Dialogic®

White Paper

# Session Border Controllers: Rationalizing the Border of the Network

## Executive Summary:

As service providers transform their networks more and more to IP, they are taking on a new role that involves the orchestration of applications and content from multiple participants in the service delivery supply chain. This translates into multiple networks - both internal and external to service providers - for providing end-to-end services to customers. The multiplying capabilities and expanding capacities of Session Border Controllers (SBCs) have become central to this evolution to IP-to-IP interworking and can help service providers as they endeavor to improve performance and cope successfully with spiraling traffic volumes and complexity.

From once being looked upon as primarily a security device, SBCs have taken on an expanded role for fostering successful connectivity and providing high quality IP service. They can provide vital support for SIP normalization, QoS, NAT traversal, IPv4-IPv6 interworking and support for a host of value added services, and much more.

## Table of Contents

## Introduction: Today's Real-World Networking Environment

Today's communications networking environment is rapidly changing, complex and highly nuanced. IP has become the new transport methodology for delivering voice services while converged applications are growing rapidly and video is expanding at rates often called "exponential." More and more IP networks are being installed and used as core networks, and until recently, these were considered "adjunct" networks connected to "core" time division multiplexing (TDM) networks through gateways. However, these core IP networks are now increasingly being used today as the primary service delivery network.

While the world is inarguably moving more and more towards an all-IP infrastructure, the global communications scene will still include a large TDM component into the foreseeable future. So "all-IP" networks will still need to interconnect with existing TDM networks. In the real (vs. the ideal) world in which service providers and enterprises have to operate on a day-to-day basis, this means there will be service delivery challenges encountered in making these disparate networks work well together. This will place a premium on technology solution providers, experienced in connecting IP with legacy TDM networks, who thoroughly know, understand and appreciate both sides of this mixed communications world, and who can develop solutions that can serve the broadest range of networking options while at the same time support a wide range of multimedia IP-based services.

Indeed, service providers today look for solutions that provide a broad set of capabilities that enable both IP and TDM networks. The migration to an all-IP network architecture in service provider networks is proceeding with increased momentum around the globe. A new set of requirements relating to end-to-end service integrity, network security, and application support has emerged due to the blended nature of services being offered today that may involve multiple participants in the service delivery supply chain in order to connect customers and content. The Session Border Controller (SBC) is a being counted upon as a critical component to meet these requirements. SBCs not only provide functionality at the borders between network environments to support baseline voice services, but they also enable and support a host of new IP-based services and applications, including high-definition (HD) voice and real-time video communications.

## The Session Border Controller: Standing Guard in IP Networks

From a market validation perspective, service providers and enterprise network operators alike recognize the value SBCs can provide as they transform their networks to all-IP. With the worldwide explosion in IP networking, the global adoption of SBCs is fast-growing and highly dynamic.

### Benefits to Service Providers

When an IP network interacts with another network, equipment is put in place at the border of both networks to insulate each network and provide security. At the same time, the equipment must allow for interoperability between diverse network elements, signaling protocols and their variants, and media types that, in essence, help rationalize and integrate the connectivity between networks. The SBC, counted upon in many ways with regard to IP-to-IP interconnection, sits at demarcation points between the networks, providing a wide range of important functions for security, protocol translation, normalization and call handling, among other things. An SBC enables seamless communication between different service provider networks and end-user networks that are comprised of elements from a heterogeneous array of equipment manufacturers.

