Timers

The DBE will stop re-arming the media timeout timers after a pinhole timeout occurs. As a result, the receipt of a packet on a pinhole on which a media timeout has occurred will not generate a media-up notification, or restart the timer again.

The media timeout timers can be restarted by the MGC by its sending in a Modify request for the pinhole. An example of a Modify request is to change the state of an H.248 event subscription. In this case, the Modify request takes the call on hold or off hold and the DBE forwarding process changes the nt/qualert event subscription, which, in turn, restarts the media timeout timers.

## Restrictions for DBE Resetting the Media Timeout Timers

The following are DBE restrictions pertaining to Enhanced Event Notification and Auditing feature:

- After the DBE has determined that the Notify message for a given event occurrence has failed, it does not attempt to send the Notify message again.
- The event buffering model of DBE is unchanged. The DBE continues to detect and report events that match the current events descriptor.
- Receipt of a transaction response acknowledgement for an AuditValue response is not used to clear the ObservedEvents descriptor.

## Related Commands

The commands related to the resetting the media timeout timers include:

The **h248-event-storage** command enables permanent H.248 event storage, which retains all H.248 events until the stream on which they occurred is deleted.

The **h248-association-timeout** command configures the DBE to reset associations with a SBE when the controller does not respond to an event notification.

The **h248-preserve-gates** command configures the DBE to preserve the media terminations or contexts when there is a media timeout while the association with the controller is down.

# H.248 Network Package Quality Alert Event and Middlebox Pinhole Timer Expired Event

When the DBE detects media loss (media has stopped flowing and a call is not on hold), the DBE may issue one or more H.248/Megaco events to the media gateway controller (MGC): a Network (nt) package Quality Alert (qualert) event, a Middlebox Pinhole Timer Expired event[1], or both events.

## Network Package Quality Alert Event

The DBE will return a Network (nt) package Quality Alert (qualert) event when media loss is detected if the media gateway controller (MGC) requests it.

When the MGC requests an nt/qualert event, it specifies a Threshold parameter value based on a percentage of network quality loss. Although the DBE accepts any valid value (0 through 99) for this parameter, only a value of 99 triggers the generation of the nt/qualert event because the DBE only detects complete media failure and is not able to detect partial frame loss, which can occur during network congestion.

Requests for nt/qualert events are on a per-stream or per-termination basis, but the event is always reported on a per-stream basis. The event subscription can be added or removed during the lifetime of the stream. The event is monitored independently for each side of the stream.

## Middlebox Pinhole Timer Expired Event

The **h248-media-alert-event** command defines whether a Middlebox Pinhole Timer Expired event is generated when the DBE detects media loss.

**Note** The Middlebox Pinhole Timer Expired event and the Network package Quality Alert event are independently generated, so that either, both, or neither of these events are generated when the DBE detects media loss.

## Restrictions for DBE Middlebox Pinhole Timer Expired Event

The following are restrictions pertaining to DBE support for the H.248 Network Package Quality Alert Event feature:

- The DBE does not send notification when the last termination in a context expires.
- The DBE deletes the context when all of its terminations time out during an H.248 association outage.
- When an H.248 association is down and then resumes, the DBE resumes sending notification events. However, during the H.248 association outage, notification events may be lost after retries.

[1] ETSI TS 101 332 Version 4.1.1

## Related Command

The **h248-media-alert-event** command is used to enable or disable the Middlebox Pinhole Timer Expired event when the DBE detects media loss.

# Improved Media Timeout Detection

In the previous media timeout functionality on the data border element (DBE), if no SBC packets had been seen by the configured number of seconds since the call had been established, the DBE generated a media timeout alert to the media gateway controller (MGC). The enhanced media timeout capability delays reporting of the media timeout event by instructing the DBE to wait until it has received the first packet since the call was established. Only then does the media timeout timer start counting the number of seconds for which it has not seen an SBC packet. At the end of the count, the DBE generates an alert to the MGC. During the reporting delay, SBC packets can continue to be forwarded because there is no media timeout yet.

