Cisco Unified Border Element (SP Edition) on Cisco ASR 1000 Series

The Cisco® Unified Border Element (SP Edition) is a high-scale, carrier-grade Session Border Controller (SBC), which is integrated into Cisco routing platforms and can use a huge number of router functions to provide a very feature-rich and intelligent SBC application. In Cisco earlier known as Session Border Controller, Cisco Unified Border Element (SP Edition) provides a network-to-network demarcation interface for signaling interworking, media interworking, address and port translations, billing, security, quality of service, call admission control, and bandwidth management. This paper provides an overview of the Cisco Unified Border Element (SP Edition) implementation in a Unified Session Border Controller (SBC) deployment model on the Cisco ASR 1000 Series Aggregation Services Routers. It also briefly explains what the Session Border Controller is, its different deployment models, and where the SBC's different functionalities can be used to achieve different solution objectives. This paper assumes that the reader has basic understanding of voice technologies such as Session Initiation Protocol (SIP) and H323 protocols and the need for an SBC.

Challenges in Direct Voice-over-IP Communication

In the early days of voice over IP (VoIP), packet voice networks existed in isolation from one another, interconnecting primarily to the public switched telephone network (PSTN) to complete off-network calls. Eventually, VoIP service providers sought to establish direct peering relationships between their networks, and to do so they installed back-to-back time-division multiplexing (TDM) media gateways as bridges between their separate VoIP "islands." Although this architecture was functional, it introduced new problems due to the repeated voice encoding and decoding at the media gateways, and it affected voice quality.

Also with the development of newer technologies, the multimedia devices started becoming more feature rich and popular. It increases the variety of usage such as VoIP, video streaming, instant messaging, interactive gaming, and so on, and all these bring various types of interop problems. All these functionalities to interoperate transparently require a device that can make different types of functionalities and protocols interoperable.

Role of Cisco Unified Border Element (SP Edition) in Direct VoIP Communication

The Cisco Unified Border Element (SP Edition) is the devices that replaces the back-to-back media gateway pairs and allows native IP interconnects between VoIP networks. It can interconnect, control, and manage real-time VoIP/multimedia sessions at the borders between different IP networks. Service providers find 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.

In addition, Cisco Unified Border Element (SP Edition) is 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 helping ensure QoS

To overcome some challenges, Cisco Unified Border Element (SP Edition) can be deployed at various interconnect points.

## Deployment Models Offered by Cisco Unified Border Element (SP Edition)

SBCs are generally deployed in one of two models: Unified Deployment and Distributed Deployment. Cisco Unified Border Element (SP Edition) supports both models.

SBC functions can be broadly divided into two logical subelements: 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 part of a single, physical device as shown in Figure 1 (left side).

Figure 1.   Unified and Distributed SBC Model
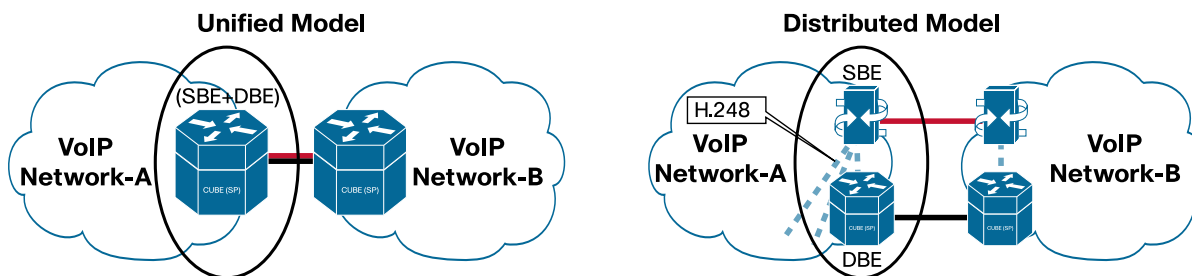
The SBE functionalities handle SIP/H323 protocol handling, identity and topology hiding, CAC, and so on, and the DBE functionalities handle media packet handling and apply different policies defined by SBE for the media packets. The unified model provides the complete solution to the SBC functionalities without any external dependencies.

Distributed Deployment Model

In the distributed SBC model, the SBE and DBE are part of different device, and they interact by standard H.248 interface as shown in Figure 1 (right side). Generally in this model the SBE functions are concentrated in central locations and the DBE functions are distributed with the network routing functions.

The distributed approach to SBC aligns with the directional approach of IMS, ITU, and TISPAN (Telecoms and Internet Converged Services and Protocols for Advanced Networks) architectures, where a variety of different elements and applications in the network can provide the SBE function.

Deployment Scenarios

As mentioned before, Cisco Unified Border Element (SP Edition) was formerly known as Session Border Controller (SBC).

Cisco Unified Border Element (SP Edition) deployment can be divided into two main categories, and that is UNI (User-Network Interconnect) and NNI (Network-Network Interconnect) modes. Figure 2 describes UNI and NNI positions where Cisco Unified Border Element (SP Edition) can be deployed.

