Cisco ASR 1000 Series Session Border Controller

This paper provides an overview of the Cisco® Session Border Controller (SBC) implementation in a distributed deployment model on the Cisco ASR 1000 Series Aggregation Services Routers. It also briefly explains what the SBC is, its different deployment models, and how the SBC helps with multimedia applications. It explains the features available on the Cisco ASR 1000 Series Router that facilitate its functioning as a data border element (DBE) in the SBC distributed deployment model. This paper assumes that you have a basic understanding of voice technologies and the need for a SBC.

SBC Overview

SBC functions are becoming very popular in the voice-over-IP (VoIP) industry; they are the key components used for interconnecting enterprise and service provider VoIP and multimedia networks.

Because the SBC meets the growing need for secure, IP-centric interconnections between enterprise and service provider networks, a critical need for intelligent border element functions has grown. With the SBC, you can make voice or video calls without worrying about protocols, network reachability, or security of your network. Such elements provide physical and logical ingress and egress demarcations, signaling and media control, consolidated security, and management features. The SBC is in a sense a toolkit of functions such as Signaling Interworking, network hiding, security, quality of service (QoS), and much more.

The SBC facilitates simple and cost-effective connectivity between independent networks. It provides direct IP signaling and media interconnections, thereby lowering cost and performance latencies and improving media quality for multimedia sessions. Additionally, it offers greater flexibility in migrating from traditional time-division multiplexing (TDM) to unified communications services.

Challenges in Direct VoIP Interconnect

When a voice call connects from one service provider to another service provider, usually TDM interconnects are used. With the emergence of VoIP technologies, service providers started using IP connectivity to connect to other networks so that calls originating from an IP phone could stay on the packet network from end to end. Service providers then found new challenges in passing VoIP calls to other service providers.

Because VoIP subscribers can have unique environments with respect to protocols, IP addresses, codecs, the way they carry dual tone multifrequency (DTMF) traffic, etc., interconnecting two network domains can be very difficult. In addition, each provider wants to protect its own network from other providers' networks. Furthermore, service providers face other concerns with regard to call detail records (CDRs), billing records, quality of voice calls, troubleshooting, and feature interactions – all of which make end-to-end VoIP performance extremely challenging.

Role of SBC in VoIP Interconnect

VoIP, video streaming, instant messaging, multimedia conferencing, and interactive gaming are just some of the real-time, IP-based applications enjoying rapid growth in today's competitive communications market. Service providers are now finding it efficient and economical to directly interconnect their real-time VoIP and multimedia networks to their subscribers as well as to other service provider networks. This trend has created a requirement for SBCs to help service providers control and manage real-time multimedia communications sessions at the borders between their IP networks. In addition, SBCs are also useful for the following requirements:

- Creating proper points of demarcation between service providers, or between enterprises and service providers, for manageability in the rich-media deployments such as VoIP and video

- Hiding internal network topology from the peering partner or the outside world for security purposes

- Using the SBC to provide interworking of protocols between H.323 and SIP, or between SIP and SIP (because of the rapidly changing standards and implementation of SIP)

- Media transcoding, routing VoIP traffic to traverse firewalls, performing Network Address Translation (NAT) and Port Address Translation (PAT), and ensuring QoS

To overcome some challenges, devices such as SBCs are needed at various interconnect points.

SBCs are generally deployed in one of two models: unified and distributed deployment. This paper covers the Cisco ASR 1000 Series implementation in the distributed deployment model.

Deployment Scenarios

The SBC plays an important role in many different deployment scenarios. Figure 1 shows some network topologies in which an SBC is used.