The following example describes how this enhanced media timeout capability is used. In a scenario where the improved media timeout detection is not configured, a signaling node fails during call setup and takes 30 seconds to recover. Therefore, the SIP “200 OK” is delayed from reaching the caller by 30 seconds. During this time, the caller is unable to send any media to the callee. This results in the callee’s DBE reporting a media timeout notification (nt/qualert) to the MGC. The undesirable timeout is avoided by configuring the improved media timeout detection capability. The configuration is done with a new **first-packet** option on the **media-timeout** command.

The **first-packet** keyword of the **media-timeout** command instructs the DBE to wait until it receives the first SBC packet on a flow before starting the media timeout function. See *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html for more details on the **media-timeout** command.

## Restriction for DBE Improved Media Timeout Detection

In this mode, no media alerts can be generated until the first packet is seen on a flow.

## Configuring Improved Media Timeout Detection

This section contains steps to configure the Improved Media Timeout Detection functionality in a typical configuration scenario on the Cisco ASR 1000 Series Routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface sbc** {*interface-number*}
4. **ip address** *ip-address*
5. **exit**
6. **sbc** {*sbc-name*} **dbe**

7. **media-timeout** {*timeout*} **first-packet**
8. **vdbe** [**global**]
9. **h248-version** *version*
10. **h248-napt-package** [**napt** | **ntr**]
11. **local-port** {*port-num*}
12. **control-address h248 ipv4** {*A.B.C.D*}
13. **controller h248** {*controller-index*}
14. **remote-address ipv4** {*A.B.C.D*}
15. **remote-port** {*port-num*}
16. **transport** {**udp** | **tcp**} [**interim-auth-header**]
17. **exit**
18. **attach-controllers**
19. **exit**
20. **location-id** {*location-id*}
21. **media-address ipv4** {*A.B.C.D*}
22. **activate**
23. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **`enable`**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **`configure terminal`**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **`interface sbc`** {*`interface-number`*}<br>**Example:**<br>`Router(config)# interface sbc 1` | Creates an SBC virtual interface and enters into interface configuration mode. |
| **Step 4** | **`ip address`** *`ip-address`*<br>**Example:**<br>`Router(config-if)# ip address 1.1.1.1 255.0.0.0` | Configures an IP address on the SBC virtual interface. |
| **Step 5** | **`exit`**<br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **sbc** {*sbc-name*} **dbe**<br>**Example:**<br>`Router(config)# sbc global dbe` | Creates the DBE service on the SBC and enters into SBC-DBE configuration mode. |
| **Step 7** | **media-timeout** {*timeout*} **first-packet**<br>**Example:**<br>`Router(config-sbc-dbe)# media-timeout 1000 first-packet` | Configures the DBE to wait until it receives the first SBC packet after the call has been established before it starts to count the configured number of seconds, after which the DBE generates a media timeout alert to the SBE. |
| **Step 8** | **vdbe** [**global**]<br>**Example:**<br>`Router(config-sbc-dbe)# vdbe global` | Enters into VDBE configuration mode with a default DBE named “global”.<br>Only one DBE is supported and its name must be “global”. |
| **Step 9** | **h248-version** *version*<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# h248-version 3` | Specifies that the DBE uses an H.248 version when it forms associations with an H.248 controller.<br>Version 2 is the default. |
| **Step 10** | **h248-napt-package** [**napt** \| **ntr**]<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# h248-napt-package napt` | Defines whether the DBE uses the Network Address and Port Translation (NAPT) or NAT Traversal (NTR) H.248 package for signaling NAT features. NTR is the default.<br>The example shows how to configure the DBE to use NAPT. |
| **Step 11** | **local-port** {*port-num*}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# local-port 2971` | Configures the DBE to use the specific local port number when connecting to the default media gateway controller (MGC). |
| **Step 12** | **control-address h248 ipv4** {*A.B.C.D*}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# control-address h248 ipv4 200.50.1.41` | Configures the DBE to use a specific IPv4 H.248 control address, which is the local IP address the DBE uses as its own address when connecting to the SBE. |
| **Step 13** | **controller h248** {*controller-index*}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# controller h248 2` | Configures the H.248 controller for the DBE and enters into Controller H.248 configuration mode.<br>In the example, the configured number 2 identifies the H.248 controller for the DBE. |
| **Step 14** | **remote-address ipv4** {*A.B.C.D*}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe-h248)# remote-address ipv4 200.50.1.254` | Configures the IPv4 remote address of the H.248 controller for the SBE.<br>In the example, 200.50.1.254 is configured as the remote SBE IP address. |
| **Step 15** | **remote-port** {*port-num*}<br>**Example:**<br>`Router(config-sbc-dbe-vdbe-h248)# remote-port 2971` | Configures the port number of the H.248 controller that is used to connect to the SBE. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 16** | **transport** {**udp** \| **tcp**} [**interim-auth-header**]<br>**Example:**<br>`Router(config-sbc-dbe-vdbe-h248)# transport udp` | Configures the DBE to use either UDP or TCP for H.248 control signaling, and to configure the Interim Authentication Header (IAH). |
| **Step 17** | **exit**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe-h248)# exit` | Exits Controller H.248 configuration mode. |
| **Step 18** | **attach-controllers**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# attach-controllers` | Attaches the DBE to an H.248 controller. |
| **Step 19** | **exit**<br>**Example:**<br>`Router(config-sbc-dbe-vdbe)# exit` | Exits VDBE configuration mode. |
| **Step 20** | **location-id** {*location-id*}<br>**Example:**<br>`Router(config-sbc-dbe)# location-id 1` | Configures a location ID for the DBE.<br>The location ID is used by the network to route calls. |
| **Step 21** | **media-address ipv4** {*A.B.C.D*}<br>**Example:**<br>`Router(config-sbc-dbe)# media-address ipv4 1.1.1.1 255.0.0.0` | Adds the IPv4 address to the set of addresses, which can be used by the DBE as a local media address. This address is the SBC virtual interface address. Configure this command for each IP address that you specified under the SBC virtual interface in Step 4. |
| **Step 22** | **activate**<br>**Example:**<br>`Router(config-sbc-dbe)# activate` | Initiates the DBE service of the SBC. |
| **Step 23** | **end**<br>**Example:**<br>`Router(config-sbc-dbe)# end` | Exits SBC-DBE configuration mode and returns to privileged EXEC mode. |