Figure 2.   UNI and NNI Cisco Unified Border Element (SP Edition) Model
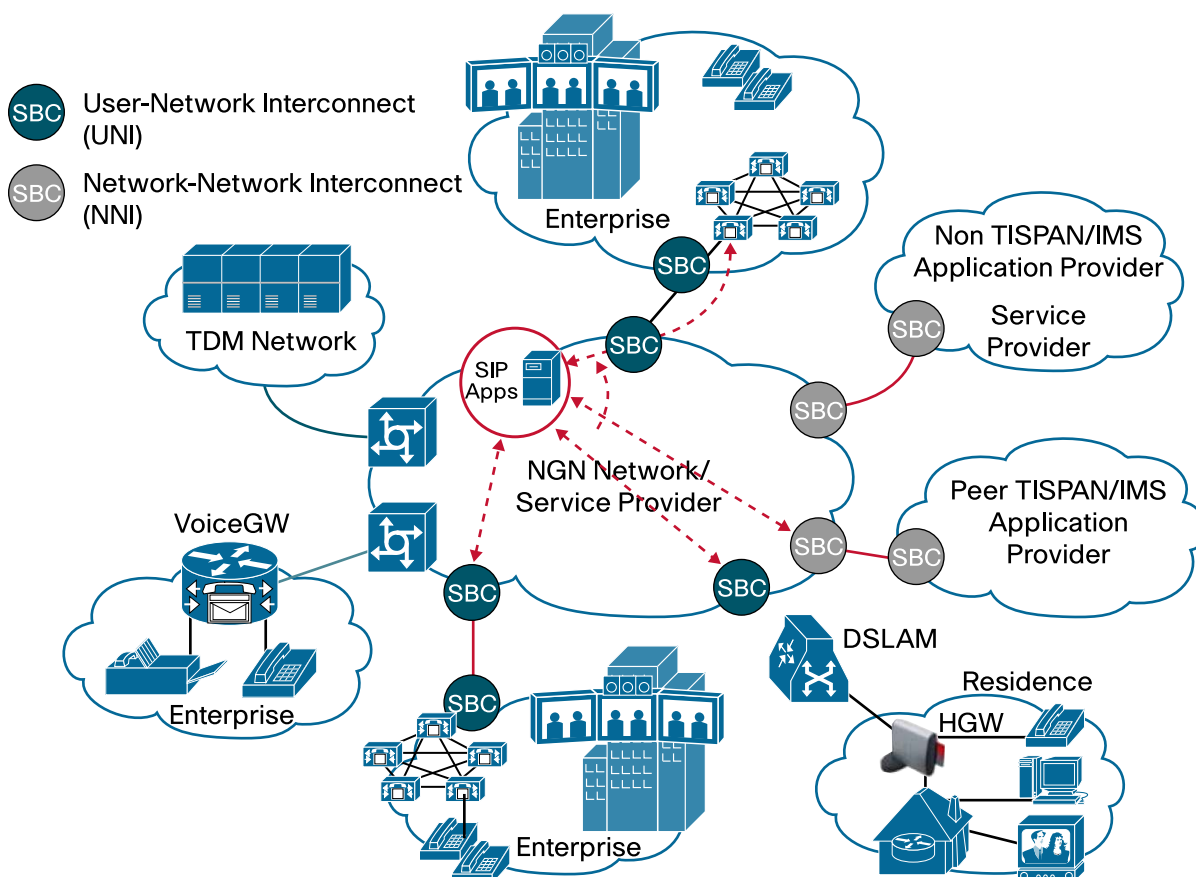
In Figure 2, Cisco Unified Border Element (SP Edition) is used at different locations to protect service provider and large enterprise networks. The service provider network uses UNI mode Cisco Unified Border Element (SP Edition) to connect to either residential users or enterprise networks. Here it enabled different set of functionalities such as topology hiding, NAT traversal, marking packets, billing record collection, and other security feature. The service provider side also needs to protect its network from DoS attacks, signaling, and malformed packets flooding toward networks, especially from residential users. On the enterprise side, it also uses Cisco Unified Border Element (SP Edition) to protect its side of network and requires similar functionalities such as UNI mode.

When one service provider network connects to other service provider networks, it uses Cisco Unified Border Element (SP Edition) in NNI mode. With NNI mode it enables different set of functionalities such as topology hiding, demarcation, CAC, marking packets, checking for quality of packets before leaving its network, and billing. Service provider wants to make sure that their side of network is reliable and provide proper SLA as defined. With proper equipment such as Cisco Unified Border Element (SP Edition) they can collect the right data to claim reliability of their side of IP networks.

Residential Scenario

Figure 3 describes sample residential deployment mode with triple play services. ASR 1000 based Cisco Unified Border Element (SP Edition) can allow triple play services simultaneously. The Cisco Unified Border Element (SP Edition) functionality is used for managing voice/video calls; broadband functionality is used for connecting PC to the Internet, and the same router can also enable multicasting for IPTV traffic.

