

White Paper

SIP Trunking: Deployment Considerations at the Network Edge

SIP Trunking: Deployment Considerations at the Network Edge

White Paper

Executive Summary

The move to Voice over IP (VoIP) and Fax over IP (FoIP) in the enterprise has, until relatively recently, been focused on communication within the private enterprise network. Now, some enterprises are using SIP trunks provided by Internet Telephony Service Providers (ITSPs) to connect their internal networks to external, public IP networks. SIP trunking is one of the first steps in an enterprise's PSTN to VoIP transition, and it enjoys broad availability from service providers in many regions, including many incumbent PSTN service providers.

Adopting a SIP trunking service is not a simple process. In fact, many enterprises need support and guidance as they move to SIP trunking. Enterprises need a way to connect their existing voice infrastructure to SIP trunks without making major changes to their existing voice or data infrastructures. In addition, to provide the necessary protections for the enterprise, there needs to be a mechanism for implementing Network Address Translation (NAT) and firewall traversal, SIP interoperability, and network edge security; as well as a mechanism for providing a clear demarcation point or boundary for real-time IP communication services at the enterprise edge between the external and internal IP networks.

This paper provides an overview of SIP trunking and the benefits it can bring to the enterprise. It also provides information about how to address issues at the enterprise network edge when deploying a SIP trunking service.

Table of Contents

Introduction	2
Significant Cost Savings.	2
Increased Provisioning Flexibility	2
SIP Trunking Challenges for the Enterprise	2
Network Address Translation and Firewall Traversal Issues.	2
SIP Interoperability Issues	3
Network Edge Security Issues	3
Network Demarcation Issues	4
Legacy PBX Infrastructure Issues	4
Fax over IP Issues	5
Defining and Securing the Enterprise Network Edge for SIP Trunking	5
Using an Enterprise Border Element to Facilitate a SIP Trunking Service	6
TDM or Hybrid PBX Support	6
IP-PBX Support.	7
Future Options.	7
Unified Communications and Multimedia	8
High Definition Voice	8
Network Monitoring.	8
Dialogic® Products that Provide Border Element Functionality	8
Dialogic® BorderNet™ 500 Enterprise Session Border Controller	8
Dialogic® IMG 1010 Integrated Media Gateway.	9
Summary	9
Acronyms	10
For More Information	11

Introduction

SIP Trunking is a real-time IP communications service delivered by an Internet Telephony Service Provider (ITSP) that allows enterprises to route inbound and outbound voice and fax traffic over a broadband data service using the Session Initiation Protocol (SIP), Real-Time Transport Protocol (RTP), and Fax over IP (FoIP) protocol known as T.38. As an access alternative to the traditional Public Switched Telephone Network (PSTN), SIP trunking extends VoIP and FoIP connectivity beyond the enterprise network edge.

A SIP trunk is primarily implemented as a set of concurrent call sessions routed over the IP backbone of an Internet Service Provider (ISP) by an ITSP. The ISP and ITSP may be one and the same, or an ITSP may leverage third-party ISP IP backbones and enterprise broadband connections to deliver the SIP trunking service. Because SIP trunking enables an enterprise to use the same IP connection for voice, fax, and data communications, it can yield significant cost savings compared to TDM trunking. SIP trunking also offers more provisioning flexibility than TDM trunking.

Significant Cost Savings

Most of the installed base of TDM PBXs, hybrid PBXs, and IP-PBXs is provisioned with TDM trunking (T1/E1/PRI, analog, or BRI) for PSTN voice connectivity. At the same time, most enterprise sites have broadband IP connectivity for Internet/WAN services. By moving some or all public network voice and fax traffic from TDM trunks to SIP trunks, the enterprise can remove expensive TDM trunks and leverage its broadband data pipe to run voice service over a cost-reduced SIP trunk.

Increased Provisioning Flexibility

With a SIP trunking service, customers can subscribe to concurrent SIP trunking sessions on an as-needed basis instead of subscribing to PSTN services, such as PRI T1/E1, which are typically provisioned in fixed channel increments. In addition, ongoing changes to SIP trunking service provisioning are typically done remotely, eliminating the need to schedule a site visit. This allows customers to more easily add or remove SIP trunking sessions when circumstances change.