# Improved Media Timeout Detection Configuration Example

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 MGC:

```
interface sbc 1
 ip address 1.1.1.1 255.0.0.0
sbc global dbe
media-timeout 1000 first-packet
 vdbe global
  use-any-local-port
  control-address h248 ipv4 210.229.108.254
 controller h248 1
  remote-address ipv4 210.229.108.252
 attach-controllers
location-id 1
media-address ipv4 1.1.1.1
activate
```

# Provisioned Inactivity Timer

The DBE can be configured with a default value for the H.248 connection’s inactivity timer value (the it and ito properties). This default value is used if the media gateway controller (MGC) does not request that the DBE runs an inactivity timer.

The advantage is that the DBE can detect media gateway controller (MGC) failure whether or not the MGC has subscribed to the inactivity timer event.

The system default is that no provisioned inactivity timer is configured. The provisioned timer is started when a successful response is received to the media gateway (MG) initial ServiceChange request to the MGC.

The MGC subscription timer duration can override the provisioned timer duration value if the MGC subscribes to the inactivity timer with a different timer duration than the provisioned timer duration. However, the subscribed timer value is replaced by the provisioned timer value if the MGC cancels its subscription or the association fails.

## Related Commands

The **h248-inactivity-duration** command configures the duration of the inactivity timer. The provisioned duration time is zero unless the user sets the duration parameter. It returns to zero if the user configures the **no h248-inactivity-duration** command.

# ServiceChange Notification for Interface Status Change

This 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. This feature is described in the “ServiceChange Notification for Interface Status Change” section on page 6-22.

CHAPTER 13

# Topology Hiding

The Cisco Unified Border Element (SP Edition) distributed model for the Cisco ASR 1000 Series Routers has a primary purpose in protecting the network and providing seamless interworking functions. Cisco Unified Border Element (SP Edition) can protect the network by hiding the network addresses and names for both the access (customer) side and the backbone (network core) side. Cisco Unified Border Element (SP Edition) also provides network protection for firewalls or home gateway users with private addresses.

When a user connects to the outside network, its IP address and port needs to be properly translated to protect its identity. The data border element (DBE) performs translation of IP addresses and port numbers via Network Address and Port Translation (NAPT) and Network Address Translation (NAT) Traversal functions in both directions.

