

SBC on the Cisco 7600 Series Router

This chapter provides information about SBC on the Cisco 7600 series router and contains the following sections:

- [SBC Deployment on the Cisco 7600 Series Router, page 1-1](#)
- [SBC Features on the Cisco 7600 Series Router, page 1-3](#)
- [Supported MIBs, page 1-14](#)

SBC Deployment on the Cisco 7600 Series Router

The Session Border Controller (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 voice over IP (VoIP) device that sits on the border of a network and controls call admission to that network.

The SBC protects the interior of the network from excessive call load and malicious traffic. Additional functions provided by the SBC include media bridging and billing services.

The SBC is available as a service in the Cisco 7600 series router and is implemented on a service card.

For ACE SBC Release 3.0.00 or later, the SBC application runs on an Application Control Engine (ACE) module. (See [ACE Configuration Prerequisites for the SBC](#) for more details.)

The SBC service includes two functional areas:

- **Signaling SBC function**—Managed by the signaling border element (SBE), controls access of VoIP signaling messages to the core of the network, and manipulates the contents of these messages. It does this by acting as a Session Initiation Protocol (SIP) back-to-back user agent (B2BUA) or H.323 gateway.
- **Media SBC function**—Managed by 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. It does this by acting as a real-time transport protocol (RTP) proxy.

For ACE SBC Release 3.0.00 or later, the SBC can operate in two modes or deployment models, as follows:

- **Unified**—In the unified model, both the SBE and DBE logical entities co-exist on the same network element. In this model, the signaling entity controls the media local to the router and to a single service card (the Application Control Engine [ACE]).

- **Distributed**—In the distributed model, the SBE and the DBE entities reside on different network elements. Logically, each of the SBE entities controls multiple DBE elements, and each DBE could be controlled by multiple SBE entities. The SBE interacts with the DBE entities using a session controller interface (SCI). The SCI interface supports the H.248 protocol.

In this model, the bearer always flows through the DBE, and the SBE participates only in the signaling flow. This model must be used in conjunction with a third-party SBE that supports the DBE H.248 profile.

**Note**

For ACE SBC Release 3.0.00 or later, in the distributed model, the SBC can only function as an DBE; it cannot function as an SBE.

Figure 1 illustrates the unified mode. Figure 2 illustrates the relationships between SBEs, DBEs, and other network elements.

Figure 1 Relationships Between SBEs/DBEs and Other Network Elements in the Unified Model