SIP Trunking Challenges for the Enterprise

There are a number of challenges that need to be addressed in order to support the enterprise in the move to SIP trunking, including:

- Network Address Translation (NAT) and firewall traversal
- SIP interoperability
- Network edge security
- Network demarcation
- Legacy PBX infrastructure
- Fax over IP

Network Address Translation and Firewall Traversal Issues

Network Address Translation (NAT) is the technology that translates between the IP addresses in the private enterprise network topology and the public addresses on the Internet. It is often used to maintain an internal network of private addresses and to map them externally to a single public address. NAT is implemented at the routing device or network edge border device.

SIP is an application layer protocol that sends network addresses and port allocations within the application data, and it may use multiple ports to set up a connection. For instance, SIP as the signaling protocol may use a different network port than the RTP stream that carries the actual media (audio packets that make up the voice communications). NAT, however, resides at the transport layer and does not change the SIP addressing, which makes information received at the remote end invalid.

SIP Server functionality, combined with SIP Proxy and SIP Registrar functionality, can resolve NAT and port allocation issues by correctly translating IP addresses and port allocations in SIP from private internal addresses and port allocations to public external addresses and port allocations. SIP Server, SIP Proxy, and SIP Registrar can also monitor incoming SIP connections to provide similar address and port translations for incoming SIP calls. This monitoring functionality needs to be in the network edge border device, whether it is a SIP firewall or a SIP-capable edge device.

An alternative for resolving NAT traversal issues is to use the IETF protocols STUN (Simple Traversal of UDP through NATs), TURN (Traversal Using Relay NAT), and ICE (Interactive Connectivity Establishment). These protocols allow the creation of pinholes through the enterprise firewall that allow the SIP signaling and media to pass through. While these approaches provide viable alternatives for addressing NAT issues, they bypass the firewall and run on client and external servers. Keeping NAT translation functionality inside the firewall provides a more secure environment than using STUN, TURN, or ICE for NAT traversal.

SIP Interoperability Issues

Different vendors can have subtle differences in their SIP implementations, and there are SIP components and extensions that may be supported by one vendor but not another. These differences can lead to interoperability issues between different equipment types, and can create a significant issue for the ITSP or reseller trying to support the enterprise in the switchover to VoIP.

For the reasons described above, it is important to consider interoperability when choosing an equipment vendor. Vendors should have published results and configuration guides that describe their testing with SIP trunking providers and other equipment manufacturers. This type of testing can be costly and time consuming, and may require product customization by the vendor to achieve optimum interoperability. However, a vendor that ensures that its equipment interoperates with SIP trunking services and other equipment can provide the best flexibility in terms of overall solution design.

Interoperability can be further achieved by compliance with the SIP Forum's SIPconnect recommendation. The SIP Forum is the body for generating industry-wide technical recommendations related to SIP interoperability. For more information, see the [SIP Forum home page](#).

Network Edge Security Issues

Security should be a primary requirement for SIP trunking deployments in an enterprise, just as it is for other external connectivity deployments. In SIP, a user is identified with a SIP Uniform Resource Identifier (URI) in the format of **person@domain**. Unfortunately, the SIP URI can be used maliciously to launch attacks on a network. SIP-related security issues include:

- **Denial of Service Attacks** — Continued requests to the network that overload resources and cause the network to slow down or crash. This type of security breach can disrupt or completely disable services in a short period of time.
- **SPIT (Spam over Internet Telephony)** — Unwanted automatically-dialed calls coming into the network from malicious persons or telemarketers.
- **Toll Fraud** — Gaining access to PSTN resources to force calls to premium rate lines.

Taking the following steps can help alleviate these and other SIP security concerns:

- Dynamically encrypt the URI as recommended in the SIP specification.
- Change the port being used for every call, thus removing a known port scenario.
- Ensure that NAT is being used to maintain the integrity of the enterprise private address space, as discussed in “Network Address Translation and Firewall Traversal Issues,” above.
- Maintain data integrity by using Transport Layer Security (TLS) encryption for the SIP signaling and Secure Real-time Transport Protocol (SRTP) for the media data.
- Use Intrusion Detection and Prevention Systems (IDPS) to monitor and gather statistics for all SIP traffic, and take action against security threats when necessary, based on defined policies and traffic routing rules.

Taken together, these security levels can provide a robust security system for a SIP trunking deployment.

Network Demarcation Issues

In the PSTN world, the demarcation point in the enterprise is the physical location where the service provider terminates its trunking service on the enterprise premise. This is the point where everything on one side is owned and maintained by the enterprise, and everything on the other side is owned by the service provider. For troubleshooting and quality of service (QoS) purposes, the demarcation point is the location where the service provider can ‘wash its hands’ of an issue by proving the integrity of its service quality to that point.

