

Cisco 7600 Series Session Border Controller

The Cisco® 7600 Series Session Border Controller (SBC) builds on the continuous system operation and multimedia scalability provided by the market-leading Cisco 7600 Series Routers. With the integration of SBC functions into Layer 2 and Layer 3 services provided by the Cisco 7600 Series, the Cisco 7600 SBC eliminates the need for overlay networks and standalone appliances. It provides an open and flexible architecture for all service provider deployments, whether for peering with other service providers or for direct end-customer access. With its ability to support unified and distributed SBC deployments, the Cisco 7600 SBC offers cable, wireline, and wireless service providers superior deployment flexibility. By supporting IP Multimedia Subsystem (IMS) and non-IMS services, the Cisco 7600 SBC further accelerates network convergence while providing investment protection for Cisco 7600 Series Routers.

Product and Application Overview

SBCs control and manage real-time multimedia traffic flows between IP network borders, handling signaling, data, voice, and video traffic. As part of this function, the SBC performs native IP interconnection functions required for real-time communications such as access control, firewall traversal, bandwidth policing, accounting, signaling interworking, legal intercept, and quality-of-service (QoS) management. With its comprehensive suite of features, the Cisco 7600 Series Routers can accommodate a broad range of SBC applications.

The Cisco 7600 SBC solution incorporates the security, QoS, and secure virtualization capabilities of the Cisco 7600 Series Router to facilitate support for service provider-to-service provider (Network-to-Network Interface [NNI]) interconnect and service provider-to-access layer (User-to-Network Interface [UNI]) interconnect for data, voice over IP (VoIP), and video services.

The Cisco 7600 SBC solution takes advantage of the advanced hardware-processing capabilities of the Cisco Application Control Engine (ACE) hardware to provide a flexible, scalable, and feature-rich SBC implementation (Figure 1).

Figure 1. Cisco 7600 SBC Module



Service Provider-to-Service Provider Interconnect

With the increasing deployment of end-to-end VoIP and IP video services, service providers are looking to interconnect directly with IP networks and minimize time-division multiplexing (TDM)-based handoffs to other service provider networks. Direct IP interconnect helps minimize operating expenses (OpEx) and capital expenditures (CapEx) by eliminating back-to-back TDM gateways. It also increases media quality and helps ensure transparency of IP-based services across network borders. The Cisco 7600 SBC provides the following critical functions required for direct IP interconnect without introducing any additional network elements:

- Protocol and media interworking
- Session routing
- Call Admission Control (CAC) and policing
- Quality monitoring and enforcement
- Media and signaling security and Network Address Translation (NAT) mechanisms
- Authentication, authorization, and accounting (AAA)
- Media transcoding with an external media server

Service Provider-to-Access Interconnect

With the rapid growth of IP telephony and other real-time services such as IP video, service providers are deploying SBC appliances at the provider edge to manage VoIP traffic in different scenarios. These scenarios include IP private branch exchange (PBX)-to-service provider peering, VPN interworking with multiple sites for the same customer and multiple customers, enterprise-to-hosted IP telephony interworking, and residential IP telephony. The Cisco 7600 SBC builds on Cisco Layer 2 and Layer 3 services and integrates the SBC function by providing the following features:

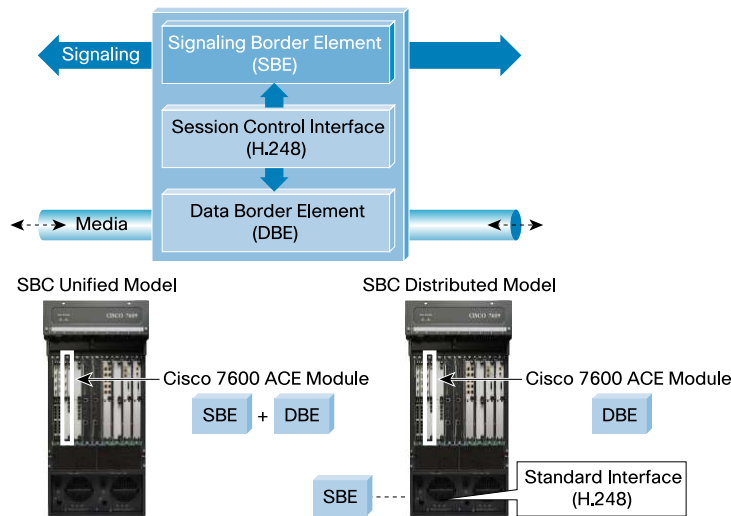
- Protocol and media interworking
- Session routing
- Hosted NAT and firewall traversal
- Security and AAA
- Intra-and inter-VPN interconnect and optimization
- Media transcoding with an external media server

SBC Deployment Models

For both the service provider-to-service provider and service provider-to-access applications, the innovative architecture of the Cisco 7600 SBC gives operators a choice of a unified or distributed signaling deployment.