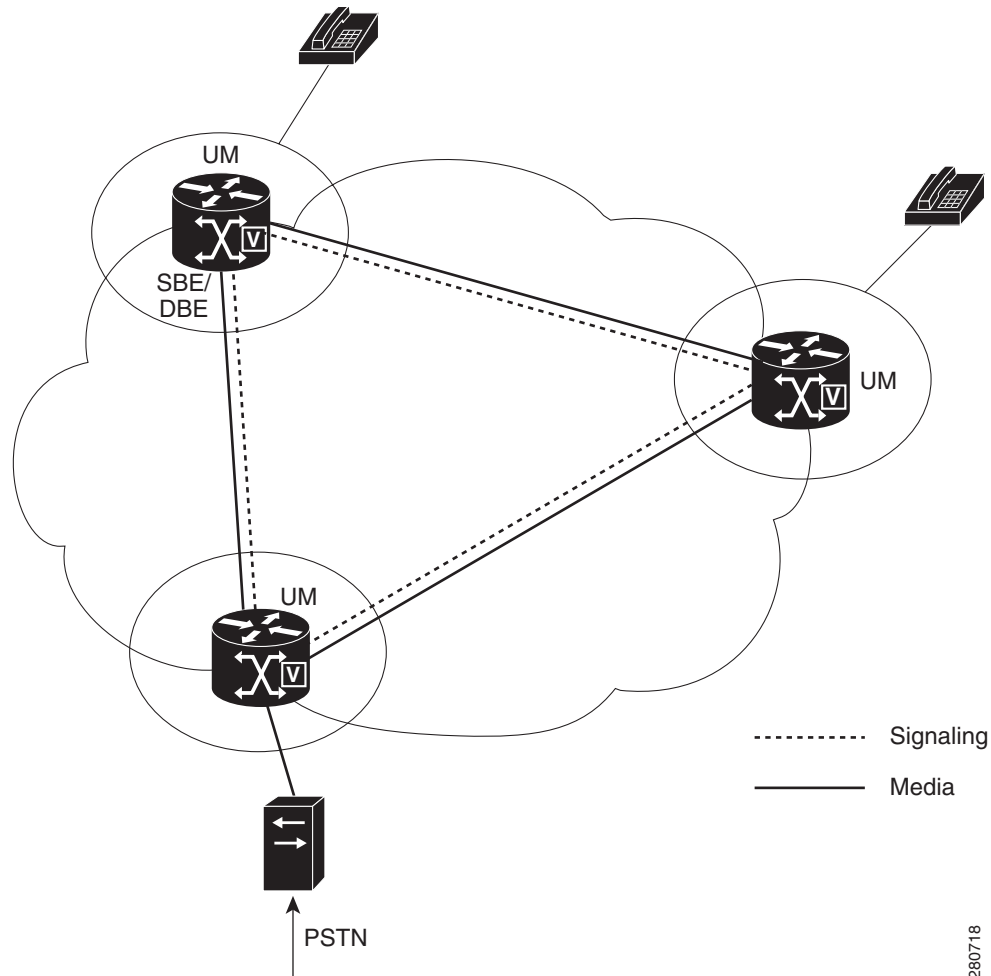
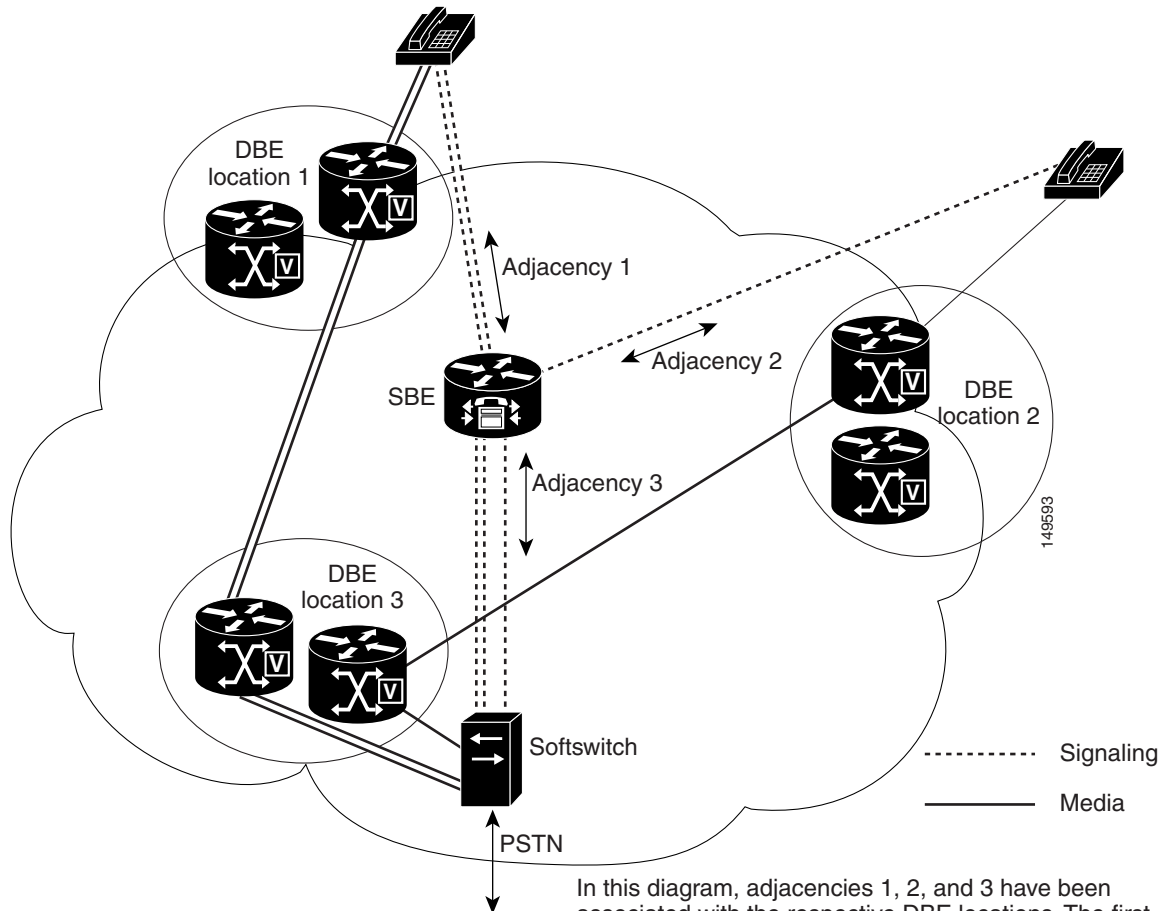