The DBE implementation supports the H.248 NAPT package, the IP NAT Traversal Package, and the ETSI TS 102 333 specification for NAT Traversal, but only one package can be active. Latch and Relatch functions of the NAT Traversal are supported by the IP NAT Traversal package. Support for these packages help protect IP addresses of the endpoints going across the other side of the network.

The NAPT implementations on the DBE described in more detail in this chapter are summarized below:

- IPv4 Twice NAPT—Where both access side and backbone side addresses are protected. In Twice NAPT, both the IP address and port are translated to a local IP address and port; and both of the end points on each side see the SBC address as a destination address.
- IPv6 Single NAPT for signaling packets—This function is useful for protecting the signaling infrastructure part of the backbone side. The backbone side is able to identify the address of the customer; however, for the customer, only the interface address of the DBE is visible.
- IPv6 No NAPT for media packets—With this method, there is no privacy on the customer side or backbone side. Both sides know each other’s address and the DBE transparently passes the packets.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, see *Cisco Unified Border Element (SP Edition) Command Reference: Distributed Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbc_book.html

# Contents

This chapter provides information about the following topics:

# NAPT and NAT Traversal

NAPT and NAT Traversal are described in Chapter 9, "Security in Cisco Unified Border Element (SP Edition) Distributed Model."

# IP NAPT Traversal Package and Latch and Relatch Support

The IP NAPT Traversal Package and Latch and Relatch Support functions are described in Chapter 9, "Security in Cisco Unified Border Element (SP Edition) Distributed Model."

# IPv4 Support for Twice NAPT

The DBE successfully forwards media through Twice Network Address and Port Translation (NAPT) pinholes that form coupled pairs. For Twice NAPT hairpinning, the DBE forwards media on demand. The SBE sees no differences between Twice NAPT hairpins and Twice NAPT non-hairpins.

When forwarding media, a hairpinned pair behaves the way two separate pinholes behave, except that a packet going through a coupled pair has its IP Time-to-Live counter decremented only once, not twice.

**Note** Twice NAPT is only supported on IPv4.

# IPv6 Inter Subscriber Blocking

Inter subscriber blocking prevents a subscriber from connecting to other subscribers without first going through a successful signaling/call setup process and having a termination established for the stream.

When the SBC DBE is implemented in the IPv4 environment, the DBE supports Twice NAPT, which has well-defined local media IP addresses or IP address pools. In the IPv4 environment, the DBE drops all SBC traffic destined for SBC local media IP addresses if there is no in-service termination successfully retrieved.

However, in the IPv6 environment, the SBC DBE only supports No NAPT for media pinholes, which, unlike Twice NAPT, does not have well-defined local media IP addresses or IP address pools. Because the same DBE Router routes non-SBC IPv6 traffic (which does not have SBC termination flow entry whatsoever), the default operation for IPv6 traffic that does not have a corresponding termination flow entry is to continue to switch these packets. This can result in a situation where subscribers are still able to connect to other subscribers through the SBC DBE Router without completing the signaling and call setup process.

To support inter subscriber blocking in the IPv6 environment, you must classify subscribers at the ingress interface so that non-SBC traffic and SBC traffic can be differentiated.

For example, you might configure QoS at the ingress interface to mark all subscriber traffic with an unused unique differentiated services code point (DSCP) value, and then configure QoS at the egress interface to drop all the packets with this unused unique DSCP value. For SBC traffic with a termination flow entry, a separate DSCP value should be used to replace the original DSCP for these SBC packets as part of the normal diffserv package processing. As a result of this configuration, SBC packets with a session established will be routed and forwarded though the egress interface without being dropped because they have an SBC DBE-updated DSCP value. Depending on the QoS classification, you also have the flexibility of blocking partial traffic between subscribers without a session established or blocking all the traffic between them.

IPv6 inter subscriber blocking can be implemented using two methods: Quality of Service (QoS) policy-map-based inter subscriber blocking, or access control list (ACL)-based inter subscriber blocking.