In the unified deployment model, the Cisco 7600 SBC acts as both a Data Border Element (DBE) for media-related functions and as a Signaling Border Element (SBE) for signaling-related functions. In the distributed deployment model, the Cisco 7600 SBC as a DBE hosts the media-related functions and communicates with an external signaling function (SBE) over an industry-standard interface based on the H.248 Protocol. The flexibility of the Cisco SBC design allows for either deployment model using the same hardware and software (Figure 2).

Figure 2. SBC Deployment Models



Product Highlights

- High performance and scalability: With 10 Gbps per slot of processing capacity for each Cisco ACE 7600 Application Control Engine Module, the Cisco 7600 SBC can scale to more than 200,000 simultaneous sessions on a single chassis. With its high-throughput interface into the Cisco 7600 switching fabric, the SBC is designed not only to scale for VoIP sessions but also to support high-bandwidth video sessions such as TelePresence.
- Industry-standard protocols and interfaces: The Cisco 7600 SBC incorporates support for industry-standard protocols for VoIP and video, including Session Initiation Protocol (SIP) and H.323. The Cisco 7600 SBC offers broad support for various SIP- and H.323-based services. In addition, the Cisco 7600 SBC supports the Telecoms and Internet Converged Services and Protocols for Advanced Networks (TISPAN) Ia interface, which is based on the H.248 Protocol and enables a distributed implementation of SBC signaling and media flow.
- Maximum flexibility: The native implementation of SBC functions on the Cisco 7600 Series Router provides a host of additional capabilities that are not possible with standalone SBC appliances. Service providers can now combine Layer 2 and Layer 3 services offered with the SBC solution to not only derive the benefits of network convergence but also to add other unique services. Operators can apply SBC functions at a more granular VPN level, and can combine business VPN services with business voice and video services. Similarly, operators can combine network-based security services such as IP Security (IPsec) and firewall with SBC functions. These new features have anticipated the array of new applications possible with converged networks.

Table 1 lists the features of the Cisco SBC on the Cisco 7600 Series Router, Table 2 lists information about compliance to industry standards and specifications, and Table 3 gives hardware specifications.

Table 1. Features Summary

Feature	Description
Flexible deployment models	<ul style="list-style-type: none"> • Unified deployment model: Signaling and media functions are hosted on the Cisco ACE 7600 Module. • Distributed deployment model: Media functions are hosted on the Cisco 7600 ACE Module, with a service control interface based on the TISPAN Ia interface (H.248) provided (supported by the Cisco PGW 2200 Softswitch functioning as a SBE).
Redundancy and high availability	<ul style="list-style-type: none"> • Support for 1:1 active/standby model intra- and interchassis • Support for hot standby (stable calls are maintained on failover) • Same alias IP address for both active and standby SBC