Figure 2 Relationships Between SBEs/DBEs and Other Network Elements in the Distributed Model



Note

ACE SBC Release 3.0.00 or later supports only one virtual data border element (vDBE).

SBC Features on the Cisco 7600 Series Router

The Cisco 7600 series routers supports the following SBC features:

- [Network Address and Port Translation and NAT/FW Traversal, page 1-5](#)
- [SBC QoS—Marking, page 1-5](#)
- [DoS Prevention, page 1-6](#)
- [SBC Interworking Dual Tone Multifrequency, page 1-6](#)
- [Unexpected Source Address Alerting, page 1-6](#)

- SBC Redundancy—High Availability, page 1-6
- DBE Overload Reporting, page 1-7
- Media Address Pools, page 1-7
- FAX Support, page 1-7
- SBC Multi-VRF, page 1-7
- SBC Adjacencies, page 1-7
- SBC Billing, page 1-8
- SBC Policies, page 1-8
- SBC Transcoding, page 1-8
- SBC Firewall Traversal and Network Address Translator, page 1-8
- SIP Method Profiles, page 1-8
- Header Profiles, page 1-9
- Restricting Codecs, page 1-9
- SIP Tel URI Support, page 1-9
- SIP Timer, page 1-9
- H.323 Support, page 1-9
- H.323-SIP Interworking, page 1-9
- Tracking Policy Failure Statistics, page 1-9
- SIP 3xx Redirect Responses, page 1-10
- SIP Call Hold, page 1-10
- SIP Call Transfer, page 1-10
- SIP Outbound Authentication, page 1-10
- SIP Inbound Authentication, page 1-10
- SIP-I Transparency and Profile Support, page 1-10
- SIP Configuration Flexibility, page 1-11
- Implementing SBC QoS (Marking), page 1-11
- DoS Prevention and Dynamic Blacklisting, page 1-11
- Early Media, page 1-11
- P-CSCF Support, page 1-11
- Integration of Resource Management and SIP, page 1-11
- IBCF Processing Support, page 1-11
- SDP Attribute Passthrough, page 1-12
- DBE Signaling Pinhole, page 1-12
- Late-to-Early Media Internetworking, page 1-12
- Secure Media Passthrough, page 1-12
- VRF-Aware DNS Query, page 1-12
- CAC Rate Limiting, page 1-12
- Subscriber Policy, page 1-12

- [Support for Media Information, page 1-12](#)
- [SIP PING Message Support, page 1-13](#)
- [P-KT-UE-IP Feature, page 1-13](#)
- [Routing Features, page 1-13](#)
- [H.323 Performance Improvement, page 1-13](#)
- [SIP Header Manipulation, page 1-13](#)
- [SIP Statistics Per Adjacency, page 1-13](#)
- [SDP Call Hold Interworking, page 1-13](#)
- [Response Code Mapping, page 1-14](#)
- [Provisional Response Filtering, page 1-14](#)
- [Parameter Profiles, page 1-14](#)
- [Codec Ordering, page 1-14](#)
- [Improved Fast Register, page 1-14](#)
- [Interchassis Redundancy, page 1-14](#)

Network Address and Port Translation and NAT/FW Traversal

The DBE performs translation of IP addresses and port numbers (through Network Address and Port Translation, or NAT) in both directions and Network Address Translation (NAT) Traversal functions.