Figure 3. Residential Cisco Unified Border Element (SP Edition) Model
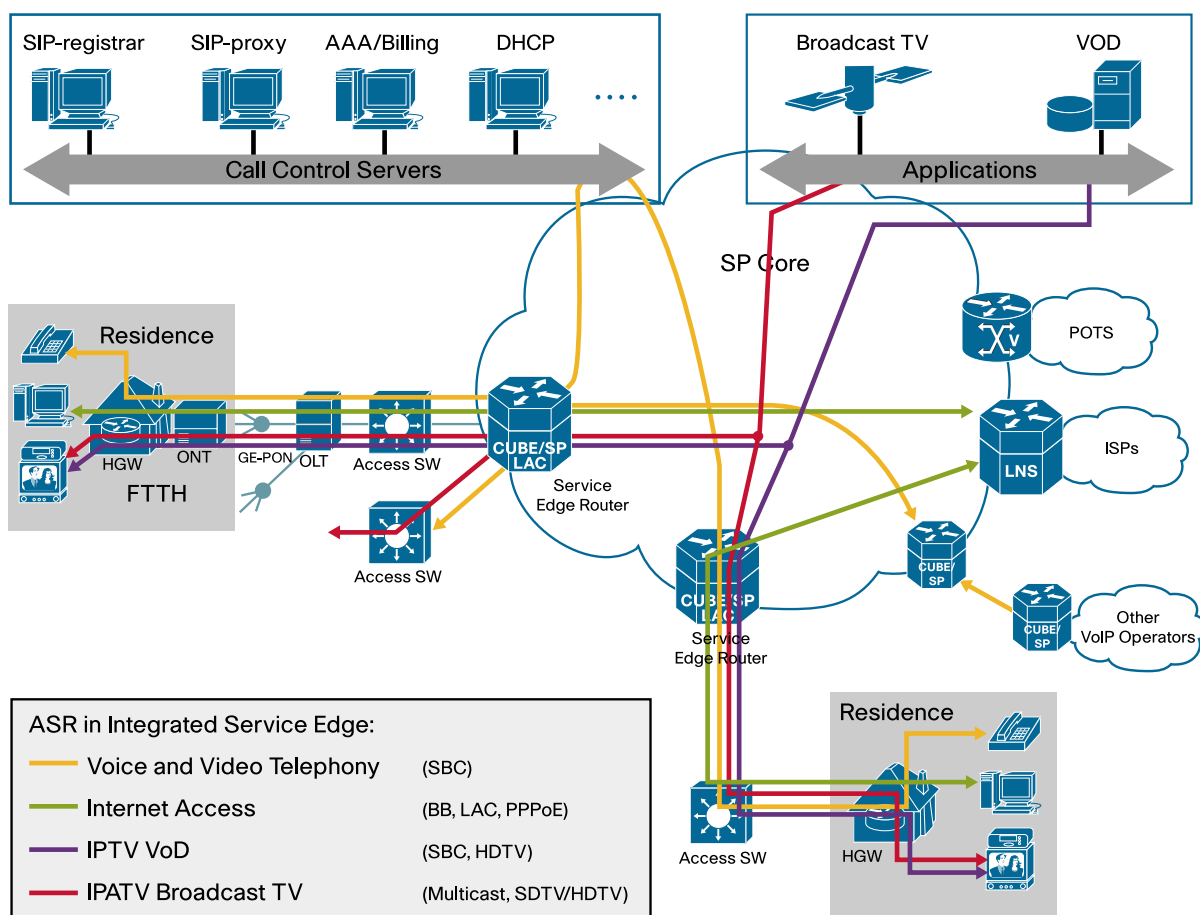
As shown in the diagram, there is set of call control servers for doing multiple functions such as authentication, DHCP, billing, and SIP registrations. These control servers give centralized control for registration and call routing, and they also collect centralized billing records. Once the endpoint is registered it can make calls to another user, and that user can be connected to the same Cisco Unified Border Element (SP Edition) or a different one. If the terminating side is on a PSTN network then that call has to be routed across media gateway for connectivity.

Also as shown in the diagram the same ASR 1000 system can also enable other functionality such as broadband, and/or multicast for IPTV traffic simultaneously with Cisco Unified Border Element (SP Edition) functionality. That way with ASR 1000 system, service provider can provide multiple services to end user.

SIP Trunking Scenarios

Service providers have been offering their business customers managed services for different kinds of applications such as VPN, security service, and so on for quite some time. Now since the evolution of IP-based unified communication, there is a need for managed services for it. VoIP protocol and interoperability with different protocols/standards/draft interpretations and its implementation can become very complex. This brings the need for managed services so that business customers do not have to look for these complexities and it becomes value additional services from service provider side.

Another advantage SIP Trunking brings is reducing cost for service providers and enterprise customers. Since the Cisco Unified Border Element (SP Edition) is integrated into routing device, service providers can provide advance multimedia services at a reduce cost by operating and managing fewer number of equipments. With this service, enterprise side can reduce cost of TDM gateways and PSTN charges. For the enterprise customers both the voice

and data will be integrating in a single device, and that will reduce the overall operating and managing cost. (See Figure 4.)