Figure 1. SBC Used for VoIP Interworking
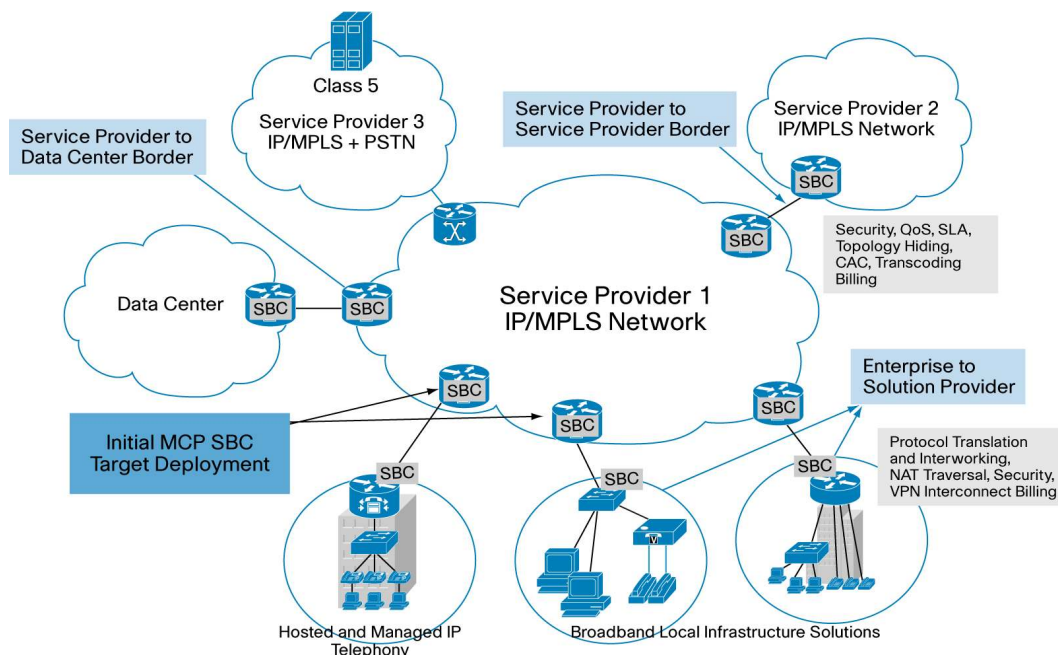
In this scenario, one service provider core network is connected to different types of networks such as data center; enterprise users; broadband users; hosted and managed IP telephony; and voice gateway connecting to the public switched telephone network (PSTN) network, and even another service provider network. Considering security requirements from these different subscribers' perspective, each wants to protect its own network, and the core service provider also wants to secure its network from these subscribers. In addition to protecting network addresses, the SBC is also useful in the conversion of different codecs, DTMF, differentiated services code point (DSCP) marking, etc. from these subscribers. Different types of subscribers have different needs, and they select the features they want to use. For example, at the service provider-to-service provider interconnect, each service provider is more interested in protecting its network, CDR and billing, QoS, etc. But at the service provider-enterprise interconnect, the service provider is more interested in taking advantage of the local private automatic branch exchange (PABX, such as call manager, IP-based PABX) and offering QoS and codec transcoding – all while protecting its networks. Thus the SBC is a toolkit of functions that can facilitate specific features depending on the requirements of the service being offered.
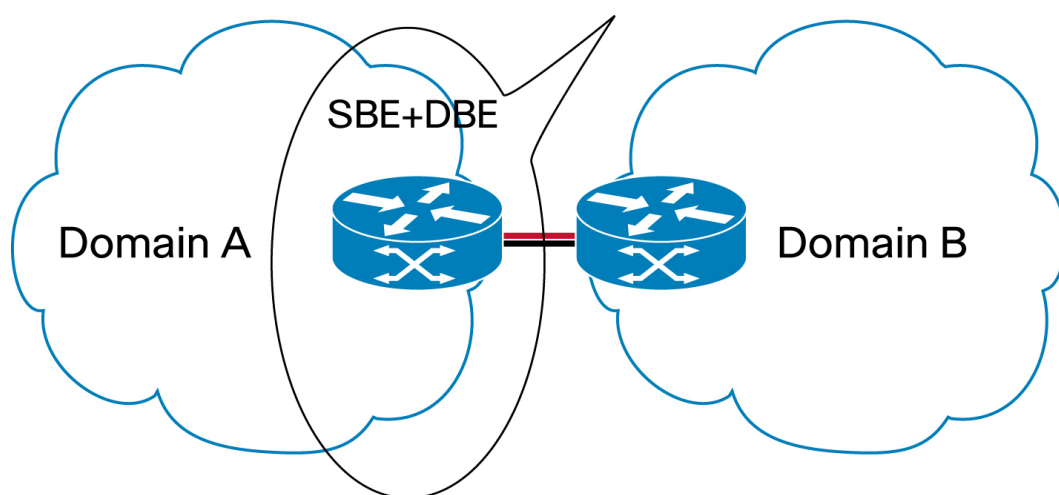
Unified and Distributed Deployment Models

SBC functions can be broadly divided into two logical sub-elements: signaling path border element (SBE) and data path border element (DBE). The SBE provides signaling functions such as protocol interworking (for example, H.323 to SIP), identity and topology hiding, and Call Admission Control (CAC). The DBE provides media-related functions such as Deep Packet Inspection and Modification, Media Relay, and firewall support under SBE control.