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

SBC QoS—Marking

The DBE supports statistics collections and re-marking of differentiated services code point (DSCP) bits for egress traffic and media relay.

QoS Statistics Collections

The DBE saves all QoS statistics including packets transmitted/second and packets dropped for exceeding allocated bandwidth on a per-call or per-interface basis. These statistics are available to the control CPU using IPCP.

DSCP Remarkings

For each media-stream, the DBE receives a DSCP (differentiated services code point) value to use in the RTP/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 each outgoing packet and update the checksum accordingly.

DoS Prevention

The Media Packet Forwarder (MPF) component for the SBC running on the Cisco 7600 series router controls DoS prevention.

Traffic sent to spurious addresses is managed by the ingress line card and never reaches MPF.

Spoofed traffic sent to media addresses:

- Usually fails flow classification. This traffic is sent to the IP stack with severe rate limiting.
- May pass flow classification. If so, this traffic is forwarded in the media flow, but it is limited according to the flow spec for the flow. Spoofed traffic sent to the H.248 address and port is passed to the DBE without rate limiting and, hence, could cause undesirable effects because no authentication is carried out on this traffic.

Because of this, you expect that the address used by H.248 is only be reachable from within the trusted network between the DBE and other SBC components. We recommend a setup of a separate (SBC) interface whose address is only reachable from the private network. Use this setup exclusively for H.248 traffic.

MPF applies a single rate limit of 10 packets per second to all traffic punted to the IP stack. However, there should be no legitimate traffic being sent to the DBE media addresses that needs punting other than the occasional ICMP ping. Hence, this rate limit should not affect any real traffic.

The MPF is only able to protect traffic addressed to one of the SBC Interface addresses. Rogue traffic sent to other local addresses on the Cisco 7600 router must be policed by other Cisco IOS mechanisms.

SBC Interworking Dual Tone Multifrequency

The SBC automatically selects the best dual tone multifrequency (DTMF) signaling technique based on the capabilities of the endpoints in a call. DTMF interworking is employed only if the caller and callee support non-overlapping DTMF event mechanisms (for example, if the caller supports sending DTMF using the SIP INFO method only and the callee supports receiving DTMF using in-channel RFC 2833 RTP signaling only).

For more details, see [Chapter 4, “Implementing SBC Interworking DTMF.”](#)

Unexpected Source Address Alerting

The SBC provides alerts for any unexpected source addresses that are received. After an unexpected source address is received, a log is created and an SNMP trap is generated.

For more details, see [Chapter 5, “Unexpected Source Address Alerting.”](#)

SBC Redundancy—High Availability

The SBC fault tolerance is based on a 1:1 paired-protection model. For each service card running active SBC components, there can be one service card providing failure protection. The same services must be provisioned on both cards (one as the primary card, one as the standby card), and the service cards are then said to be paired. Although from a Cisco 7600 series router perspective, service cards are always running in active mode, SBC services running on these cards run as either the primary service or the standby service.

For more details, see [Chapter 6, “Implementing SBC Redundancy—High Availability.”](#)

DBE Overload Reporting

The SBC provides detailed reporting of the DBE overload conditions.

For more details, see [Chapter 7, “Configuring Data Border Element Overload Reporting.”](#)

Media Address Pools

The SBC provides you with the ability to configure the SBC using a single media address or a range of 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 DBE address by address pool with or without port range, and define CoS affinity for each port range.

For more information, see [Chapter 8, “Media Address Pools.”](#)

FAX Support

The SBC supports different types of fax over IP calls, using either SIP or H.323.

For more information, see [Chapter 9, “Fax Support.”](#)

SBC Multi-VRF

The SBC support for multi-VRF (virtual "virtual routing and forwarding" routing and forwarding) on customer edge (CE) devices (that is, customer premise routers) feature provides the capability of suppressing provider edge (PE) checks that act to prevent loops when the PE is performing a mutual redistribution of packets. Multi-VRF:

- Allows for the use of only one router to accomplish the tasks that multiple routers usually perform.
- Runs on a network without the requirement of Multiprotocol Label Switching (MPLS) and Border Gateway Protocol (BGP) installed.