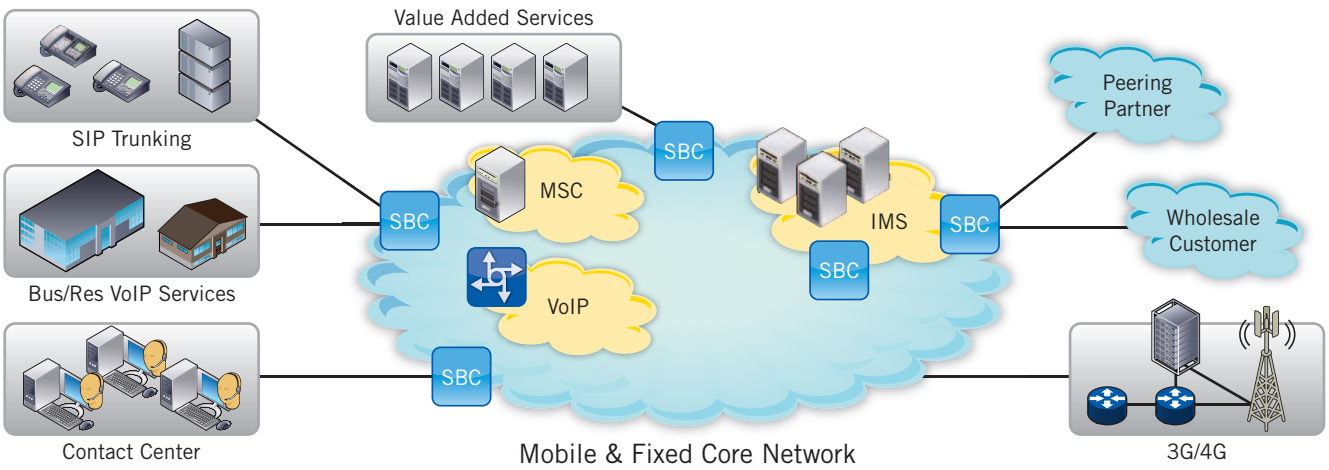


*Figure 1: Diagram showing potential SBC demarcation points in mobile and fixed networks*

While the specific capabilities of different SBCs vary by application, their role and functionality have expanded well beyond security as the importance and complexity of IP networking has increased. The SBC has evolved into an intermediary network device with an increasingly comprehensive range of functions capable of facilitating high-quality IP service delivery.

SBCs can help network operators manage calls, regulate data flows, fix or change protocols and syntax, and overcome obstacles that Network Address Translation (NAT) devices and firewalls may pose for IP calling. In addition, where SBCs are inspecting the sessions – both media and control traffic – as they are entering the network, they are also able to play a major role in maintaining high availability by helping to mitigate potential system failures and network overloads that can result when networks are confronted by Denial of Service (DoS) attacks.

### Benefits to Enterprises

A longstanding fundamental benefit of SBCs is to secure organizational assets by protecting the network it is guarding from harm. SBCs also can facilitate optimization of interoperability between service providers and end-users, while at the same time maintaining service quality. Another notable benefit is that SBCs can help expand the options enterprise organizations have when it comes to considering choices for communications equipment and solutions; for example, a premise based IP PBX or hosted solution. Insofar as an SBC compensates for or corrects potential incompatibility issues, customers have a wide variety of services and service providers to select from, and thus might no longer need to give primary attention to factors such as compatibility that in the past may have limited their communications options. As a result, SBCs allow for enterprises to be flexible in terms of taking a "best of breed approach" when choosing a platform or solution that most fits their needs, and helps to remove or minimize the limitations or restrictions imposed by one service provider versus another. In addition, while SBCs deployed within service provider networks provide infrastructure protection for the operator, those deployed at the enterprise edge provide protection against malicious attacks for enterprise networks.

## SBCs: What and Why

The growth in IP traffic, driven to a large extent by video, has continued to push more and more IP "sessions" through SBCs, promoting larger-capacity and higher-performance devices, and separate load-balancing systems. The contemporary SBC, or at least its media control element - the Border Gateway Function (BGF) - can be seen as an IP "gateway" connecting IP networks with each other. It performs functions analogous to traditional media gateways that bridge IP and TDM-based networks.

Historically, SBCs have been deployed to secure organizational assets. With the transformation of service provider networks to IP, and the demand for new and innovative services that combine voice, video and data, in many cases from different content providers, the roles of SBCs are expanding in service provider networks. In the networks of today where IP and TDM infrastructures need to operate seamlessly, SBCs provide an array of critical functionality that can be categorized into the following four general areas:

- Security
- Multimedia connectivity
- Service assurance and optimization
- Border management

In addition, due to the strategic location of SBCs in the network, service providers are leveraging SBCs to help address regulations such as emergency call prioritization and lawful intercept. More detailed examples of SBC functionality are described below.

## Security

In terms of security (arguably still an SBC's most basic role), SBCs are designed to insulate IP networks or network portions from potential problems in other networks with which they are connected. SBCs typically provide call filtering and protection to the network and other infrastructure platforms against malicious attacks and toll fraud, as well as encryption and protection against malformed packets. An SBC's position at the network border makes it well suited to provide topology hiding, which prevents outsiders from accessing internal information and viewing private communications infrastructure configurations in a detailed way (potentially to identify servers for attack).