The Unified SBC Model

In the unified SBC model, the SBE and DBE logical elements are generally within a single, physical SBC device. As shown in Figure 2, SBE and DBE are combined in a single network element and the SBC resides at the edge of the domain.

Figure 2. Unified SBC Model

In this model signaling and media both pass through the same physical device.
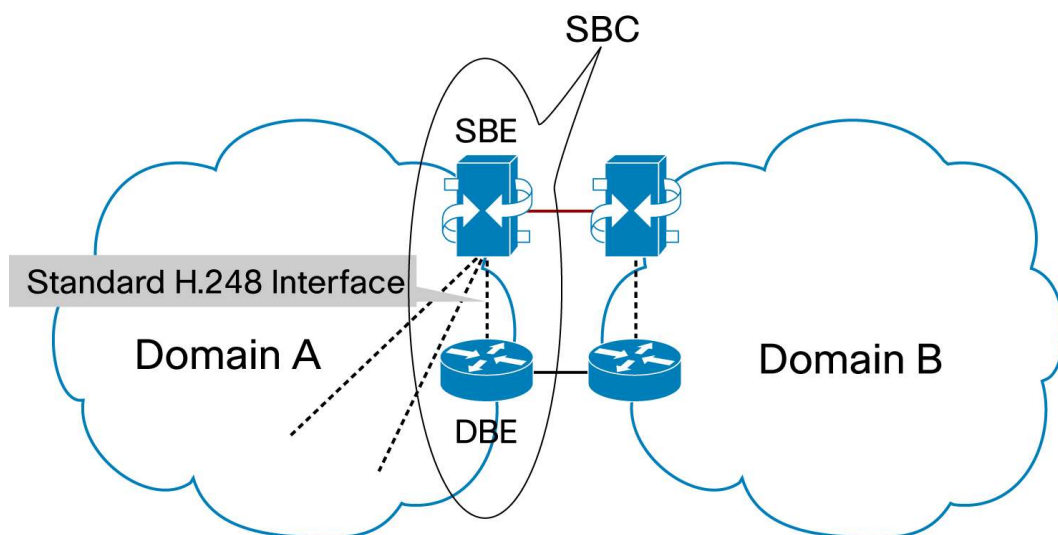

Distributed Deployment Model

Many carriers are finding that as their voice networks grow, the challenges of managing the networks grow proportionately. Service providers today want the option to decouple the SBC data-path functions from signaling functions. They want to be able to distribute DBE functions in the network separately from the SBE functions, which can be centralized to simplify management, operations, and troubleshooting. Generally in this model the SBE functions are concentrated in central locations and the DBE functions are distributed with the network routing functions.

Figure 3 shows that in the distributed deployment model communication between the SBE and DBE takes place over a well-defined standard, such as ITU-T H.248 adopted in IP Multimedia Subsystem (IMS), which allows a multiplatform implementation of the SBE and DBE elements in the network. The distributed approach to SBC aligns with the directional approach of IMS, ITU, and Telecoms and Internet Converged Services and Protocols for Advanced Networks (TISPAN) architectures, where a variety of different elements and applications in the network can provide the SBE function. In TISPAN terminology the Cisco ASR 1000 Series Router DBE function provides the Border Gateway Function (BGF) and interacts with the Service Policy Decision Function (SPDF). SPDF uses the H.248 protocol to set up and tear down media paths (gates) on the router and apply per-session policies.

In the distributed deployment model, the bearer traffic or media packets always flow through the DBE, and the SBE participates only in the signaling flow. The DBE handles the media-related functions such as Deep Packet Inspection (Real-Time Transport Protocol [RTP] and Real-Time Streaming Protocol [RTCP]), and modification of packet headers, Media Relay to handle NAT traversals, Topology Hiding, etc.