For more details, see [Chapter 10, “Implementing SBC Multi-VRF.”](#)

SBC Adjacencies

Accounts and adjacencies are the key objects used to control signaling. An account represents a service relationship with a remote organization on the SBE with which the SBC interacts. Within each account, one or more signaling adjacencies must be defined to connect the SBC to devices within that organization.

An adjacency represents a signaling relationship with a remote call agent. There is one adjacency defined per external call agent. The adjacency is used to define protocol-specific parameters as well as admission control and routing policy. Each adjacency belongs within an account. Each incoming call is matched to an adjacency, and each outgoing call is routed out over a second adjacency.

For more details, see [Chapter 11, “Implementing SBC Adjacencies”](#).

SBC Billing

The SBC billing component includes the following core features:

- Compatibility with existing billing systems—SBC billing fits seamlessly into a provider’s existing billing architecture, using existing mechanisms to obtain billing information similar to existing solutions.
- Integration with next-generation technologies and solutions—The SBC employs next-generation billing technologies so that service information from SBC, softswitches, voicemail, and unified messaging applications can be collated and billed in a distributed environment.

The function of the billing component can be broadly divided into two modes:

- Standalone, record-based call logging.
- Third-party integrated, distributed RADIUS-based call and event logging.

For more details, see [Chapter 12, “Implementing SBC Billing”](#).

SBC Policies

An SBC policy is a set of rules configured on the SBE that defines how different kinds of VoIP events are treated by the SBC. An SBC policy allows the user to control the VoIP signaling and media that passes through the SBC at an application level.

For more details, see [Chapter 13, “Implementing SBC Policies”](#).

SBC Transcoding

Transcoding is the process of translating a media stream encoded using one codec into a media stream encoded using another codec. For example, translating a media stream encoded as pulse code modulation u-law (PCMU) into one encoded as ITU-T G.726-32.

For more details, see [Chapter 14, “Implementing SBC Transcoding”](#).

SBC Firewall Traversal and Network Address Translator

The SBC enables VoIP signaling and media to be received from and directed to a device behind a firewall and NAT (network address translator) at the border of an adjacent network, without requiring the device or firewall to be upgraded. In brief, the SBC achieves this by rewriting the IP addresses and ports in the call signaling headers and the SDP blocks attached to these messages. SBC does not support options for keeping pinholes open. Instead, SBC registers messages for signaling pinhole maintenance and RTP packets for media.

For more details, see [Chapter 15, “Implementing SBC Firewall Traversal and NAT”](#).

SIP Method Profiles

SIP method profiles are used to control which SIP requests are accepted (whitelists) and which requests are rejected (blacklists) based on the method of the request.

For more details, see [Chapter 16, “SIP Profiles on the Session Border Controller”](#).

Header Profiles

Header profiles are used to control which headers are passed through (whitelists) and which headers are discarded (blacklists) on SIP messages.

For more details, see [Chapter 16, “SIP Profiles on the Session Border Controller”](#).

Restricting Codecs

The SBC is hard-coded with a set of recognized codecs including all commonly used voice and video codecs.

For more details, see [Chapter 17, “Restricting Codecs”](#).

SIP Tel URI Support

The SBC supports Tel Uniform Resource Identifier (tel URI) in SIP messages, permitting call set up from a SIP IP-phone or SIP User Agent Application to an endpoint in the Public Switched Telephone Network (PSTN).

For more details, see [Chapter 18, “SIP Tel URI Support”](#).

SIP Timer

The SIP Timer feature configures a number of SIP timers.

For more details, see [Chapter 19, “SIP Timer”](#).

H.323 Support

H.323 allows multimedia products and applications from multiple vendors to interoperate and communicate without concern for compatibility.

For more details, see [Chapter 20, “H.323 Support”](#).

H.323-SIP Interworking

The H.323-SIP interworking feature allows interworking between SIP and H.323 for Voice over IP (VoIP) service providers.

For more details, see [Chapter 21, “H.323-SIP Interworking”](#).