## QoS Policy Map-Based Inter Subscriber Blocking Method

In the following example of the QoS policy map-based inter subscriber blocking method, all the packets entering the Router (DBE) (through 0/1.1101) are marked using the policy-map INPUT_POLICY with DSCP=default (0). Any packets leaving the DBE (gigabitEthernet 0/2) with DSCP=0 will be blocked by the class-map IPv6_intersubscriber in the policy-map CORE_OUT. IPv6_intersubscriber uses the ACL ipv6_dscp0_any.

```
Router# show run interface gigabitEthernet 0/1.1101
...
Current configuration : 711 bytes
!
interface GigabitEthernet0/1.1101
encapsulation dot1Q 1101
ip dhcp relay information option subscriber-id 1101
ip address 12.21.1.1 255.255.255.0
ip access-group InFilter_IPv4 in
ip access-group OutFilter_IPv4 out
ip verify unicast reverse-path
ip helper-address 12.1.99.2
pppoe enable group global
ipv6 address 2000:12:21:1::1/64
ipv6 address FE80::1 link-local
ipv6 traffic-filter InFilter_IPv6 in
ipv6 traffic-filter OutFilter_IPv6 out
ipv6 verify unicast reverse-path
ipv6 mld explicit-tracking
ipv6 mld access-group VLAN1
ipv6 dhcp relay destination 2000:12:1:99::2
snmp trap link-status
no cdp enable
service-policy input INPUT_POLICY
service-policy output PARENT_OUTPUT_POLICY
end
```

```
Router# show policy-map INPUT_POLICY
Policy Map INPUT_POLICY
  Class class-default
  set dscp default

Router# show policy-map PARENT_OUTPUT_POLICY
Policy Map PARENT_OUTPUT_POLICY
  Class class-default
  Average Rate Traffic Shaping
  cir 100000000 (bps)
  service-policy CHILD_OUTPUT_POLICY

Router# show policy-map CHILD_OUTPUT_POLICY
Policy Map CHILD_OUTPUT_POLICY
  Class EF
  set cos 5
  set dscp ef
  priority level 1 10000 (kbps)
  Class AF4
  set cos 4
  priority level 2 75000 (kbps)
  Class AF1
  set cos 1
  priority level 2 5000 (kbps)
  Class IPv6_intersubscriber
  police cir 8000 bc 1500
  conform-action drop
  exceed-action drop
  Class class-default
  set cos 0
  bandwidth 9990 (kbps)
  queue-limit 1 packets

Router# show class-map IPv6_intersubscriber
Class Map match-all IPv6_intersubscriber (id 16)
  Match access-group name ipv6_dscp0_any

Router# show ipv6 access-list ipv6_dscp0_any
IPv6 access list ipv6_dscp0_any
  permit ipv6 any any dscp default sequence 10
  deny ipv6 any any sequence 20

Router# show run interface gigabitEthernet 0/2
...
Current configuration : 505 bytes
!
interface GigabitEthernet0/2
description to AER1-1 gi0/0/0/2
ip address 12.11.21.2 255.255.255.252
ip access-group Core_InFilter in
load-interval 30
carrier-delay msec 5
media-type sfp
speed 1000
duplex full
negotiation auto
ipv6 address 2000:12:11:21::2/64
ipv6 traffic-filter Core_InFilter_IPv6 in
ipv6 traffic-filter OutFilter_IPv6 out
no ipv6 mld Router
snmp trap link-status permit duplicates
keepalive 1
service-policy output CORE_OUT
```

```
hold-queue 1000 in
hold-queue 1000 out
end

Router# show policy-map CORE_OUT
Policy Map CORE_OUT
 Class IPv6_intersubscriber
 police cir 8000 bc 1500
 conform-action drop
 exceed-action drop
 Class class-default
```

## ACL-Based Inter Subscriber Blocking Method

In the following example of the ACL-based inter subscriber blocking method, packets entering the DBE from the access side are marked with DSCP=0 using the same INPUT_POLICY as the QoS method above, but packets leaving the DBE use the ACL OutFilter_IPv6 as follows:

```
Router# show ipv6 access-list OutFilter_IPv6
IPv6 access list OutFilter_IPv6
 permit icmp any any packet-too-big sequence 10
 deny icmp any any sequence 20
 deny ipv6 any any dscp default sequence 40
 permit ipv6 any any sequence 50
```

## Restrictions for DBE ACL-Based Inter Subscriber Blocking Method

The following is a restriction pertaining to DBE support for IPv6 inter subscriber blocking:

Because the configuration of inter subscriber blocking in the IPv6 environment relies on Cisco IOS QoS to mark the DSCP value in the ingress feature process, the original DSCP value of the packets arriving at the DBE Router will not be preserved.