SBC security functions include:

- Denial or admission of access by address, network and/or other characteristics
- Authentication (including prevention of "spoofing" by malicious users)
- Limiting traffic - by the number of calls and the rate at which calls are received - to prevent network overload
- Encryption - to keep transmitted content secure
- Detection and rejection of malformed SIP and H.323 signaling messages

While these SBC security capabilities have allowed service providers to begin to directly interconnect their IP islands, situations where some parts of the service provider network are transforming to IP at a faster pace than others will call for additional SBC capabilities to better rationalize real world network border situations.

SBCs are often counted upon primarily – if not entirely - for providing security for VoIP (i.e., SIP and H.323 based services), but not as much for supporting for SS7-based applications. The legacy circuit-switched network is still here and poised to remain a fixture for many years, which means service providers will continually seek to leverage their investment in SS7/Intelligent Network (IN) based services. This implies that in addition to supporting VoIP, service providers will need to provide equivalent security for applications that are actually SS7-based but carried in next generation signaling protocols like SIP (e.g., SIP-I).

SBCs typically focus on syntactical checking of VoIP messages. This is concerning, since as hackers get more sophisticated, it stands to reason that security attacks will increasingly be based on semantic - not syntactical - holes. SBCs also do not provide security for web-services based applications. While session control protocols like SIP and H.323 are important for enabling VoIP services, service providers today are increasingly focused on services that rely directly on web-services protocols (e.g., HTTP, MSRP and XCAP). Once a user establishes a session with an application server, SBCs treat web-services protocols as media (i.e. transparently), passing them directly into the core. To address this, service providers overlay another security layer around their application services, which in turn can further add complexity and cost to their networks.

## Multimedia Connectivity

Connecting diverse IP networks requires more than just compensating for differences in signaling behavior. Transcoding voice and video codecs is also gaining importance, especially due to the continual growth of video as a component of overall IP traffic. To facilitate connectivity from a multimedia perspective, SBCs can provide both "normalization" and transcoding capabilities.

Normalization is used to accommodate the differences between various SIP versions or implementations by manipulating the SIP headers and messages. Often, one (sending) service provider will put something on the network that is "illegal" from the perspective of another (receiving) service provider's internal networking logic or syntactic rules. It may, for example, use a frame "tag" in a manner not acceptable to or readable by the other. Allowing such traffic to cross the threshold between providers without being "normalized" can potentially risk call failure and prevent effective peering. Since not every softswitch, PBX and SIP proxy has implemented the exact same subset of specifications or even a given specification in exactly the same way, IP network interoperability creates extensive requirements for SIP normalization.

Also, connectivity may require an SBC to enable interworking between different IP network layer variants as well as protocol translation between SIP and H.323, and support for VPN connectivity.

One notable function of an SBC beyond security is allowing NAT traversal and firewall access for real-time IP traffic. Without this feature implemented, incoming IP calls typically would be dropped. NAT traversal is of growing importance as organizations are increasingly distributed rather than being concentrated at central locations. The NAT'ing function allows interworking between private and public networks and communication across protective firewalls, albeit on a limited basis. The SBC is counted upon, among other things, to maintain caller information to appropriately refresh firewall "pinholes" that allow entry of external IP calls.

SBCs need to provide, depending on the application, transcoding between different media codecs (for example, G.711 and G.729). Other multimedia related capabilities include detecting and interworking in-band Dual Tone Multi-Frequency (DTMF) tones, adjusting for different packetization periods and silence suppression techniques along with providing support for T.38- based faxing. With the proliferation of video-based applications, there is also a need to support transcoding for video services or combinatorial services that involve video and voice as well as data.

## Service Assurance and Optimization

Assurance of both service quality and availability is also something that service providers are called upon to be able to provide to their customers. SBCs typically provide service assurance through a combination of call admission control and quality of service features. This combination includes the use of layer 3 (IP) and layer 5 (SIP) access control lists to prioritize media flows by mapping them to appropriate service levels through IP header bit marking and VLAN mapping. In addition, SBCs can also provide network overload and failure detection and attempt to re-route traffic through alternate routes if they detect a far-end problem. Some SBCs also provide Service Level Agreement (SLA) verification. Media bridging, meanwhile, is a separate function for making sure that various media formats are handled appropriately.

From an architectural standpoint, SBCs can provide a set of services at the border to help optimize and assure service performance on both ingress traffic into the core network as well as egress traffic going to other peering networks. For example, SBCs can load balance traffic coming into the core network from a peering partner and even reroute traffic in the event of a failure situation for a given internal endpoint. On egress traffic, SBCs can load balance sessions to multiple peering partner servers as well as redirect traffic to a primary or secondary server if there is a failure at the far end. By load balancing traffic, SBCs can help optimize overall network and service performance as well as assure service continuity in the event of proxy or server failure.