Tracking Policy Failure Statistics

The tracking policy failure statistics feature tracks the number of calls that the SBC rejected based on the rules established in the number analysis policies, routing policies, or Call Admission Control (CAC) policies.

For more details, see [Chapter 22, “Tracking Policy Failure Statistics”](#).

SIP 3xx Redirect Responses

The SIP 3xx redirect response feature configures the SBC to process SIP 3xx responses.

For more details, see [Chapter 23, “SIP 3xx Redirect Responses”](#).

SIP Call Hold

The SIP call hold feature provides a standard telephony service of putting a caller on hold.

For more details, see [Chapter 24, “SIP Call Hold”](#).

SDP Call Hold Interworking

The SDP call hold interworking provides two ways of setting up call hold using SIP.

For more details, see [Chapter 24, “SIP Call Hold”](#).

SIP Call Transfer

The SIP call transfer feature allows a wide variety of decentralized multiparty call operations.

For more details, see [Chapter 25, “SIP Call Transfer”](#).

SIP Outbound Authentication

The SIP outbound authentication feature allows network entities that communicate using SIP to challenge one another to determine if authorization exists to transmit SIP signaling into the challenger's network.

For more details, see [Chapter 26, “SIP Outbound Authentication”](#).

SIP Inbound Authentication

The SIP inbound authentication feature provides two modes (local and remote) of SIP inbound authentication to challenge inbound SIP requests.

For more details, see [Chapter 27, “SIP Inbound Authentication”](#).

SIP-I Transparency and Profile Support

This feature enables the SBC to pass through the ISDN User Part (ISUP) parameters in SIP messages that may have been added by a SIP or Public Switched Telephone Network (PSTN) interworking gateway.

For more details, see [Chapter 30, “SIP-I Transparency and Profile Support”](#).

SIP Configuration Flexibility

This feature offers flexibility when configuring different features of a SIP adjacency.

For more details, see [Chapter 29, “SIP Configuration Flexibility”](#).

Implementing SBC QoS (Marking)

This feature provides quality of service (QoS) profiles that the integrator configures for IP packet marking on the data path.

For more details, see [Chapter 28, “Implementing SBC QoS \(Marking\)”](#).

DoS Prevention and Dynamic Blacklisting

The denial of service (DoS) prevention and dynamic blacklisting feature blocks malicious endpoints from attacking the network.

For more details, see [Chapter 31, “DoS Prevention and Dynamic Blacklisting”](#).

Early Media

The early media feature allows two user agents to communicate before a call is actually established.

For more details, see [Chapter 32, “Early Media”](#).

P-CSCF Support

The P-CSCF functions as a proxy server for the user equipment; all SIP signaling traffic to and from the user equipment must go through the P-CSCF.

For more details, see [Chapter 35, “P-CSCF Support.”](#)

Integration of Resource Management and SIP

This feature allows call endpoints to determine whether resources are fully reserved for a media stream before using it.

For more details, see [Chapter 36, “Integration of Resource Management and SIP”](#).

IBCF Processing Support

This feature allows the SBC to perform the role of an Interconnection Border Control Function (IBCF) Session Initiation Protocol (SIP) border gateway, both managing requests across a network border between IP Multimedia Subsystem (IMS) core networks and interworking with non-IMS core networks, such as H.323 networks.

For more details, see [Chapter 37, “IBCF Processing Support.”](#)

SDP Attribute Passthrough

The SDP attribute passthrough feature allows the user to change or add certain kinds of attribute lines. For more details, see [Chapter 38, “Configuring SIP SDP Attribute Passthrough.”](#)

DBE Signaling Pinhole

The DBE signaling pinhole feature allows the user to configure a media address pool for signaling pinholes to allow the DBE to forward signaling packets to the SBE. For more details, see [Chapter 8, “Media Address Pools.”](#)

Late-to-Early Media Internetworking

The late-to-early media internetworking feature supports interworking on a per-adjacency basis between late and early media. For more details, see [Chapter 33, “Late-to-Early Media Internetworking.”](#)