# IPv6 Support

IPv6 support includes the following functionality:

- The DBE supports IPv6 pinholes for both media endpoints and signaling endpoints.

  See the "IPv6 Pinholes" section on page 13-6.

  **Note** *Pinhole* is an informal term for a pair of terminations in the same stream and same context.

- Media flows do not support Network Address and Port Translation (NAPT); they must be No NAPT.

  As a result, you cannot configure any media addresses under IPv6. Media flows may consist of voice or video.

- Signaling flows support Single NAPT.

  You are able to configure signaling addresses under IPv6.

The DBE examines all IPv6 packets that arrive from the network and determines which ones belong to authorized SBC media streams. The DBE normally uses the destination (and possibly the source) IP address and port for packet classification. The DBE identifies packets belonging to an authorized media stream as SBC packets and applies the appropriate traffic policing rules to the packets. The counter showing number of packets received is modified.

After that, SBC performs packet processing and updating. The packet is forwarded out of the specified interface. IPv6 packet forwarding works in the same way as IPv4 packet forwarding, except for a few differences in the IP header processing.

Single NAPT for signaling means that packets arriving from an endpoint are addressed to an SBC media address. When they are passed to the media gateway controller (MGC), also know as an SBE, the packets need to keep the endpoint's source IP address and port number. Therefore, only destination addresses and ports are translated in Single NAPT. When the MGC/SBE sends a reply back to the endpoint, the packet has the endpoint's IP address as the destination address, and the MGC/SBE IP address as the source address. In Single NAPT, the DBE changes the source address to use the DBE IP address. See the "IPv6 Single NAPT for Signaling" section on page 13-7.

No NAPT means the received SBC packets do not contain any DBE local addresses because the DBE does not translate any IP addresses and ports during packet forwarding. The DBE rewrites neither the source nor destination addresses and ports in both directions. See the "IPv6 No NAPT Support for Media Flows" section on page 13-7.

# IPv6 Pinholes

DBE support for IPv6 pinholes includes the following functionality:

- The DBE supports forwarding of media from one IPv6 endpoint to another IPv6 endpoint.
- The DBE supports IPv4 and IPv6 endpoints simultaneously. However, no interworking between IPv4 and IPv6 endpoints is supported. IPv4 endpoints can only forward media to other IPv4 endpoints and IPv6 endpoints can only forward media to other IPv6 endpoints.
- The DBE supports configuration of IPv6 pinhole addresses and pinhole address pools.
- DBE supports signaling pinholes using IPv6 addresses.

Support is added for the MGC to specify the address and port in the Megaco local descriptor for terminations as one of the following:

- An address and port that are not owned by the SBC and not configured in a media address range on the SBC, but matching the remote address and port for the other termination in the stream.
- An address range, in the form of a classless interdomain routing (CIDR) mask (for example, 10.13.8.0/21) together with a 0 port number, that does not overlap with any address ranges owned by the SBC or any media address range configured on the SBC, but the address and port match the gm/rsam (Gate Management/remote source address mask) for the other termination in the stream.

SBC recognizes these "local" addresses as signifying Single NAPT pinholes. And if specified for both terminations in the stream, SBC recognizes these addresses as No NAPT pinholes. All pinholes only forward packets to a full destination address and port that was either specified in the remote descriptor or latched to (within a gm/rsam that matches the local address mask).

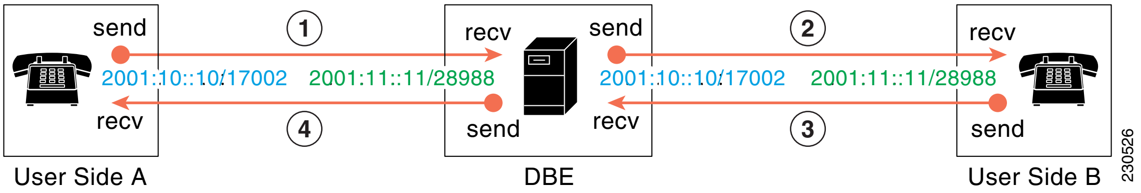
# IPv6 No NAPT Support for Media Flows

To support IPv6 on the DBE deployment, media flows do not support NAPT. No NAPT support means that no IP addresses and ports are translated by the DBE from a private address to a public address (for multiple users to share a single public address).