Figure 4.   Managed Services Scenario
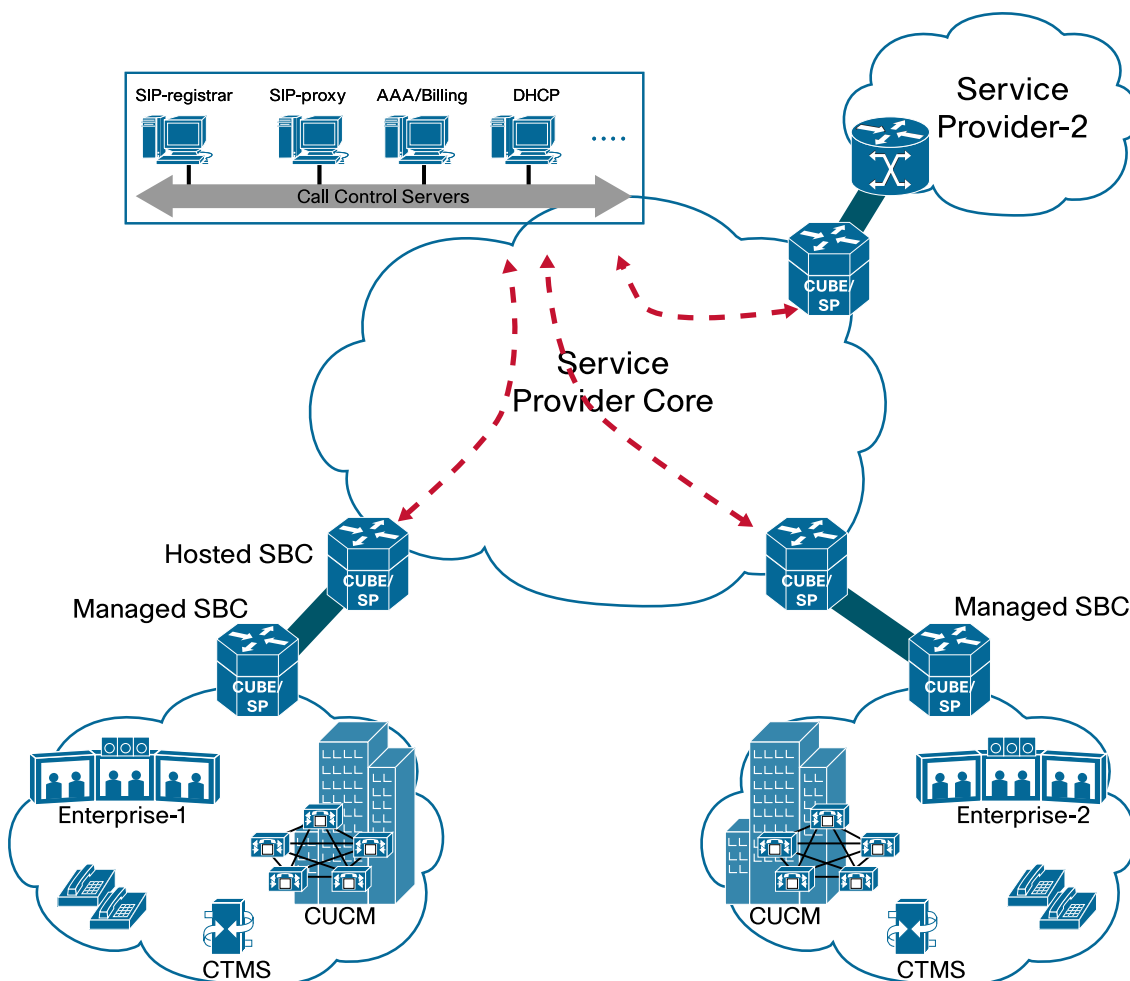
As shown in Figure 4, large enterprises can have Cisco Unified Border Element (SP Edition) at their edge but will be managed by service provider. The diagram also shows Cisco Unified Border Element (SP Edition) at the SP edge, which is required to protect SP network domain. With the managed SBC following are advantages for service provider and enterprise customers:

- Service provider can provide defined SLA and dedicated service
- Service provider can define the use of latest standard to offer newer services
- Enterprise side does not need to develop expertise to manage the services and could result in saving cost
- Consistent and reliable services with a global reach

A managed service generates additional revenue for service providers with the value addition service and simultaneously saves operational costs for the enterprise customers.

SIP Peering Scenario

The SIP peering scenario helps VoIP carriers as well as enterprises to interconnect their networks so calls originating or terminating as VoIP are not carried over to TDM networks. Figure 5 shows two service provider networks connected by Cisco Unified Border Element (SP Edition) at their respective edges. Each service provider

---

has its own central call control center to manage their side of networks and uses peering Cisco Unified Border Element (SP Edition) if the endpoint is located across their network. This way both side can avoid using TDM network for their call connections.