Whether SIP trunking is delivered as a service provided by a broadband internet service provider (ISP), or as an over-the-top third party service on an ISP’s broadband data pipe, there may be no clear demarcation point between the termination of the trunking service and the enterprise’s network. However, for the reasons given above, it is often beneficial for the service provider and enterprise to establish a demarcation point. Enterprises deploying SIP trunking services need to consider how QoS will be managed; that is, where the service provider’s responsibility for QoS ends, and the enterprise’s responsibility for QoS begins. The logical place for SIP trunking demarcation is within a border element that addresses the related issues of NAT traversal, security, and interoperability.

Legacy PBX Infrastructure Issues

As previously noted, most of the installed base of hybrid PBXs, IP-PBXs, and TDM PBXs is provisioned with TDM trunking for PSTN voice connectivity. Many of these PBX systems are not equipped with the SIP protocol for trunk service, or even a VoIP network interface. But in many cases, the existing PBX does not need to be updated in order to use SIP trunking. Instead, the PBX can be augmented with a border element that provides SIP-to-TDM trunk conversion and a secure connection to the SIP trunking service provider (ITSP).

Table 1 describes the gateway capabilities that may be required to interface SIP trunks to a legacy TDM or hybrid PBX:

Capability	Description
VoIP-to-TDM Data Conversion	Translates packet VoIP streams to traditional TDM circuit-switched voice channels
SIP-to-TDM Protocol Conversion	Translates SIP signaling into any Primary Rate ISDN signaling (T1 or E1), including the Digital Network Interface (DNI)
Emulate PSTN Trunk Service	Provides physical connections to legacy PSTN trunk ports on the PBX or contact center system
Dial Plan Modification	Appends or strips digits as needed to normalize routing between the SIP trunking service and PBX

Table 1. Gateway Capabilities for Interfacing SIP Trunks to a Legacy TDM or Hybrid PBX

Fax over IP Issues

It is well documented that the circuit-switched fax protocol, T.30, does not work well on an IP packet network with SIP trunks. The T.30 protocol treats fax image data as an in-band pass through audio transmission using SIP and RTP, which makes it prone to packet loss and jitter. Failure rates grow at an increasing rate as individual fax document lengths increase, and those failure rates are generally deemed unacceptable for a production fax environment where images are part of an automated workflow.

The Fax over IP (FoIP) protocol, T.38, addresses these issues. Like VoIP, FoIP has primarily been deployed on the private enterprise data network. As enterprise customers look to the advantages of SIP trunking for voice, they often ask if they can shift their fax communications to the IP service as well.

Ensuring support for the T.38 protocol has been a low priority for many ITSPs. It requires network elements such as a carrier gateway between the PSTN and the IP networks to fully support the T.38 protocol. Even then, interoperability testing with premise equipment is necessary for there to be reliable fax transport. Because T.38 relies on the SIP protocol for signaling, its successful use requires resolving the network edge issues of NAT traversal and security, as well as considering the interface to the legacy fax infrastructure.

Defining and Securing the Enterprise Network Edge for SIP Trunking

The issues of defining and securing the enterprise network edge for SIP trunking, as described in the previous section, can be addressed by using a border element that includes an enterprise session border controller **and** a media gateway:

- Enterprise session border controllers reside at the edge of the enterprise network to address the SIP interoperability, network edge security, and network demarcation issues.
- Media gateways in both the customer premise and service provider network bridge IP networks with PSTN networks or TDM networks and systems.

Today, the challenges of moving to SIP trunking are driving the need for a new enterprise premise device that solves the issues at the network edge. Loosely defined as an enterprise border element, the device needs to combine SIP-to-SIP-session border control functions with SIP-to-TDM media gateway functions. By integrating these functions in a single enterprise edge border device and adding critical firewall and NAT traversal functions, a complete solution can be delivered that enables the adoption of SIP trunking services in virtually any enterprise environment with any legacy architecture.

An enterprise border element should perform the following functions:

- Integrate with current enterprise network architecture with the aim to disrupt it as little as possible by supporting the existing PBX.
- Protect the internal network behind NAT, but have the capability to traverse this protection for VoIP and FoIP connectivity.
- Meet the challenges of SIP security to protect the enterprise network.
- Offer SIP, PBX, and PSTN interoperability to alleviate concerns related to equipment not within control of the enterprise.
- Demarcate the enterprise edge, so there is a distinct physical location for determining network service responsibility.