Figure 3.   Distributed SBC Model

A flexible network component with an integrated SBC supports both the unified and the distributed deployment models. Networks continually grow and evolve, and a multimedia IP transport network that scales adequately today with a unified SBC will likely outgrow the unified model and necessitate a distributed approach. Operators want a SBC that can grow with their networks – they do not want to make capital-intensive complete equipment upgrades of in-service network elements.

Table 1 gives the main differences between unified and distributed SBC models.

Table 1.   Unified and Distributed SBC Model Differences

Unified SBC Model	Distributed SBC Model
All required SBC functions integrated	Centralized signaling and control logic
No dependency on other applications	Scalable design enabling a pay-as-you-grow business model

Cisco ASR 1000 Series Implementation of SBC

As mentioned in the distributed deployment model discussion, the SBE and DBE entities reside on different network elements. The SBE interacts with the DBE entity using a H.248 standard interface.

Consider the data flow inside the Cisco ASR 1000 Series Router. Figure 4 shows two views of the implementation: a software view and a systems view. With regard to hardware, the main components of the Cisco ASR 1000 Router are the Cisco ASR 1000 Series Route Processor, the Cisco ASR 1000 Series Embedded Services Processor (ESP), the Cisco QuantumFlow Processor (QFP), and the Cisco ASR 1000 Series SPA Interface Processor (SIP), which brings in the data from the endpoints. The system view shows that the route processor has the CPU to perform the control function and the ESP has the Cisco QuantumFlow Processor to process the media packets.

The function of the route processor is to process H.248 control packets arriving from the SBE and use the per-session policy received from the SBE to set up pinholes and media packets to handle criteria on the ESP. The ESP forwards media packets based on these criteria with the help of the Cisco QuantumFlow Processor. When the data comes from the SIP to the Cisco QuantumFlow Processor, it checks and determines whether it is an H.248 control packet or a regular media packet. If it is an H.248 control packet, it then punts these packets to the route processor for processing; if it is a regular media packet for the defined pinhole, then the forwarding processor handles the data itself with the help of the Cisco QuantumFlow Processor. So in the DBE case, when the media pinholes are created the ESP processes the voice and video media packets and the route processor is not involved. The route processor gets involved only for the SBC control packet by communicating with the SBE using the H.248 protocol for defining and modifying pinholes and policies.

The Cisco ASR 1000 Series Router also has a cryptographic hardware engine built into the ESP to help in processing encrypted data. Whenever encrypted data comes to the Cisco QuantumFlow Processor, the processor punts that data to the cryptographic engine for decrypting and encrypting. Having the hardware cryptographic engine built in helps in fast processing of the encrypted data.

Figure 4. Functional Diagram of Cisco ASR 1000 Series Router
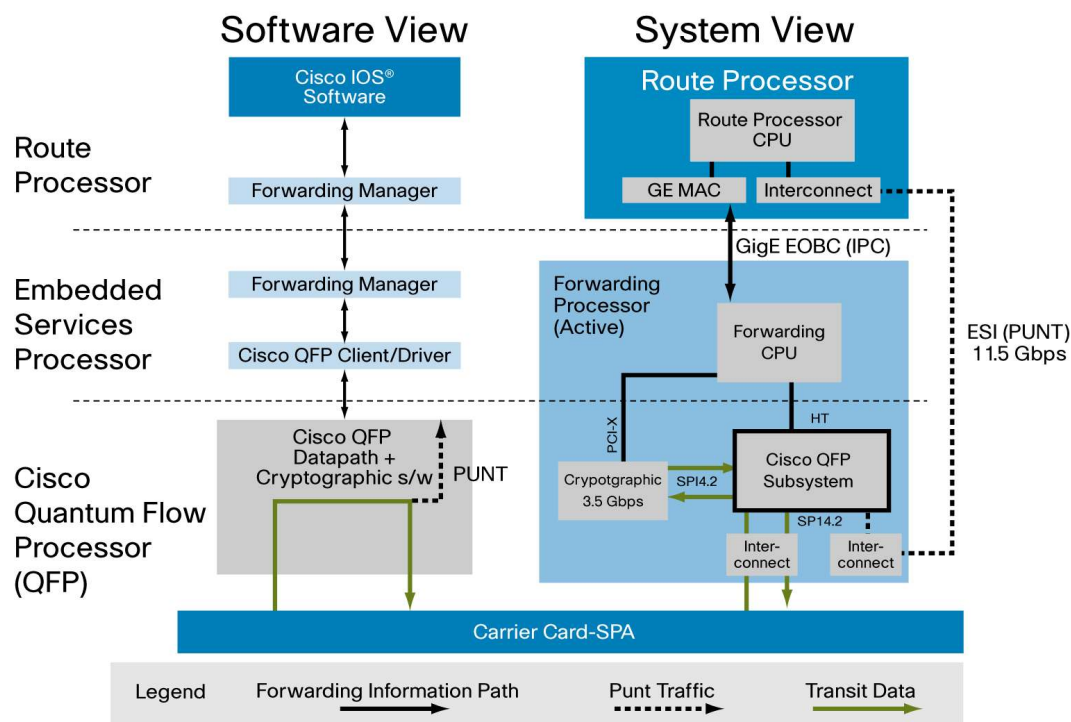
SBC Basic Call Flow