Figure 5.   SIP Peering SBC Scenario
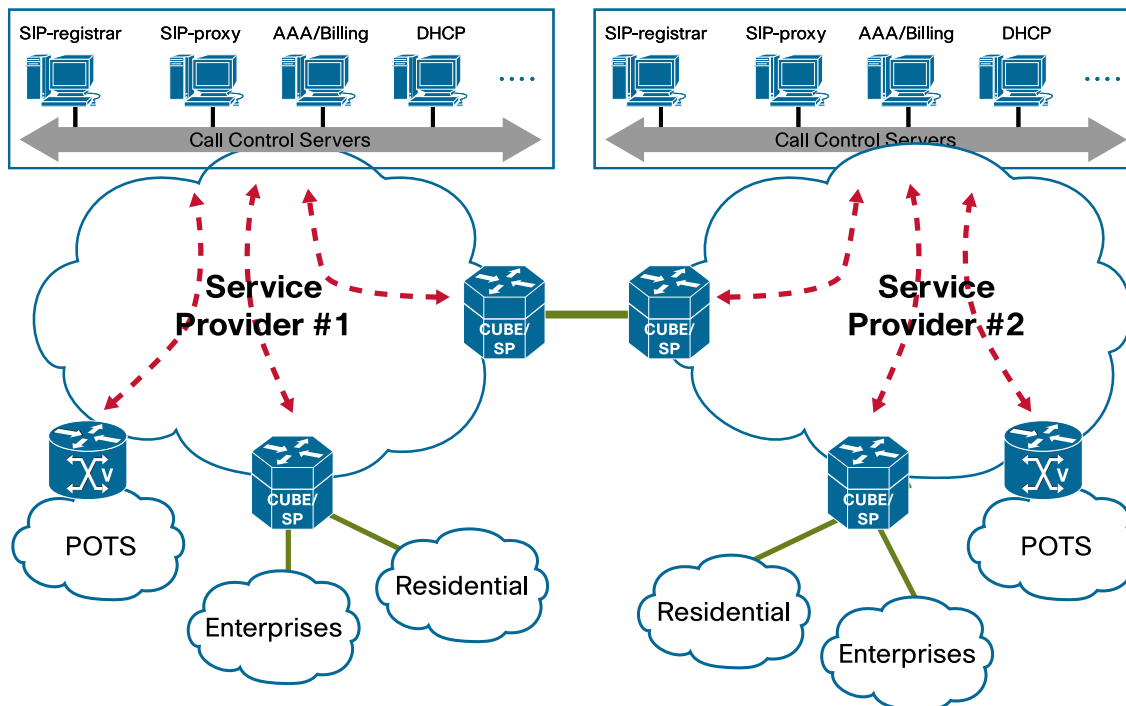
There are many advantage of using SIP peering services. SIP peering reduces need for voice packet packetization from G.711 to PSTN and back; this helps not only reduce the cost for the service provides but also improves the voice quality by reducing the end-end delay for the media packets. Another advantage of using SIP peering is that the call doesn't have to be restricted to voice call but it can be video call, Cisco TelePresence™ call, or even wide band codec call. With TDM network the session is restricted to voice call with narrowband codecs.
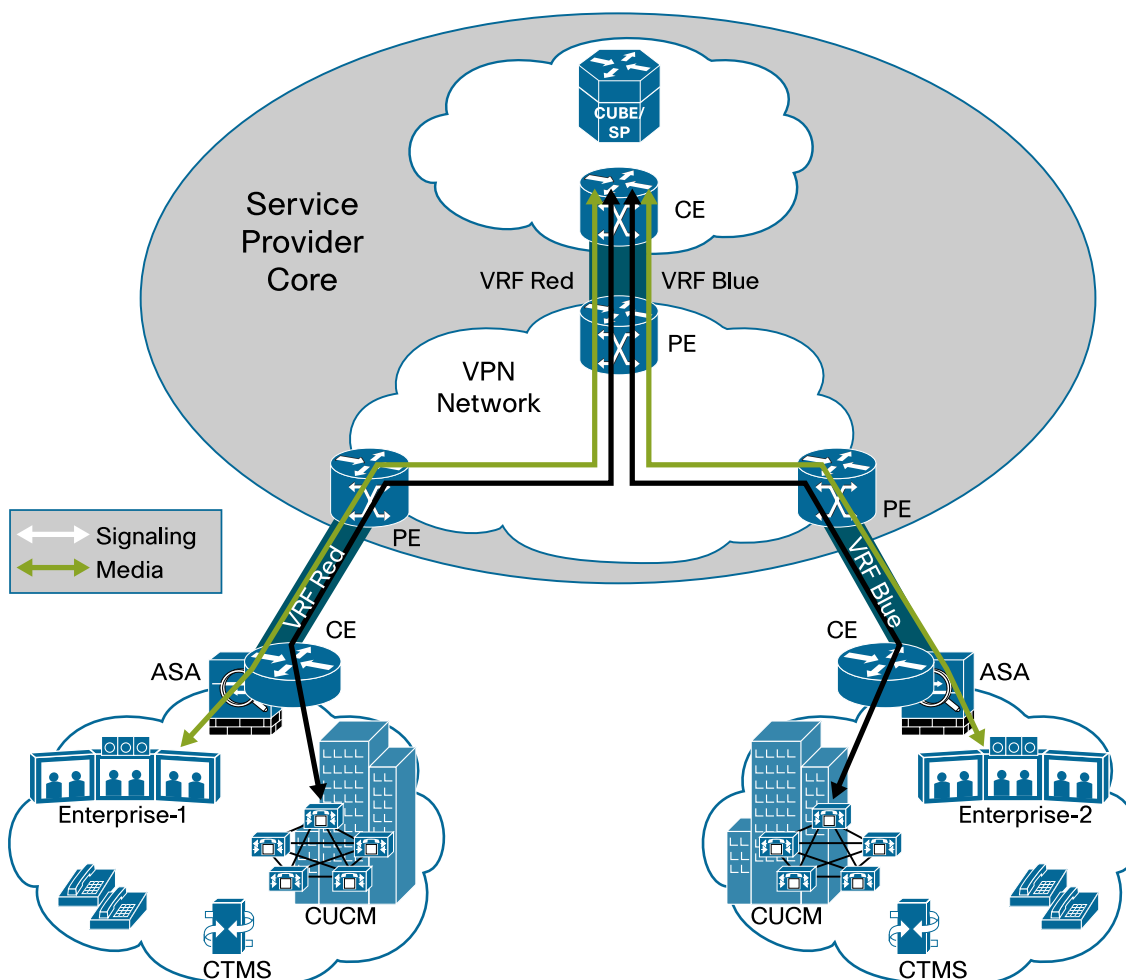
Cisco Unified Border Element (SP Edition) offers range of functions from SBC (toolkit), and one can enable the functionality when required. Service providers with SIP peering are mainly interested in following functionalities:

- Topology hiding to protect their side of network
- Call routing is another function important so that they can route the call to the right service providers
- Accounting functionality: To keep check on calls between providers so that billing can be generated
- Security is another important function they use to protect the identity and media spoofing by third party

With these functionalities and added advantages, SIP peering is becoming more common among service providers to interconnect their network, and Cisco Unified Border Element (SP Edition) plays a very important role in it.