Careful consideration of these requirements can help make the switch-over to SIP trunking non-disruptive, and can enable the enterprise to take advantage of the many benefits that SIP trunking offers.

Using an Enterprise Border Element to Facilitate a SIP Trunking Service

An enterprise border element can work with a TDM PBX, hybrid PBX, or IP-PBX to facilitate a SIP trunking service.

TDM or Hybrid PBX Support

TDM PBXs are configured and equipped to support TDM trunks only. Thus, they require a way to deal with the enterprise IP network edge issues surrounding SIP trunks. They also require SIP trunks to be converted back to TDM trunks in order to complete voice service connectivity to the legacy TDM environment. A SIP-to-TDM gateway can provide these capabilities.

Many first generation hybrid IP-PBX systems, deployed between 2000 and 2006, were based on VoIP protocols other than SIP, and may require an expensive upgrade to support SIP trunking services. And even then, they may not completely address the network edge issues discussed in this paper.

Figure 1 depicts how SIP trunking can work in an architecture containing a legacy TDM or hybrid PBX using an enterprise border element. In this architecture, the border element contains both the session border control functions and SIP-to-TDM gateway, which converts SIP trunk sessions into TDM signaling and channels, and resides between the corporate LAN and the legacy PBX.

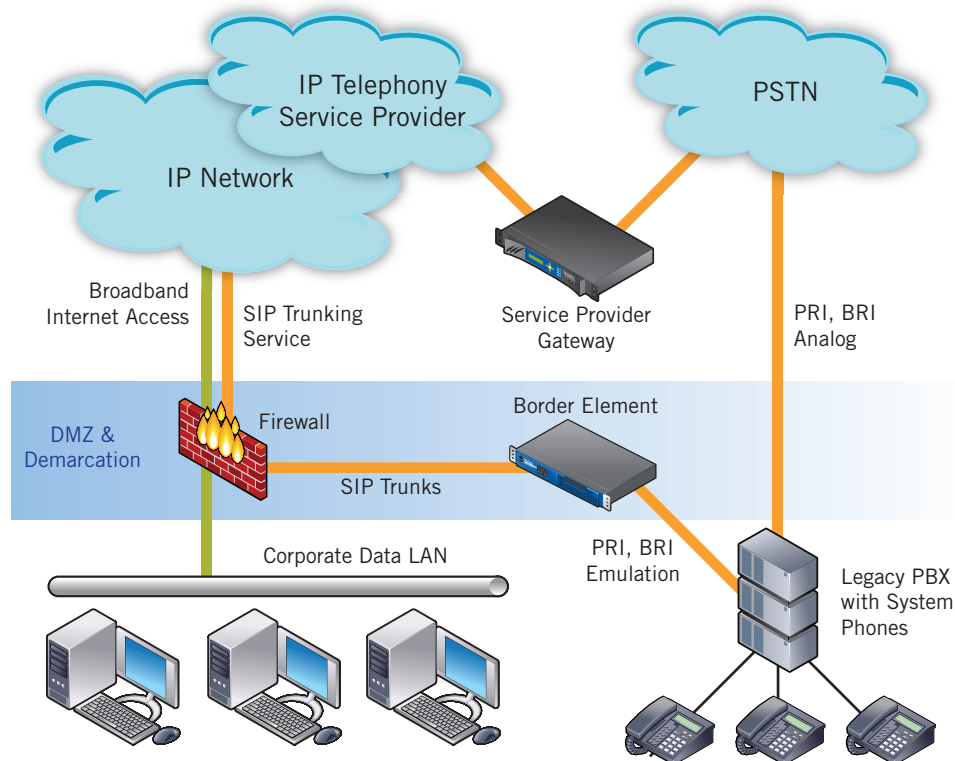


Figure 1 : Supporting SIP Trunking in an Architecture with a TDM or Hybrid PBX

IP-PBX Support

While some current IP PBXs are capable of supporting a SIP trunk directly, they typically are not equipped to completely resolve all of the enterprise network edge issues of NAT and firewall traversal, security, SIP interoperability, and service demarcation. In addition, most enterprise customers will want a mix of PSTN trunk service and SIP trunk service, if only for survivability and redundancy in the event of a SIP trunking service outage.

Figure 2 depicts how SIP trunking can work with a SIP-based IP-PBX using a border element that supports both PSTN connectivity and SIP trunks. In this architecture, the border element connects the Corporate LAN, IP-PBX, and PSTN, providing connectivity, security, routing, and interoperability between all three service elements.