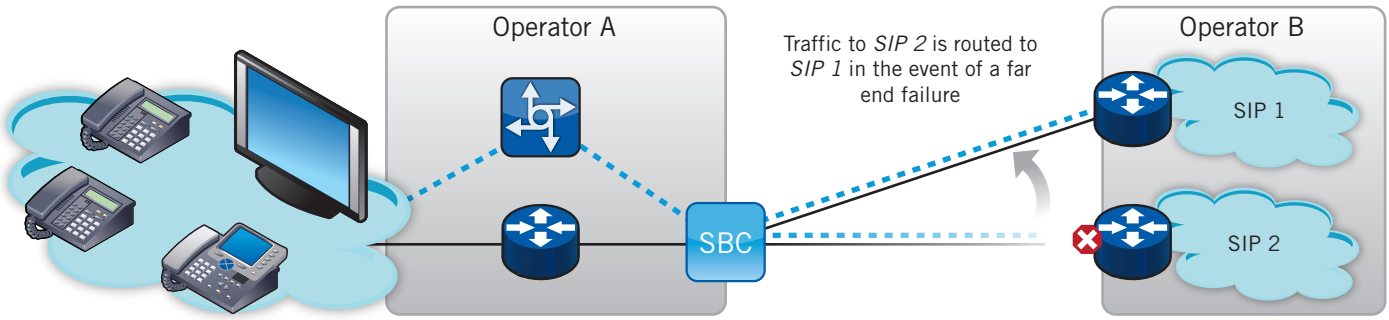


*Figure 2: Diagram showing how SBCs can provide a set of services at the border to help balance traffic loads and assure service performance on both ingress traffic into the core network, as well as egress traffic going to other peering networks. In the event of a far end failure, an SBC can help assure end-to-end service continuity for customer traffic.*

However, SBCs do not have access to the real-time network-wide knowledge required to make optimal routing decisions to avoid congestion and far-end failures. This is because many SBCs function as Back-to-Back User Agents (B2BUAs) whereby a network of SBCs inherently makes routing decisions on a hop-by-hop basis rather than globally, which in turn can lead to sub-optimal routing decisions and increased call failure rates.

In addition, some SBCs can sub-optimally use transcoders, which can cause significant degradation in voice quality. Because a local SBC might not reliably know what the ultimate destination codec will be, some SBC vendors suggest transcoding all incoming media streams to a single network-wide codec. In many cases, such a deployment can result in low end-to-end voice quality due to repetitive (and perhaps unnecessary) transcoding.

As service providers are faced with more aggressive competition, they can find themselves under increasing pressure to minimize their end-to-end service costs. In response, they may opt to implement a network architecture that drives end-to-end and not local cost minimization, e.g., real-time network-wide least cost routing. Service providers also may choose to limit the number of signaling resources required to properly route each session request and minimize the use of media intensive resources (e.g., codecs). However, because traffic patterns and applications are dynamic and change over time, the ability to scale signaling and media resources is seen by many as critical.

## Border Management

Service providers look for solutions that enable them to drive down the total cost of operations and support. Since SBCs sit at the border between peering networks as well as provide connectivity between different domains within a service provider's network (such as between the session control layer and services layer), they are well suited to provide management capabilities from a configuration and reporting perspective. Beyond being able to help assure service performance and enforce policy, as the number of network peering partners increase and the array of multimedia services broaden, SBCs will be counted upon to provide the appropriate tools to streamline and automate the process of managing the sessions and connections as well.

SBCs provide a demarcation between internal and external networks that can effectively help isolate user experience issues to a particular network domain. This in turn can help reduce the time to isolate and resolve issues affecting service performance. Also, understanding signaling and media performance from network peers can be used to identify events and trends that impact user experience. This visibility into signaling and media performance can provide intelligence on overall service performance that can be used for optimization purposes, and on utilization and capacity to help allocate capital expenditures for transport and equipment expansions.

In next generation networks where service providers manage hundreds to thousands of end points that they connect with on a per SBC basis, managing network additions and configuration changes can become administratively burdensome when using traditional command line based tools. SBCs that provide tools to streamline and automate configuration changes and new peering endpoints can help service providers prepare to take on their emerging role as an orchestrator of combinatorial services that rely on resources and applications from multiple partners in the service delivery supply chain.