B2B Cisco TelePresence Scenario

Cisco TelePresence conferencing is an intercompany communication system with advance visual and audio technology that delivers a face-to-face interaction experience between people across geography. Since the enterprise uses VPN to protect their network, there is a need for a device that can deliver Cisco TelePresence calls across to different VPN networks. Cisco Unified Border Element (SP Edition) is capable of providing this service across different networks.

Figure 6.   Business-to-Business Cisco TelePresence Scenario

As shown in Figure 6, we can see two enterprises with Cisco TelePresence units in different VPN networks. ASR 1000 Cisco Unified Border Element (SP Edition) can detect sessions coming from different VRFs and allow them to connect to each other.

This deployment model enables service providers to reduce their TCO by avoiding additional equipment and simplifies the operation management for the overall solution.

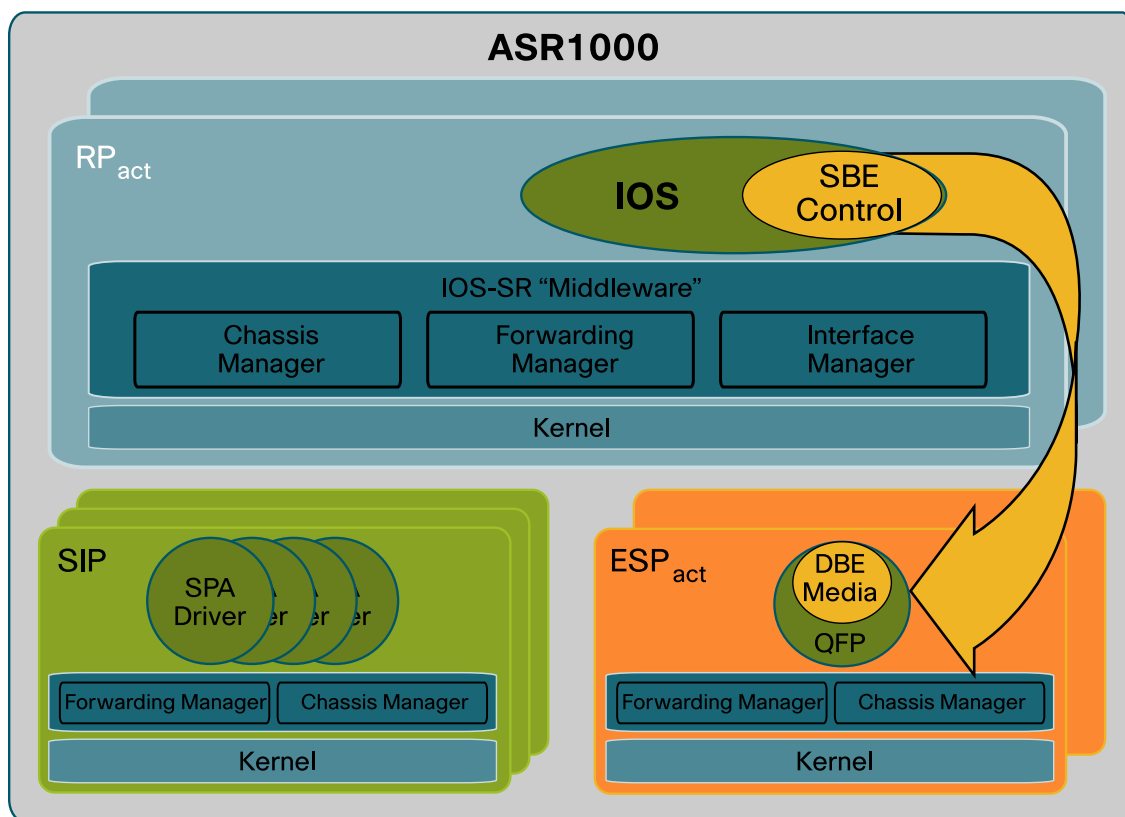## Cisco ASR 1000 Series Implementation of Cisco Unified Border Element (SP Edition) Unified Model

As mentioned before with Cisco Unified Border Element (SP Edition) Unified model, both the SBE and DBE reside on the same system.

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 SBE control module is resides on RP, and the DBE control module resides on ESP. The SBE and DBE interact using ASR 1000 internal control communication bus, as shown in Figure 7.

The function of the route processor is to process SIP/H.323 signaling packets arriving from the endpoints and use the per-session policy defined in configuration 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 SPA to the Cisco QuantumFlow Processor, it checks and determines whether they are

signaling packets or any regular media packets. If it is a signaling packet then it punts to route processor for further processing. On processing the signaling packets the RP instructs ESP to open a media pinhole for that session. And if the incoming packets are regular media packets for a defined media pinhole, then ESP processes them based on defined per session policies.

Figure 7. ASR 1000 Architecture

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.

Cisco Unified Border Element (SP Edition) Features

As discussed, Cisco Unified Border Element (SP Edition) is a toolkit of functionalities and one can enable them to meet their design criteria. The Cisco Unified Border Element (SP Edition) Unified model implements both signaling and media features in a system to meet the requirements of topology hiding, signaling interworking, QoS, CAC, security, billing/CDR, and high availability. More details on these functionalities are described below.

Signaling Interworking (Network Interoperability)

ASR 1000 Cisco Unified Border Element (SP Edition) Unified model operates in back-to-back user agent (B2BUA) mode, and that means that incoming call signaling gets terminated and reoriginated on terminating side. That way topology hiding functionality is achieved by separating incoming and outgoing sessions. On media side, ASR 1000 Cisco Unified Border Element (SP Edition) modifies just the headers and apply policies while forwarding RTP payload without modification.