Figure 5 illustrates the signaling flow in the distributed SBC model.

Figure 5. Basic SBC Call Flow
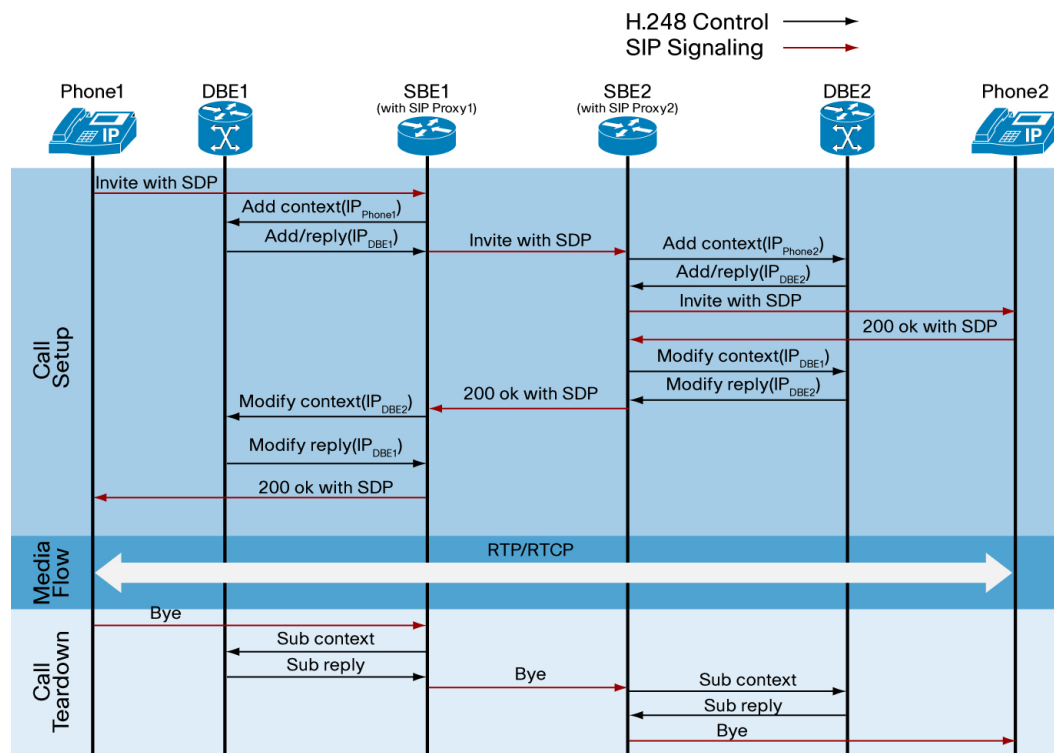
The figure shows that the SIP invite message is sent from the end device (phone1) to SBE1 directly. Based on that SIP message, SBE1 instructs DBE through H.248 to open a media pinhole using H.248 commands. On receiving a reply from DBE, SBE1 sends a SIP invite message toward the other SBE for the terminating side. That SBE also opens a media pinhole on its side of the SBE using an H.248 interface. On receiving a reply from DBE2, SBE2 sends an invite message to the end user (phone2). When SBE2 gets a 200 ok SIP message from the end user, it asks the DBE to configure the stream in SendReceive mode using the modify context command of H.248 and forwards that 200 ok message toward the originating-side SBE. The originating SBE also modifies the media stream to send a receive message in DBE using a modify H.248 command and then forwards the 200 ok message to the originating user (phone1); then the media traffic can start. In this way media is established. Similarly, the BYE message is sent from one of the end users and SBE instructs the respective DBEs to subtract the connection; in this way the call gets cleared.