### Governmental and Regulatory Support

Service providers, both legacy TDM and IP, are required to support a wide range of regulatory requirements. For example, United States service providers need to enable lawful intercept of messages as provided for under Communications Assistance for Law Enforcement Act (CALEA). In addition, they need to ensure that emergency calls such as E911 or Government Emergency Telecommunications Service (GETS) are always provided priority service and not blocked. The role that SBCs have in IP networks and their ability to prioritize sessions make them a logical platform to help support such initiatives.

## Network Scenarios: How SBCs Are Used

Traditionally for service providers, there were two general "use cases" for an SBC:

- As an "interconnect" device located at the "peering" border, or Network-to-Network Interface (NNI), between interconnecting carrier networks
- As an "access" device, in which the SBC protects the edge of a service provider network and provides SIP trunking to an enterprise

The functionality and capacity requirements for an access SBC are typically different compared to an SBC used for peering purposes. Moreover, for access applications, the SBC, while located in the service provider's cloud, may be described notionally as located between the provider and customer networks.

However, other applications are emerging that leverage the transformation, security and connection capabilities that SBCs provide. Some of these applications include:

**Value Added Services:** In today's increasingly complex and competitive communications marketplace, it is not uncommon for some service providers to have much of their revenue attributed to a variety of Value Added Services (VAS). These services refer to advanced and/or additional revenue generating applications a service provider offers to help them remain competitive and differentiate their offerings. These services can include text messaging, enhanced TV, video conferencing and video on demand, m-commerce, tele-shopping, voice and video mail, Internet access, communal gaming, interactive advertising and subscription gaming. SBCs deployed in VAS applications can be instrumental in helping service providers accelerate the time to market for such services, and in turn can contribute to a service provider's top-line revenue.

**VPNs:** A service provider may use an SBC in offering VPN services to customers to bridge calls across customer VPN sites. This can allow VoIP calls (and other IP transmission) between customers in different VPNs that are provided by the same service provider. The SBC in the service provider network is then configured to be a member of each VPN and thus routable to each.

**IP Multimedia Subsystem (IMS):** In IMS networks, SBCs can provide call session control and border gateway functions at both NNIs (carrier-to-carrier connections) and UNIs (carrier-to-customer connections). While IMS relies on SIP as the primary session control protocol, there are extensions in the applicable architecture standards (for example 3GPP) that SBCs will need to support. Access control, interworking, policy enforcement, DoS protection and topology hiding capabilities of SBCs make them well suited for use in the IMS architecture.

One application for SBCs is to serve as the Proxy Call Session Control Function (or P-CSCF) element, which serves as the connection between the subscriber and the IMS network as well as between a "trusted" network in which a mobile customer is roaming and the subscriber's "home" network. Other functional elements in the IMS responsible for activities like media control and NAT traversal can also be incorporated in the SBC. On the peering side of the IMS architecture that defines the functions required for interconnection to other networks, SBCs can be tasked to provide the Interconnect Border Control Function (I-BCF) along with the Interconnect Border Gateway Function (I-BGF) to support session control and media connectivity respectively.

**Enterprise applications:** As stated above, an SBC can facilitate interoperability among service provider networks and enterprise equipment, providing the enterprise customer with the flexibility to choose "best-of-breed" solutions that enable them to also take advantage of innovative service provider applications.

Additionally, enterprises may seek to utilize SBCs on their own LANs, in front of an IP PBX or other IP switch. The SBCs are often used along with firewalls and other Intrusion Prevention Systems (IPS) to facilitate VoIP calling to and from their own networks while providing network protection. Alternatively, enterprises may opt to use an SBC in conjunction with SIP trunks to provide call control and make routing and policy decisions on how calls are routed across networks. Routing traffic through internal IP networks in preference to riding the PSTN can pave the way for large cost savings opportunities for enterprises.

## What to Consider When Choosing an SBC

There are a number of important considerations for a service provider when choosing an SBC for its network. This includes taking into account the desire to have sufficient capacity in a compact form factor as well as the availability of high-performance features that can support high-volume demands. For service providers looking to deploy an SBC in a network evolving towards IP, they may want to consider a solution that has been designed from the ground up for a pure IP network environment.