VPN interconnect and optimization	<ul style="list-style-type: none"> • Through Layer 3 VPN awareness, support for interconnect and security for sessions between two different VPNs with overlapping addresses • Optimized media flow for sessions on the same VPN • Virtual Route Forwarding (VRF)-aware Domain Name System (DNS) query
Number analysis	<ul style="list-style-type: none"> • Caller and callee number analysis and manipulation • Call categorization based on caller and callee numbers
Session routing	<ul style="list-style-type: none"> • Fully configurable session routing engine integrated into the SBC • Routing by category • Least-cost and weighed routing • Time-based routing • Routing based on source and destination username and domain-name matching using regular expression
Admission control	<ul style="list-style-type: none"> • Comprehensive set of functions for admission control • CAC per session, per endpoint, per dialed number, per peer or adjacency, and per VPN to control maximum concurrent sessions, maximum bandwidth, maximum call-setup rate, and codec restrictions • Rate-limit endpoint-initiated in-call and out-of-call signaling messages • Call limiting per subscriber IP address or account • Call prioritization (Example: Emergency calls)
QoS	<ul style="list-style-type: none"> • QoS and differentiated services code point (DSCP) remarking for signaling and media packets • Collection of QoS statistics (packets transmitted, dropped, etc.)
Protocol support	<ul style="list-style-type: none"> • Broad support for various SIP-based services (RFCs 3261, 3262, 2976, 3311, and 3326) and Session Description Protocol (SDP) • ITU-T H.323 (Fast Start, Slow Start, Gatekeeper, carrier ID-based routing, Q.SIG and H.450 tunneling, and Tech Prefixes) • IMS profiles • H.248/Megaco • Voice codecs (G.711, G.723, G.729, and more), and dual tone multifrequency (DTMF) (Inband, RFC 2833, SIP Info, SIP Notify, and H.245 alphanumeric), fax (Inband and T.38), and video codecs (H.263, H.264, and more)
SIP features	<ul style="list-style-type: none"> • Support for call hold and call transfer (REFER) • Support for redirection (300 response in SIP) • Peer availability detection (OPTION ping) • Support for SUBSCRIBE/NOTIFY pass-through • Support for upstream and downstream call forking • Support for P-KT-UE-IP headers • Support for SIP PING messages defined in the IETF draft midcom-unaware NAT and firewall traversal
SIP registration	<ul style="list-style-type: none"> • SIP registration forwarding to registrar specified in address of record (AOR) • Registration shielding from softswitch (fast register) • Fast registration (to keep NAT and firewall pinhole open) • Rewrite registration (rewrite request uniform resource identifier [URI] and AOR before forwarding) • Delegated registration (register with registrar on behalf of client) • Aggregate registration (receiving aggregated REGISTER message from IP private branch exchange [PBX])
SIP header and parameter manipulation	<ul style="list-style-type: none"> • SIP method filtering (black-list and white-list) • SIP header insertion, deletion, and manipulation • SIP parameter insertion, deletion, and manipulation
Topology hiding and privacy	<ul style="list-style-type: none"> • Functioning as SIP Back to Back User Agent, hiding signaling and media IP address from one side to another • Removing diversion header • Rewriting From header in outbound messages to remove any display name and replacing the user part of the From URI with "anonymous" • Changing the SIP Call-ID, From tag, and To tags for the call • Changing the SIP Contact header • Rewriting the SDP to reroute media through the SBC
IMS and non-IMS models	<ul style="list-style-type: none"> • Support for ETSI/TISPAN IMS (Proxy-Call Session Control Function [P-CSCF], Interfacing Border Control Function [IBCF], Interworking Function [IWF], Service Policy Decision Function [SPDF], and Interconnect Border Gateway Function [I-BGF] functions) and non-IMS networks
H.323 features	<ul style="list-style-type: none"> • Fast Start, Slow Start, carrier ID-based routing, and Tech Prefixes • Fast-Start to Slow-Start interworking • Gatekeeper discovery, registration, admission authentication, alternate endpoints, bandwidth reporting, information request, and request-in-progress message • Empty Terminal Capability Set (call hold and media renegotiation) • H.245 tunneling

Hosted NAT and firewall traversal	<ul style="list-style-type: none"> • Support for all NAT, Port Address Translation (PAT), and firewall-traversal schemes • Forwarding and filtering signaling packets from DBE to SBE (DBE signaling pinhole) in distributed model
Authentication, encryption, and security	<ul style="list-style-type: none"> • Software and hardware support for VoIP-specific malicious attacks that complements the security features of Cisco 7600 Series Routers • Denial-of-service (DoS) and distributed DoS (DDoS) prevention • Outbound message flood prevention (limit rate of outgoing requests) • Support for endpoint authentication by passing authentication messages to a third-party (RADIUS) server using digest authentication • Support for the termination of IPsec and Transport Layer Security (TLS)-encrypted signaling arriving at the SBC
Signaling and media Interworking	<ul style="list-style-type: none"> • Support for SIP-to-H.323 interworking • H.245-to-SDP interworking (codecs PCMU, PCMA, G.722, G.723, G.728, G.729A, G.729B, GSM, and T38) • IMS-to-non IMS network • SIP provisional response filtering • Call hold interworking • Support for native DTMF interworking (RFC 2833 to SIP Info) and the ability to route • SDP attribute white list, black list, and pass-through in offer and answer messages • Late-to-early media interworking for SIP calls • SIP response code mapping • SIP header and parameter manipulation • Support for transcoding (ability to route media to external media servers for transcoding) • Secure media pass-through for Secure Real-Time Transport Protocol (SRTP), Secure Real-Time Transport Control Protocol (SRTCP), and Datagram Transport Layer Security (DTLS) packets
Billing records	<ul style="list-style-type: none"> • Detailed session detail records with RADIUS-based billing records • Media QoS statistics reporting • Enhanced media information such as local IP address or port, remote IP address or port, media stream direction (send-only, receive-only, send-receive, and inactive), negotiated codec, bandwidth used, etc.
Management and operations	<ul style="list-style-type: none"> • Cisco Command Line Interface (CLI) • SNMP traps and call and media statistics • Memory statistics, call-rate statistics, resource monitoring, display active calls list, display specific call detail, call statistics, SIP statistics (global and per adjacency), media statistics, policy failure statistics, and DBE overload reporting