ASR 1000 Cisco Unified Border Element (SP Edition) Unified model currently supports SIP signaling interworking. It also supports different types of interworking such as delayed offer to early offer for SIP sessions. This particular

functionality is useful with Cisco Unified CallManager, which initiates the call with delayed offer and later on it negotiates the SDP capabilities, but many of the third-party endpoint and SIP trunk providers expect SDP with initial invites. Beside that ASR 1000 Cisco Unified Border Element (SP Edition) also supports REFER, Re-INVITE, SIP-INFO, and other messages so that it can successfully support supplementary services such as Call-hold, MOH, forward, and transfer functionalities.

In SIP services, registration is very important as it can flood the system in case of some services interruption. ASR 1000 supports different types of registrations mechanism such as registration pass-through with different timing to protect core side registrar-server. It also supports fast registration where ASR 1000 WFP plays an active role in protecting route processor from overloading. Here the first registration message is executed properly with RP, but then it creates cache copy with ESP module so that any further registration update coming from user-side can be processed at QFP level and that way protecting from extra load on RP. Beside that ASR 1000 Cisco Unified Border Element (SP Edition) also supports delegated registration where it sends registration on behalf of endpoint.

Beside all this functionality, SIP is still an open standard and various manufacturers implement SIP functionality differently. To make it all compatible and interoperable Cisco Unified Border Element (SP Edition) has functionality of header manipulation. With this functionality Cisco Unified Border Element (SP Edition) can manipulate any message by adding, modifying, or removing any optional part of the messages.

Media Interworking

On media interworking side, as mentioned before, ASR 1000 Cisco Unified Border Element (SP Edition) just modifies the header information to protect the IP addresses of the different domain and apply policies. The actual media is forwarded without any modifications.

ASR 1000 Cisco Unified Border Element (SP Edition) supports RTP/RTCP traffic and pass-through of encrypted SRTP traffic. It also supports various types of voice and video codecs. On DTMF support side, it supports pass-through and interworking of different types: In-band (RFC2833) and Out-of-band (SIP-notify and SIP-info) methods.

NAT Traversal

One of the important functions of Cisco Unified Border Element (SP Edition) is to enable the access to the SIP devices across NAT and FW devices. Firewall with ALG functionality is able to open signaling and media stream for SIP calls, but it has difficulties in media allowing for incoming calls. The SBC performs translation of IP addresses and port numbers (through Network Address and Port Translation, or NAPT) in both directions.

Billing /CDR

Another important function of Cisco Unified Border Element (SP Edition) Unified model is able to generate reliable call detail records for billing purposes. ASR 1000 Cisco Unified Border Element (SP Edition) Unified model implementation supports PacketCable 1.5 Event Messages Specification compliant billing methods. ASR 1004 and ASR 1006 Platforms also support storing of the billing records on the local hard disk if the billing server is not reachable.

Security

Since ASR 1000 Cisco Unified Border Element (SP Edition) Unified model sits at the edge of the domain, security becomes a very important function. The enterprise or SP user wants its service to be secure and reliable from different attacks and unscrupulous users. To achieve higher security ASR 1000 Cisco Unified Border Element (SP Edition) Unified model has different types of security functionality which can be enabled as needed.

From a Cisco IOS® Software point of view, it supports different types of DoS attack protection. SBC functionality run under Cisco IOS Software, so all the security functions of Cisco IOS Software are also available to SBC and that makes ASR 1000 Unified SBC environment much more secure.

Cisco Unified Border Element (SP Edition) also supports incoming call authentication, encryption at signaling using TLS and media level with secure RTP. It also supports call routing between two different VPN domains (multi-vrf).

ASR 1000 Cisco Unified Border Element (SP Edition) also supports black and white listing to protect what kind of messages it should receive and what kind of messages it should forward to other legs of the session.

Along with this functionalities, Cisco Unified Border Element (SP Edition) also provides topology hiding, protects against malformed packets, policing per session flow to check for bandwidth protection, and source address filtering. All these functionalities increase security and protect the domains while connecting to the external devices.

Call Admission Control/Quality of Service

ASR 1000 Cisco Unified Border Element (SP Edition) supports different CAC methods to control sessions. It is in a unique position in the network to control the end-user communication and enforce defined service level agreements (SLA).

Cisco Unified Border Element (SP Edition) can monitor the active calls and bandwidths used per call. It can also police the media flowing through a call and reject the packets if the limits are exceeded.

It can monitor and remark the signaling and media packets with different DSCP and TOS marking. This helps ensure that user data will be prioritized compared to other types of traffic. This way Cisco Unified Border Element (SP Edition) helps in providing stable and quality service as defined by SLAs.

Regulatory Compliance

Service provider customer has requirement of Lawful Intercept (LI) functionality, and since ASR 1000 Cisco Unified Border Element (SP Edition) sits at the edge, it is in an ideal position to tap the traffic if required. ASR 1000 platform supports LI based on SII model and can tap traffic of an ongoing session with the help of a mediation device.

High Availability

ASR 1000 Cisco Unified Border Element (SP Edition) supports high-availability features such as stateful switchover (SSO) and In-service software upgrade (ISSU). Established voice calls are successfully switched over in case of internal hardware or software failures.