Because media addresses and ports are not translated, media flows on both sides of the media address are programmed with private, local addresses and ports that do not belong to the DBE. These local addresses and ports are specified by the MGC to match the remote address and port on the opposite side of the media address. Traffic in both directions is addressed directly to the remote endpoint on the other side of the DBE. The DBE rewrites neither the source nor destination addresses and ports in both directions because the DBE does not translate any IP addresses and ports during packet forwarding. Neither the source address nor destination address contains any DBE local media addresses.

Figure 13-1 illustrates a No NAPT media flow through the DBE between user side A and user side B.

***Figure 13-1 No NAPT Media Flow***



1. User side A sends a packet from IP address and port 2001:10::10/17002 to destination address and port 2001:11::11/28988 on side B. The DBE intercepts this packet and matches it to the side A flow.
2. The DBE applies QoS policing and forwards the packet to endpoint B without changing the destination address to a DBE local media address (as is done in Single NAPT). Under No NAPT processing, the DBE does not rewrite either source or destination IP addresses and ports.
3. Side B sends a packet from IP address and port 2001:11::11/28988 to originating source address and port 2001:10::10/17002. The DBE intercepts this packet and matches it to the side B flow.
4. The DBE applies QoS policing and forwards the packet to user side A without rewriting either source or destination IP addresses and ports.

# IPv6 Single NAPT for Signaling

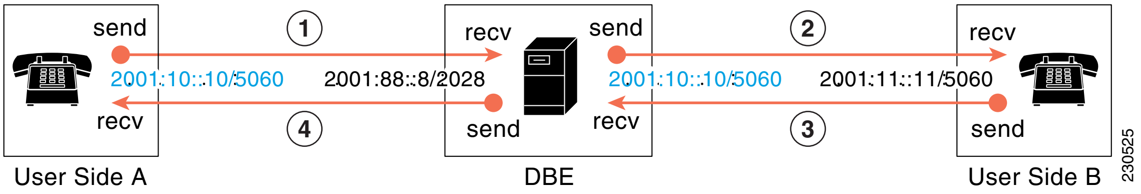
Support of IPv6 signaling flows requires Single NAPT.

The DBE is able to translate IP addresses and port numbers in both directions of a flow. However, Single NAPT means only one IP address and port is translated. In Single NAPT processing, the flow on one side of the pinhole is programmed with a local address and port that do not belong to the SBC. Instead, that local address and port of the flow are specified by the MGC to match the remote address and port on the other side of the pinhole. Thus, incoming traffic (downstream traffic of SIP server to access side) is addressed directly to the remote endpoint and the SIP server details are hidden from subscribers. Network topology must be used to route the downstream traffic through the DBE. In one sense, Single NAPT provides one-way topology hiding.

SBC rewrites destination IP address and port for packets received from the user. SBC does not rewrite source IP address and port of packets received from the user (they are unchanged from the IP address and port of the source endpoint). Correspondingly, SBC rewrites the source IP address and port of packets received from the MGC, but not the destination IP address or port.

Figure 13-2 illustrates a Single NAPT signaling flow through the DBE between user side A and user side B.