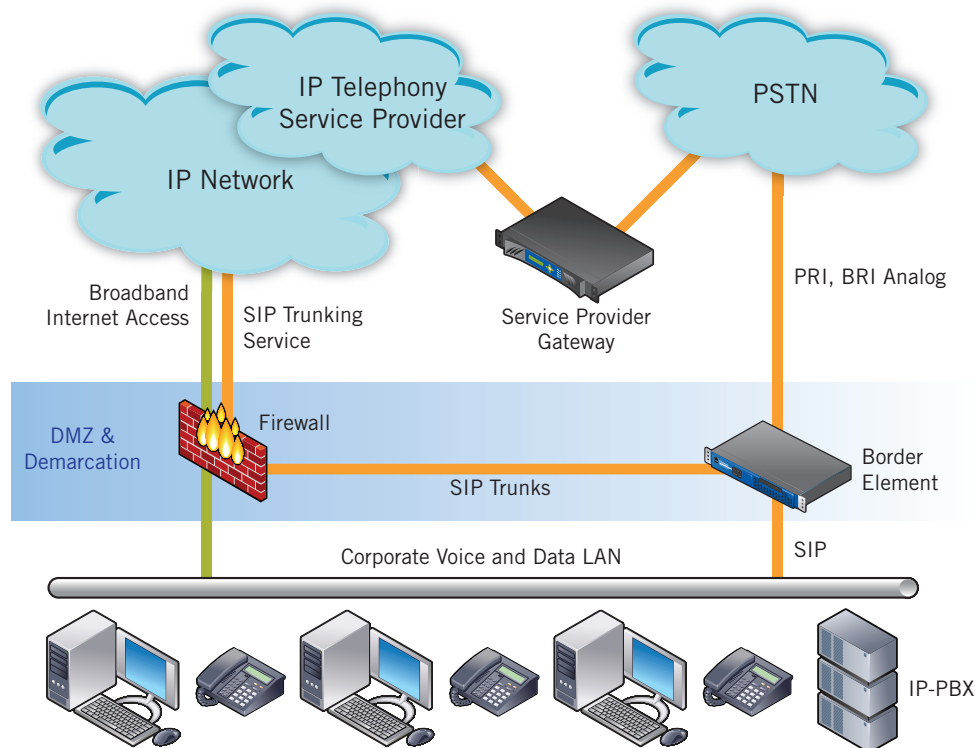


Figure 2: Supporting SIP Trunking in an Architecture with an IP-PBX

Future Options

While SIP trunking service adoption is primarily driven by the desire to reduce operational and capital infrastructure costs, it also enables broader SIP capabilities. Supporting enterprises in the move to SIP trunking provides opportunities for the enterprise to adopt the following additional functionality:

- Unified Communications (UC) and multimedia
- High Definition (HD) Voice
- Network monitoring

Unified Communications and Multimedia

As a multimedia, real-time, interactive IP-based protocol, SIP can deliver a range of UC sessions, starting with basic presence indicators, and scaling from instant messaging, voice, and video to full multimedia conferencing and collaboration. Once SIP is enabled to traverse into the public networks, it opens the door to a much richer and productive way to communicate beyond the corporate walls.

Many of the same enterprise network edge issues that must be resolved for SIP trunking are common to broader SIP services such as UC, multimedia collaboration, and hosted SIP services.

High Definition Voice

HD Voice is now available through services such as Skype and Microsoft® Office Communication Server (OCS), and is being rolled out by mobile service providers. When used with an IP-PBX that supports HD SIP phones, the SIP-aware border element is well-positioned to transcode the different HD Voice codecs used by the services. Thus, the border element can enable the interconnectivity of enterprise and mobile services to support an end-to-end HD Voice connection.

Network Monitoring

A border element is well suited to provide network monitoring functionality, because it can examine the data before it arrives in the service provider's network, at which point the signaling and media may split and follow different routes. For example, an enterprise may need to maintain connection logs that can be used for managing services and understanding the bandwidth usage of the pipe. Providing these connection logs can determine whether extra capacity is needed or can identify further costs savings through lower bandwidth needs.

Dialogic® Products that Provide Border Element Functionality

Both the Dialogic® BorderNet™ 500 Enterprise Session Border Controller (ESBC) and Dialogic® 1010 Integrated Media Gateway (IMG 1010) can provide border element functionality.

Dialogic® BorderNet™ 500 Enterprise Session Border Controller

The BorderNet 500 ESBC is a turnkey appliance that can enable the rapid deployment of new SIP-based communications services to enterprise customers by providing a flexible means to deliver SIP services from public IP networks to private enterprise IP networks and their resident communications systems.