Even though DBE handles only media packets, the signaling packets also pass through the DBE. On instructions from SBE, DBE can create signaling pinholes that can be used for traversing signaling packets. The signaling pinholes are created like media pinholes, and you can enforce different policies on them. Signaling pinholes support can help in protecting the SBE infrastructure from the end users who are using NAT traversal packages.

DBE Features

As discussed before, the SBC is a toolkit of functions that helps particular functions meet different design criteria and needs. The distributed SBC DBE implementation covers various functions such as Signaling Interworking or Control Path Management, Topology Hiding, billing and CDR, QoS, etc. In the distributed deployment model, the many DBE functions are controlled by the SBE with the H.248 signaling control. The following DBE features are supported on the Cisco ASR 1000 Series Routers:

- **Signaling Interworking or Control Path Management:** For signaling, DBE opens signaling pinholes and forwards the traffic to SBE; for the control path, DBE interacts with SBE and opens media pinholes and executes policies defined by SBE through the H.248 interface.
- **Topology Hiding:** The DBE protects the signaling infrastructure and media packets by NAT and PAT. It supports no-, single- and twice-NAT and -PAT traversal schemes.
- **Security:** The different H.248 packages such as gate management and traffic management provide infrastructure security and bandwidth protection. With these packages, the DBE can enforce different policies such as checking the originating addresses of allowed traffic and allowed bandwidth. It can also watch for denial-of-service (DoS) attacks by monitoring incoming packet addresses and dropping suspicious source packets. The SBE is alerted when these types of events occur.
- **QoS:** For QoS, the DBE implementation supports per-session DSCP marking of packets and the traffic-management package for bandwidth management (using two-rate, three-color policing). The Cisco ASR 1000 Series Router platform also supports other QoS functions such as Low Latency Queuing (LLQ), Class-Based Weighted Fair Queuing (CBWFQ), Traffic Shaping, etc. at (sub) interface level.

- **Media management:** The Cisco ASR 1000 DBE implementation supports RTP and RTCP for media packets. The DBE checks for the media supported by five addresses (source IP address, source port address, distribution IP address, distribution port address, and the IP address). The DBE implementation is independent of codec type, so all codecs are supported. The DBE can also detect and insert DTMF digits in the media stream with the help of H.248 packages. It can also detect any hung calls using the inactivity timer.
- **Billing:** Accurate billing and CDRs are provided to the SBE on completion of the call. The DBE can also generate information about packet loss, jitter, and round-trip time on completion of the session.

High Availability

DBE High Availability is similar to other features. Cisco ASR 1000 Series Routers support Stateful Switchover (SSO) and In Service Software Upgrade (ISSU). The Cisco ASR 1000 Series Router platform includes 2-rack-unit (2RU), 4RU, and 6RU platforms, with different types of redundancy available.

In the 6RU Cisco ASR 1000 Router chassis, DBE can have a redundant route processor and a redundant ESP. When the active route processor fails, the standby route processor becomes active without any packet loss. Similarly for active ESP failure, the standby ESP becomes active, with some in-flight packet loss. Ongoing calls statistics are maintained and switchover is transparent, but SSO of calls is available only to the already set up active calls; calls in the setup process need to redialed.

In the 4RU Cisco ASR 1000 Router chassis, no redundant route processor or ESP is available, but it can have dual Cisco IOS Software daemons running, with one active and the other in redundant mode. Thus for SBC implementation on Cisco ASR 1000 Series Router platform, extensive hardware and software redundancy is available with SSO capability.

The Cisco ASR 1000 Series Routers also provide In-Service Software Upgrade (ISSU) support, and with that support the routers can upgrade specific software components (referred to as sub-packages) within a software consolidated package. For example, the route-processor subpackage can be upgraded without affecting the other subpackages and without affecting ongoing services. For details on the consolidated packages and sub-packages please refer to the Cisco ASR 1000 Series Software Release Strategy Product Bulletin at http://www.cisco.com/go/asr1000.