Secure Media Passthrough

The secure media passthrough feature allows the SBC to reserve additional bandwidth to ensure that the DBE will allow secure media packets to pass through. For more details, see [Chapter 34, “Secure Media Passthrough.”](#)

VRF-Aware DNS Query

This feature allows allows DNS queries to be performed on a per-context basis. For more details, see [Chapter 10, “Implementing SBC Multi-VRF.”](#)

CAC Rate Limiting

The CAC Rate Limiting feature provides for rate limiting all in-call and out-of-call messages. For more details, see [Chapter 13, “Implementing SBC Policies.”](#)

Subscriber Policy

This feature provides the ability to configure the CAC limits. For more details, see [Chapter 13, “Implementing SBC Policies.”](#)

Support for Media Information

This adds support for media information to billing messages.

For more information, see [Chapter 12, “Implementing SBC Billing.”](#)

SIP PING Message Support

Release 3.1.0 adds support for SIP PING messages defined in the IETF draft Midcom-unaware NAT/Firewall Traversal.

For more information, see [Chapter 15, “Implementing SBC Firewall Traversal and NAT.”](#)

P-KT-UE-IP Feature

Release 3.1.0 provides support for P-KT-UE-IP headers. These headers are a type of P-headers used for a variety of purposes within the networks, including charging and information about the networks a call traverses.

For more information, see [Chapter 16, “SIP Profiles on the Session Border Controller.”](#)

Routing Features

Release 3.1.0 provides support for additional routing features including routing by category, source number manipulation, least cost routing, weighted routing, time-based routing, and regular expression routing.

For more details, see [Chapter 13, “Implementing SBC Policies.”](#)

H.323 Performance Improvement

Release 3.1.0 provides support for H.323 performance improvement.

For more details, see [Chapter 20, “H.323 Support.”](#)

SIP Header Manipulation

Release 3.1.0 provides support for SIP Header Manipulation.

For more information, see [Chapter 16, “SIP Profiles on the Session Border Controller.”](#)

SIP Statistics Per Adjacency

Release 3.1.0 provides support for SIP Statistics per adjacency. This feature allows you to configure the collection of SIP message statistics at the level of adjacencies.

For more details, see [Chapter 11, “Implementing SBC Adjacencies.”](#)

SDP Call Hold Interworking

Release 3.1.0 provides support for SDP call hold interworking. This feature provides two ways for setting up call hold using SIP.

For more details, see [Chapter 24, “SIP Call Hold.”](#)

Response Code Mapping

Release 3.1.0 provides support for Response code mapping. This feature provides an ability to manipulate the SIP response codes when the messages traverse through the SBC.

For more information, see [Chapter 16, “SIP Profiles on the Session Border Controller.”](#)

Provisional Response Filtering

Release 3.1.0 provides support for provisional response filtering. Provisional response filtering makes it possible to block 183 responses sent by endpoints.

For more information, see [Chapter 16, “SIP Profiles on the Session Border Controller.”](#)

Parameter Profiles

Release 3.1.0 provides support for parameter profiles.

For more information, see [Chapter 16, “SIP Profiles on the Session Border Controller.”](#)

Codec Ordering

Release 3.1.0 provides support for codec ordering.

For more details, see [Chapter 17, “Restricting Codecs.”](#)

Improved Fast Register

Release 3.1.0 provides support for improved fast register.

For more details, see [Chapter 11, “Implementing SBC Adjacencies.”](#)

Interchassis Redundancy

Release 3.1.0 provides support for interchassis redundancy.

For more details, see [Chapter 6, “Implementing SBC Redundancy—High Availability”](#)

Supported MIBs

The following MIBs are supported in ACE SBC Release 2.0.00 and later for the SBC on the Cisco 7600 series router:

- CISCO-STACK-MIB
- ENTITY-MIB

- CISCO-SESSION-BORDER-CONTROLLER-EVENT-MIB
- CISCO-SESSION-BORDER-CONTROLLER-CALL-STATS-MIB

For more information about MIB support on a Cisco 7600 series router, refer to the *Cisco 7600 Series Internet Router MIB Specifications Guide* at:

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_technical_reference_list.html

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at:

<http://www.cisco.com/register>