***Figure 13-2 Single NAPT Signaling Flow***



1. User side A sends a packet from IP address and port 2001:10::10/5060 to the DBE's local media address and port 2001:88::8/2028 for this pinhole. User side A only knows the DBE's local address and port 2001:88::8/2028. The source IP address is within the specified gm/rsam, so the DBE matches this packet to the flow.
2. The DBE applies QoS policing and forwards the packet to the MGC (user side B) without rewriting the source IP address and port. Under Single NAPT processing, the DBE changes the destination address and port to 2001:11::11/5060 on the MGC (side B) by replacing 2001:88::8/2028 with side B's address and port from the remote descriptor on side B. The MGC (side B) does not know about the 2001:88::8/2028 address and port on the DBE. After the DBE performs latching, the source address and port from side A becomes, in effect, the destination address and port in step 3 and step 4 for side B.
3. The MGC (side B) sends a packet to user side A with the destination address and port 2001:10::10/5060 copied from the source IP address and port of the packet it just received—that is, the address and port of side A. The DBE has intercepted the packet and matched it to the side B flow.
4. The DBE applies QoS policing and forwards the packet to side A without rewriting the destination IP address and port 2001:10::10/5060. However, under Single NAPT processing, the DBE rewrites the source IP address and port 2001:11::11/5060 to be 2001:88::8/2028, which is the local address and port of the side A flow.

# Restrictions for DBE IPv6 Single NAPT for Signaling

The following are restrictions pertaining to DBE support for IPv6 pinholes:

- DBE does not support IPv6 for control communications with the SBE. H.248 communication with the controlling SBE is over IPv4 only.
- DBE does not support IPv6 addresses that are not global unicast addresses.
- DBE does not support IPv6 addresses that do not use the default zone.

- DBE does not use the IPv6 Flow Label to classify packets. It continues to use the transport protocol type (UDP/TCP) and local and remote ports, as with IPv4. Outgoing packets originating from the DBE, such as DTMF packets, have a Flow Label of 0.
- DBE does not support forwarding between IPv4 and IPv6 endpoints. In particular, 6 to 4 addresses (prefixed with 2002::/16) are treated as global unicast native IPv6 addresses.
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) link-local addresses are not supported.

## Related Commands

The commands related to IPv6 Single NAPT for Signaling include:

- The **ipv6 address (session border controller)** command sets or creates the IPv6 address prefix on an SBC interface.
- The **media-address ipv6** command adds an IPv6 address to the set of addresses that can be used by the DBE as a local media address.
- The **media-address pool ipv6** command creates a pool of sequential IPv6 media addresses that can be used by the DBE as local media addresses.
- The **port-range (ipv6)** command creates a port range associated with a single IPv6 media address or a pool of IPv6 media addresses. IPv6 addresses must be configured with the **signaling** keyword. The **any**, **voice**, **video,** and **fax** keywords supported in the IPv4 **port-range** command are not supported in IPv6.
- The **ipv6** {*ipv6-address*} keyword is added to the **debug sbc filter** command.
- The **ipv6** {*ipv6-address*} keyword is added to the **show sbc dbe media-flow-stats** and **show sbc dbe signaling-flow-stats** commands.

# No NAPT Pinholes

No NAPT pinholes can form coupled pairs only under the following circumstances:

- Both pinholes are No NAPT.
- Each “internal termination” has local and remote addresses that are identical to those of the external termination on the associated pinhole.

**Note** The two terminations between which media loops back are called the “internal terminations” of their respective pinholes. Only external terminations directly receive packets from the network.

- Any remote source address masks (rsams) are duplicated. For example, if a termination with remote address A in one pinhole has an rsam of 1111:2222:3333:4444::/48, then the termination with remote address A in the other pinhole also has an rsam of 1111:2222:3333:4444::/48.

## Restrictions for DBE No NAPT Pinholes

The following are DBE restrictions pertaining to the No NAPT Pinholes feature:

- The DBE chooses the internal terminations as follows:
  - The first specified termination is chosen to be internal.

  - The other termination is chosen accordingly from the other pinhole. If the termination with remote address A on one pinhole is internal, then the termination with local address A on the other pinhole is also internal.
  - The DBE does not support choosing internal terminations based on termination names.
- For No NAPT coupled pairs, any Network Address Translation (NAT) latching requests are duplicated. For example, if a termination with remote address A in one pinhole requests NAT latching, then the termination with remote address A in the other pinhole must also request NAT latching. The "request NAT latching" can be done using the ipnapt/latch H.248 signal.
- A hairpin of two pinholes in which both external terminations are provisioned with the NAT latching instruction cannot latch and cannot forward media. No NAPT pinholes are not allowed to (re)latch to the remote addresses on both sides.
- IPv6 hairpinning are supported on UDP and TCP.
- Coupling of Single NAPT pinholes is not supported.

# INDEX