Why Cisco?

Cisco is the worldwide leader in networking and VoIP technologies. The difference between Cisco solution and Appliance solution and topological diagram is explained below in Figure 6. With appliance model, SBC functionality and routing functionality resides on separate system and with Cisco solution both resides on the single system.

Figure 6.   Cisco Integrated Model Versus Appliance Model
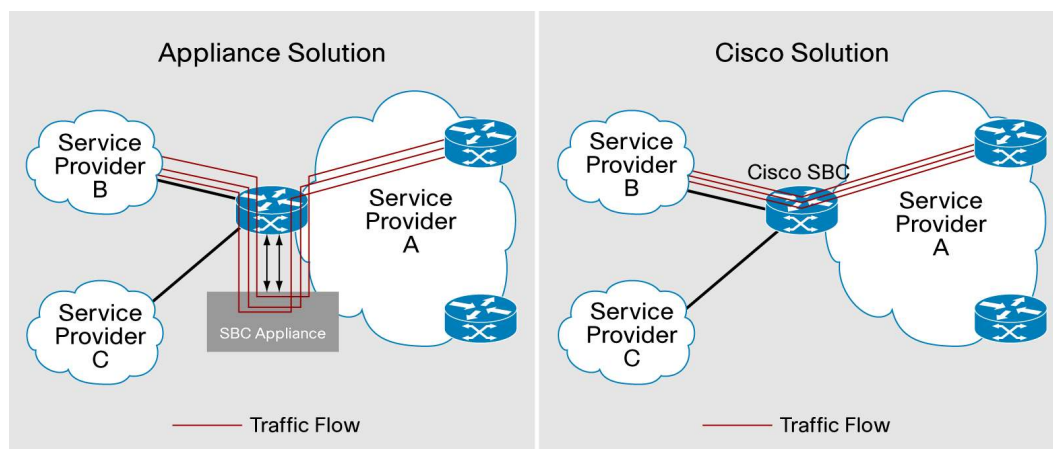
- The Cisco solution helps reduce capital expenses (CapEx) and operating expenditures (OpEx) by using the distributed SBC deployment model wherein the DBE is integrated in the Cisco ASR 1000 Series Router.
- The distributed SBC model with the DBE function integrated with the router has fewer hops compared to the appliance model, resulting in lower latency for the packets. Lower latency is important for real-time traffic applications such as VoIP and video.
- Because SBC is a Cisco IOS Software-based solution, you can take advantage of Cisco IOS Software features such as QoS, access control lists (ACLs), IP Routing, etc.
- Cisco ASR 1000 Series Routers can also provide stateful redundancy by using dual route-processor and ESP modules.

Summary

The SBC is becoming an increasingly important component of VoIP networks. It provides important features such as Signaling Interworking, Topology Hiding, QoS, security, etc. The Cisco ASR 1000 Series Router can act as a DBE in the distributed SBC deployment model; this design also meets the IMS and TISPAN terminology. The Cisco ASR 1000 Series Router with an integrated DBE function can reduce CapEx and OpEx for enterprises and service providers.

The distributed architecture of the Cisco ASR 1000 with a high-capacity data forwarding engine provides a more scalable implementation of the DBE portion of the SBC. Because this function runs on Cisco IOS Software, you can use features of the software also with the SBC. In addition, it provides higher redundancy of routing and embedded services processors so that service providers can give nonstop service to their users.

For More Information

For more information about the Cisco SBC implementation on the Cisco ASR 1000 Series Aggregation Services Routers, visit:

- H.323 forum: http://www.h323forum.org/papers/
- VoIP information: http://www.packetizer.com/
- Scalable SBC capabilities for service provider networks: http://cisco.com/en/US/products/ps6342/products_white_paper0900aecd80391b66.shtml
- Overview of H.248 protocol: http://www.packetizer.com/voip/h248/
- SIP: http://www.cs.columbia.edu/sip/
- TISPAN: http://www.etsi.org/tispan/
- Cisco ASR 1000 Series Session Border Controller data sheet: http://www.cisco.com/go/asr1000
- Cisco IOS XE Software Licensing product bulletin: http://www.cisco.com/go/asr1000