- **Any-to-Any Connectivity and Call Routing** — Provides flexibility in connecting to a wide variety of services and equipment, including SIP trunks, PSTN trunks, and legacy, hybrid, and IP PBXs
- **Extensive SIP Interoperability Testing with Service Providers and PBX Manufacturers** — Delivers a high degree of confidence that the BorderNet 500 ESBC will work effectively with a wide variety of vendor interfaces and equipment
- **Robust SIP Security Features** — Create a secure demarcation point for an enterprise at the network edge to fend off malicious outside threats
- **Built-In SIP Proxy to Enable Firewall and NAT Traversal** — Allows an enterprise to connect to a SIP trunk or SIP service
- **Detailed Call Quality Statistics** — Enhance the ability to troubleshoot voice quality issues
- **T.38 FoIP at V.34 Speeds** — Provide high speed, reliable FoIP, reducing expenses by decreasing the time to transmit/receive fax messages

For more information, see the [Dialogic® BorderNet™ 500 Enterprise Session Border Controller](#) and [Enabling Secure and Interoperable SIP Services for the Enterprise](#) on the Dialogic website.

Dialogic® IMG 1010 Integrated Media Gateway

Supporting media and signaling in a single chassis, the IMG 1010 is a VoIP gateway that provides any-to-any voice network connectivity (SIP to PRI, CAS, and SS7 networks) and allows carriers to deliver new telephony services quickly. The IMG 1010 also supports IP-to-IP carrier-oriented border element functions, such as media transcoding, topology hiding, and SIP mediation for network applications. The IMG 1010 offers connectivity between a carrier's SIP-I, SIP-T, and SS7 over SIGTRAN resources and the SIP network.

For more information, see [Dialogic® IMG 1010 Integrated Media Gateway](#) on the Dialogic website.

Summary

SIP Trunking is a cost-effective way for an enterprise to support a move to an all-IP environment, while opening up a range of service possibilities in the future. Supporting the enterprise in this move does not need to be a complex task, since many of the potential issues can be addressed by implementing a supporting border element that is flexible enough to deal with potential pitfalls and able to deliver the many benefits SIP trunking provides.

Acronyms

BRI	Basic Rate Interface
DNI	Digital Network Interface
ESBC	Enterprise Session Border Controller
FoIP	Fax over IP
HD	High Definition
ICE	Interactive Connectivity Establishment
IDPS	Intrusion Detection and Prevention Systems
IETF	Internet Engineering Task Force
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider
NAT	Network Address Translation
PBX	Private Branch Exchange
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
ROI	Return On Investment
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SIP	Session Initiation Protocol
SPIT	Spam over Internet Telephony
SRTP	Secure Real-time Transport Protocol
STUN	Simple Traversal of UDP through NATs
TDM	Time-Division Multiplexing
TLS	Transport Layer Security
TURN	Traversal Using Relay NAT
UC	Unified Communications
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VoIP	Voice over IP

For More Information

For more information about SIP and SIP trunking, see:

SIP Forum, "IP PBX/Service Provider Interoperability: SIPconnect 1.0 Technical Recommendation" at http://www.sipforum.org/component/option,com_docman/task,cat_view/gid,43/Itemid,75/

For more information about the Dialogic® BorderNet™ 500 Enterprise Session Border Controller online, see:

[Dialogic® BorderNet™ 500 Enterprise Session Border Controller](#)
Enabling Secure and Interoperable SIP Services for the Enterprise

For more information about the Dialogic® IMG 1010 Integrated Media Gateway online, see:

[Dialogic® IMG 1010 Integrated Media Gateway](#)



www.dialogic.com

Dialogic Inc.
1504 McCarthy Boulevard
Milpitas, CA 95035-7405
USA

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH PRODUCTS OF DIALOGIC INC. AND ITS AFFILIATES OR SUBSIDIARIES ("DIALOGIC"). NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see <http://www.dialogic.com/company/terms-of-use.aspx> for more details.

Dialogic may make changes to specifications, product descriptions, and plans at any time, without notice.

Dialogic and BorderNet are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at the address above. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners. Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement their concepts or applications, which licenses may vary from country to country.

Any use case(s) shown and/or described herein represent one or more examples of the various ways, scenarios or environments in which Dialogic® products can be used. Such use case(s) are non-limiting and do not represent recommendations of Dialogic as to whether or how to use Dialogic products.