Table 2. Compliance to Industry Standards and Specifications

Feature	Description
SIP: IETF	<ul style="list-style-type: none"> • Session Initiation Protocol v2 (RFC 3261) • Reliability of Provisional Responses in SIP (RFC 3262) • HTTP Basic and Digest Access Authentication (RFC 2617) • SIP INFO Method (RFC 2976) • Control of Service Context Using SIP URI (RFC 3087) • MIME Media Types for ISUP and QSIG Objects (RFC 3204): Pass-through • SIP Update Method (RFC 3311) • Integration of Resource Management and SIP (RFC 3312) • Private SIP Extensions for Media Authorization (RFC 3313): Pass-through • A Privacy Mechanism for SIP (RFC 3323): Pass-through • Short-Term Requirements for Network Asserted Identity (RFC 3324) • Private Extensions to SIP Asserted-Identity within Trusted Network (RFC 3325): Pass-through • Reason Header Field for SIP (RFC 3326): Pass-through • SIP Extension for Registering Non-Adjacent Contacts (RFC 3327): Pass-through • Security Mechanism Agreement for SIP (RFC 3329): Partial (ipsec-3gpp security mechanism only) • User Requirements for SIP in Support of TDD (RFC 3351) • DHCP (DHCP-for-IPv4) Option for SIP (RFC 3361) • Internet Media Type message/sipfrag (RFC 3420): Partial • SIP Extension for Instant Messaging (RFC 3324): Pass-through • SIP Refer Method (RFC 3515) • Extension to SIP for Symmetric Response Routing (RFC 3581) • SIP Extension Header Field for Service Route Discovery During Registration (RFC 3608): Pass-through • SIP Basic Call Flow Examples (RFC 3665) • SIP Event Package for Registrations (RFC 3680): Pass-through • Best Current Practices for Third-Party Call Control in the SIP (RFC 3725) • Caller Preferences for the SIP (RFC 3841) • A Message Summary and Message Waiting Indication Event Package SIP (RFC 3842) • S/MIME AES Requirement for SIP (RFC 3853) • SIP "Replaces" Header (RFC 3891) • The SIP Referred-By Mechanism (RFC 3892): Partial (no support for AIB body, cid Referred-by Pass-through) • An Event State Publication Extension to SIP (RFC 3903): Pass-through • SIP "Join" Header (RFC 3911): Pass-through • Early Media and Ringing Tone Generation in SIP (RFC 3960): Partial (Gateway model only) • Session Timers in the SIP (RFC 4028): Pass-through • Transcoding Services Invocation in the SIP (RFC 4117): Not using third-party call control [3PCC], alternate method • Communications Resource Priority for SIP (RFC 4412): Partial (Accept-Resource-priority pass-through only) • Requirements for Consent-Based Communications in SIP (RFC 4453) • A Mechanism for Content Indirection in SIP messages (RFC 4483) • draft-ietf-sip-cc-transfer: Partial (Target-Dialog header not supported) • draft-ietf-sip-connect-reuse • draft-ietf-sip-location-conveyance (Pass-through for MESSAGE method) • draft-ietf-sip-answermode • draft-ietf-sip-acr-code (Pass-through) • draft-ietf-sip-certs (Pass-through) • draft-ietf-sip-uri-list-message (Pass-through) • draft-ietf-sipping-service-examples • draft-ietf-sipping-cc-framework (Partial) • draft-ietf-sipping-nat-scenario (SBC provides different solution) • draft-ietf-sipping-mwi • draft-ietf-sipping-cc-transfer (Partial) • draft-ietf-sipping-transc-conf (SBC manages transcoding) • draft-ietf-avt-dtls-srtp-06 • draft-sen-midcom-fw-nat-01.txt
SDP: IETF	<ul style="list-style-type: none"> • Session Description Protocol (RFC 2327) • Offer/Answer Model with SDP (RFC 3264)