The Cisco ASR 1000 Series 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) has redundancy support for 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. On the Cisco ASR 1002 and Cisco ASR 1004 Routers, a standby Cisco IOS Software process is running on the same route processor as the active Cisco IOS Software process. In the event of a Cisco IOS Software failure, the router switches to the standby Cisco IOS Software process. No redundant route processor or redundant ESP is available on the Cisco ASR 1002 Series and Cisco ASR 1004 Series Routers.

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

The Cisco ASR 1000 series routers also support In-service software upgrade (ISSU), and with that support the routers can upgrade specific software components (referred to as subpackages) within a software consolidated package. For example, the route-processor subpackage can be upgraded without affecting the other subpackages and without affecting ongoing services.

Primary Features

Signaling and Control	
- RFC 3261 – SIP - RFC 3264 – Offer/Answer Model - RFC 2976 - SIP Info - RFC 3262 - PRACK - RFC 3326 – Reason Header - RFC 3428 – Extn SIP messaging - RFC 3892 – Refer-by Mechanism - Supplementary Services - Call-hold - Call-hold-advance (MOH) - Call-forward (3xx Support) - Call-transfer - MWI (Message Waiting Indicator) - SIP header and Value Manipulation - SIP registration - HTTP digest authentication - Fast registration - Soft switch shielding	- Support TCP/UDP and interoperability - Diversion header support - Different header field Manipulation - Option tag "timer" in INVITE - Session-expire header - Min-SE header - Join header - SIP Date header - Support 100Rel header - Support dynamic route selection across multiple trunks - Delayed Offer – Early Offer support - SIP profile and message Normalizations - Caller-ID and Calling-name delivery - Support TEL/SIP URI

Media Interworking	
- Media packet Updates - Support different types DTMF - RFC 2833 - SIP INFO - SIP notify - DTMF Interworking - RTCP processing	- Support Media Relay - Support pool of Media IP addresses/ports - Fax/Modem Pass-through - Support Voice/Video Codecs - Support SRTP Pass-through - Media Bypass support

NAT Traversal

- Topology Hiding – Network Address and Port Traversal (NAPT).
- SBC will know that a signaling packet has traversed through NAT/NAPT/FW by examining IP layer address and Application (SIP, H.323) layer address. If both addresses are not the same, then the packet has gone through NAT/NAPT/FW.
- SBC programs and keep tracks of ingress-egress address/port mapping.
  - Define IP address and port assignment scheme for Address Mapping and Media Relay in DBE.
  - Define Table Lookup/Storage functionality/data structure for relay addresses allocated by DBE for active sessions.
  - Define Media Relay programming.

Billing/CDR	
- Call Detail Record (CDR) support - CDR report RADIUS Server	- Multiple RADIUS servers support 24 hours CDR buffering

CAC/QoS Support	
- CAC mechanism - Limits on the number of concurrent calls and registrations - Restrict the media bandwidth dedicated to active calls - Control load on network elements by rate limiting - Completely block (blacklist), or freely allow (whitelist) events with certain attributes - Monitor overall system memory usage, and block all events while the system is experiencing a critical resource shortage - Help ensure customers operate within the bounds of their SLAs	- DSCP and TOS marking - Configurable Rate limiting - Bypass admission Control for Emergency Calls - Policing and Marking for the Media packets - Per Session policing

Security	
- DoS - Guard again DoS attack at signaling level - Alert for packets from unknown source address - End point authentication - Support TLS for signaling encryption - Support SRTP	- Support multi-VRF support - Support DTLS for SIP signaling - Support for SIP authentication - Static Black-listing - Access-list configuration - Dynamic Black-listing

High Availability	

• Intra-chassis redundancy
    ○ RP (Route Processor) Switchover no Data loss
    ○ ESP (Enhanced Services Processor) Switchover with in-flight data loss
	• Stateful Switchover (SSO)
	• In-service Software Upgrade (ISSU) support

Summary

The rapid proliferation of emerging VoIP technologies requires different networks of service providers, enterprises, and residential end users to interconnect to increase efficiency and productivity. Cisco Unified Border Element (SP Edition) is the right device which provides all the required functionality to meet service provider and enterprise needs cost effectively. With the power of ASR 1000 series router, the integrated Cisco Unified Border Element (SP Edition) functionality can perform at a very high level to meet the Service providers and large enterprise scaling requirements. In addition, it provides higher redundancy of routing and embedded services processors so that service providers and large enterprise gets nonstop VoIP service.

Why Cisco?

Cisco is the worldwide leader in networking and VoIP technologies. Cisco Unified Border Element (SP Edition) provides an SBC solution with ASR 1000 series router. Other advantages are:

- No need for another appliance for SBC functionality
- Reduces Capital expenses (CapEx) and operating expenditures (OpEx) for Service providers and Enterprise users.
- Unified Border Element (SP Edition) is based on highly scalable and modular ASR 1000 series routers with advance forwarding engine based on Quantum Flow Processor.
- Since Unified Border Element (SP Edition) 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.
- ASR 1000 series router provides high availability with stateful switchover and that is very critical for voice applications.

For More Information

For more information about the Cisco Unified Border Element (SP Edition) SBC functionality and the Cisco ASR 1000 Series Aggregation Services Routers, visit:

- Cisco ASR 1000 Series Session Border Controller data sheet: http://www.cisco.com /go/asr1000
- ASR 1000 Series: Managed Services Whitepaper: http://wwwin.cisco.com/sptg/erbu/products/asr1000/files/asr_ms_tech_wp.pdf
- VoIP information: http://www.packetizer.com/
- SIP: http://www.cs.columbia.edu/sip/

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.

Printed in USA   C11-540690-00   05/09