SBC capabilities differ, which benefits the wide array of settings in which SBCs are used; for example, requirements from a peering or access perspective can differ from the capabilities required to support multimedia value added service delivery. Moreover, depending on the situation, an SBC can be called upon to provide either access specific functionality or peering functionality or, in the case of enabling value added service support, any-to-any service connectivity including legacy SS7 and SIGTRAN. Regardless, SBCs built for access, peering or business services applications have some basic connectivity, security and service assurance features in common.

Although security capabilities are important in service provider SBCs as well as enterprise-focused SBCs, scalability requirements can differ – often widely - in these settings. For enterprise environments, SBCs should be able to scale up, but also to scale down. This is important for service providers so that they can deploy a cost effective platform at the customer premise to deliver advanced business services to a wide range of companies.

Other points to consider when evaluating SBC solutions include:

- Integration with existing softswitch infrastructure
- Ease-of-use and automation tools for provisioning, SIP normalization, and management activities involving peering partners
- Any-to-any service connectivity for value added services

Since, in many cases, SBCs and softswitch solutions are separate network elements with different functionality, deployment of SBCs could require service providers to develop and use complex administrative processes to manage their networks. SBCs that integrate seamlessly with existing softswitch implementations can help address much of this complexity from an administrative perspective. Tight integration can help reduce on-going operational complexity and costs through the use of flow-through provisioning and consolidated accounting, alarming and reporting and end-to-end session tracing, which helps enable faster troubleshooting if issues do arise. Alternatively, by supporting an industry

standard Management Information Base (MIB), an SBC can integrate effectively with a service provider's 3rd party management tools that can help them leverage their existing investments in Operational Support Systems (OSS) and better enable operational consistency in the organization.

For the many service provider customers already using a softswitch and seeking to add the security and other networking capabilities of an SBC, some SBCs can help reduce accompanying changes in device configuration creating a "drop the box in" deployment situation. As a result, billing, records, and routing information already in place in the softswitch stay in place without disturbance.

Service providers are looking to automate and streamline many of the operational tasks that can be repetitive, error prone and time consuming, as there can be thousands of different end points to manage on a per SBC basis, not to mention the numerous subscribers from an access perspective. Thus, SBCs are called upon to provide capabilities to automate and streamline the border management functions. This can be done through web-based management dashboards or XML-based scripting not only to help reduce configuration errors, but also to enable integration with third party Operational Support Systems (OSS) which can help free up highly trained technical personnel for more value added tasks.

Since SBCs mediate traffic between different network borders, they are in an excellent position to monitor and collect information on session and service performance. SBCs can provide a rich set of performance and usage intelligence to help service providers better understand network trends and identify emerging issues with peering and access networks before they escalate into larger scale issues. SBCs that can provide reporting and alerts on service and system performance can help service providers manage user experience and move towards a proactive approach of addressing capacity issues with the services they deliver to their customers and peering partners.

Value added services include applications such as high definition voice, multi-media messaging, voice and video mail and location-based services. Service providers are looking to be able to offer these services across multiple access methodologies and devices, so solutions that help them deliver services across both IP and TDM domains, including those delivered to 2G and 3G mobile customers, can help them be capable of reaching more users. SBC solutions that incorporate media transcoding and IP signal interworking for application platforms on which service providers have chosen to develop and deliver mobile value added services can help improve service velocity and address top line revenue opportunities.

## Conclusion

As service providers transform their networks more and more to IP, they are taking on a new role that involves the orchestration of applications and content from multiple participants in the service delivery supply chain. This translates into multiple networks - both internal and external to service providers - for providing end-to-end services to customers. The multiplying capabilities and expanding capacities of session border controllers have become central to this evolution to IP-to-IP interworking and can help service providers as they endeavor to improve performance and cope successfully with spiraling traffic volumes and complexity.

From once being looked upon as primarily a security device, SBCs have taken on an expanded role for fostering successful connectivity and providing high quality IP service. They can provide vital support for SIP normalization, QoS, NAT traversal, IPv4-IPv6 interworking and support for a host of value added services, and much more.

As service providers around the globe migrate towards all-IP, the worldwide networking environment remains mixed, with major TDM-based elements playing a large role well into the future. In such a mixed network environment, media transcoding and signaling interworking take on considerable importance, and in this regard, not all SBCs are created equal. This consideration places emphasis on platform providers with skills and expertise in the delivery of multimedia services and the ability to negotiate this complex heterogeneous environment of diverse network elements and technology domains.

**www.dialogic.com**

**Dialogic Inc**
1504 McCarthy Boulevard
Milpitas, California 95035-7405
USA



04/12 13218-01