Public switched telephone network/SIP (PSTN/SIP) interworking	<ul style="list-style-type: none"> • SIP-I transparency • Support for Tel-URI (RFC 3966) • Using E.164 Numbers with the SIP (RFC 3824) • MIME Media Types for ISUP and QSIG Objects (RFC 3204) • SIP or Telephones (SIP-T): (SIP-T): Context and Architectures (RFC 3372): Pass-through • ISUP to SIP mapping (RFC 3398): Pass-through • SIP PSTN Call Flows (RFC 3666)
H.323: ITU-T	<ul style="list-style-type: none"> • H.323 Version 4 • H.245 Version 10 • Reliability, availability, and serviceability (RAS)
H.248/Megaco	<ul style="list-style-type: none"> • H.248.1 Version 3 (Partial) • H.248.1 Annex B (Text Encoding) • H.248.1 Annex D (Transport over IP – TCP and UDP) • H.248.1 Annex E (Basic Packages): Partial (Basic Root package [root], Basic DTMF Generator package [dg], DTMF Detection [dd], Network package [nt], RTP package [rtp], and Segmentation package) • H.248.8 Error Codes and Service Change Reason • H.248.10 (07-2001) Media Gateway Congestion Handling Package • H.248.11 (11-2002) Media Gateway Overload Package • H.248.14 (03-2002) Inactivity Timer Package • H.248.37 (09-2005) IP NAPTR Traversal Package • H.248.41(04-2006) IP Domain Connection Package • H.248.45 (05-2006) MGC Information Package • ETSI TS 102 333 NAT Traversal Package (ntr) • ETSI TS 101 332 v4.1.1 (06-2002) Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4. (Partial: Middlebox package) • ETSI TS 102 333 v.1.1.2 (07-2004) Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN): Gate Control Protocol • MSF 2006.006.002 Termination State Control Package (Partial) • MSF 2006.006.002 Session Failure Reaction Package (Partial) • H.248 Profile (Gate Information package, Enhanced Base Root package, Enhanced VPN discrimination package, and Endpoint Statistics package)
3GPP/IMS	<ul style="list-style-type: none"> • TS 24.229 Release 7 Technical Specification Group Core Network and Terminals; IP Multimedia Call Control Protocol based on Session Initiation Protocol and SDP (Partial) • TS 24.229 Release 7 Annex F and Annex G: IMS NAT Procedure (Partial) • TS 33.203: IMS Security (Partial)

Table 3. Hardware Module Specification

Feature	Description
Physical Specifications	
Chassis slots required	Occupies one slot in the chassis
Dimensions (H x W x D)	1.75 x 15.51 x 16.34 in. (44.45 x 394 x 415 mm)
Weight	11 lb (4.98 kg)
Operational Specifications	
Ambient operating temperature	0 to 40°C (32 to 104°F)
Ambient storage temperature	-40 to 70°C (-40 to 158°F)
Operating relative humidity	10 to 85%
Storage relative humidity	5 to 95%
Operating Altitude	
Certified for operation	0 to 2000m (0 to 6500 ft)
Designed and tested for operation	-60 to 3000m (-200 to 10,000 ft)

Emissions	<ul style="list-style-type: none"> • FCC Part 15 (CFR 47) Class A or B • ICES-003 Class A or B • EN55022 Class A or B • CISPR22 Class A or B • AS/NZS CISPR22 Class A or B • VCCI Class A or B • CISPR24, EN55024 • EN50082-1 • EN61000-3-2 • EN61000-3-3 • EN61000-6-1
Safety	<ul style="list-style-type: none"> • UL 60950 • Can/CSA –C22.2 NO. 60950 • EN 60950 • IEC 60950 • AS/NZS 60950 • TS001

Ordering Information

Table 4 gives ordering information for the Cisco 7600 Series SBC.

Table 4. Ordering Information

Product Description	Product Number
Cisco 7600 Series ACE 20 HW for Session Border Controller	ACE20-SBC-K9
Cisco 7600 Series Session Border Controller Application RTU	ACE-SBC-RTU
Cisco 7600 Series Session Border Control H.248 License	ACE-SBC-H248
Cisco 7600 Series Session Border Control H.323 License*	ACE-SBC-H323
Cisco 7600 Series Session Border Control SIP License*	ACE-SBC-SIP

* Not required for SBC in distributed (DBE only) model

Service and Support

Cisco has earned high customer satisfaction ratings for its wide range of products, technologies, and support offerings for service providers. Whether the goal is to speed services to market, maximize network availability, or enhance customer satisfaction and retention, Cisco is committed to the success of our service provider customers around the world.

For More Information

For more information about Cisco service and support programs and benefits, please visit:

http://www.cisco.com/public/Support_root.shtml.

For more information about the Cisco 7600 Series Router, please visit:

<http://www.cisco.com/en/US/products/hw/routers/ps368/>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCI, CCNA, CCNP, CCS, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)