



Level: Intermediate
Works with: Sametime 3.0
Updated: 03-Sep-2002

by
[Tara Hall](#)

Editor's note: Since the publication of the article in the LDD Today June issue, the Sametime team has responded to customer requests for a more secure Sametime SIP Gateway by adding support for encryption of instant messages. The Sametime SIP Gateway is available with Sametime 3.0 + service pack one. We've updated the article to reflect the new encryption functionality.

Your organization recently acquired a new company. Your offices are in Washington, D.C., and the newly acquired company is headquartered in Chicago. The good news is that you're both using Sametime for instant messaging. The bad news is that you have two separate Sametime communities. How do these communities connect with one another so both offices can communicate through Sametime? Until now, that's been a difficult task—one that can involve having more than one Sametime Connect client. But the ability to connect these disparate communities is finally available. Sametime 3.0 introduces Session Initiation Protocol (SIP) Gateway functionality to connect one SIP-enabled community to another SIP-enabled community.

This article introduces you to Session Initiation Protocol (SIP) and provides an overview of SIP support in Sametime 3.0. Knowledge of the Sametime server and some familiarity with basic networking is assumed.

What is Session Initiation Protocol?

Session Initiation Protocol (SIP) is a standard protocol defined by the Internet Engineering Task Force (IETF), the same organization that brought you TCP/IP. SIP is an application-layer signaling protocol with rules that govern interactive, multimedia sessions, including presence and instant messaging. SIP uses existing transport protocols, like TCP, to initiate a session. In addition, SIP can modify or terminate a session. SIP is a control protocol that doesn't care about content.

With SIP, users are identified by a Uniform Reference Identifier (URI). When you connect with a SIP server, you send a registration to the Sametime 3.0 server that includes your URI. A SIP Registrar stores your registration information on the SIP server. If another user wants to create a session with you, the Sametime server locates you using your URI. The same thing happens when another user subscribes to your presence or sends you an instant message—the server uses your URI to locate you. The SIP URI uses the format sip:username@domainname, which is the same format as an Internet email address. Typically, SIP uses a user's email address as a Uniform Reference Identifier.

To help you understand how SIP works, here's an analogy: Think of initiating a session as similar to making a phone call to a friend. Your friend's phone number—like an URI—identifies him on the telephone network. But your friend may have more than one phone number for his home, cell, and office phones. If so, SIP can send the phone signal across the network to all phone numbers to locate your friend. SIP can ring all phones at once, or it can ring each phone serially one after another. When your friend answers the phone, the session becomes active. During the session, SIP helps to convey your message to your friend and return his response to you. SIP is fully

bidirectional and enables clients and servers to initiate both requests and responses.

If your friend receives another phone call and places you on hold, SIP modifies the session. Hold, call waiting, call forwarding, and other such services are possible with SIP, but SIP doesn't provide those services automatically. What SIP provides is the ability or flexibility to manage multiple sessions—like receiving more than one phone call at a time. Whoever implements SIP determines which services to include and to expose to the client. This is the equivalent of deciding which telephone services you want to pay for on your home, cell, or office phone.

Finally, when the conversation is over and you hang up the phone, SIP terminates the session.

Make it SIMPLE

SIP for Instant Messaging and Presence Leveraging Extensions or SIMPLE is an emerging standard based on the Session Initiation Protocol. SIMPLE is an extension of SIP that enables awareness and instant messaging. The SIP Registrar mentioned earlier uses your registration information for call routing. SIMPLE extends call routing to online status to ask for presence and to provide instant messaging. The Sametime SIP Gateway supports SIMPLE, and as other instant messaging vendors such as AOL and Microsoft support SIMPLE, you will be able to connect your Sametime community with third-party SIP-enabled communities.

Sametime and SIP

To connect your Sametime 3.0 server to a separate Sametime community, you need the Sametime SIP Gateway, which is part of the Sametime 3.0 server, and the SIP Connector. The other community that you are connecting with needs a SIP Gateway and a SIP Connector as well. Together the SIP Gateway and SIP Connector act as a SIP proxy server. The SIP Connector creates the connections to other SIP-enabled communities. It is responsible for both networking and the preliminary parsing of instant messages. The SIP Gateway also processes messages, but the primary responsibility of the gateway is to provide translation between the SIP network and your Sametime community.

To connect Sametime communities, each community must contain at least one Sametime 3.0 server with the SIP Gateway enabled to connect the communities. If you have more than one Sametime 3.0 server in your community, you must have a SIP Gateway configured on each server. Enabling the SIP Gateway is optional. Installing or upgrading to the Sametime 3.0 server does not automatically enable the SIP Gateway. When you want to SIP-enable your Sametime community, follow this general procedure:

1. Install and setup the SIP Connector, preferably on a separate machine.
2. Configure the SIP Gateway on your Sametime 3.0 server.

Security

Once you start connecting your SIP-enabled community to other SIP-enabled communities, are you concerned that you'll open your community to just anyone? As you'll see later in this article, you can determine which communities you connect with when you configure the SIP Gateway. In addition, the Sametime SIP Gateway addresses server-to-server authentication through IP addresses, which is how Sametime currently authenticates servers. When a SIP Connector connects with another server, it first checks whether or not the external community is enabled. Whether or not a community is enabled is determined when you configure the documents in the Sametime Configuration database (discussed later in this article). When you enable a connection to another SIP-enabled community, you list the DNS domains of that external community. If the community is enabled but the SIP Connector can't find a proxy server for the external community, the SIP Connector uses the DNS to create a connection.

When an external server tries to connect to your Sametime community, your SIP Connector attempts to find the name of the proxy server using DNS. If the IP address of the proxy server matches the IP address that the message came from, then the Connector accepts the connection. If the two IP addresses don't match, the Connector rejects the connection.

Encryption

The latest Web browsers support the Transport Layer Security (TLS) protocol and so does the SIP Gateway. TLS is an Internet protocol that prevents third parties from listening in or tampering with a message communicated between a server and client. Because the SIP Gateway supports connections to other communities, Sametime 3.0 uses the TLS protocol to encrypt messages sent between servers, between servers and SIP Gateways, and between SIP Gateways. The Sametime Connect client doesn't support the TLS protocol; instead, it uses a proprietary protocol when connecting with the Sametime server.

The TLS protocol has two layers:

- TLS Record Protocol

This layer encrypts data using symmetric cryptography, which is often referred to as "secret keys," although not all messages using this protocol are encrypted. But for encrypted messages, only the communicating parties share the secret key for encryption and decryption of messages. To obtain a key, the client and server negotiate a "secret."

- **TLS Handshake Protocol**

This layer negotiates the secret and an encryption algorithm between the communicating parties. It also enables the parties to authenticate one another using asymmetric cryptography, which uses a single private key and a single public key. The public key decrypts data encrypted by the private key, and the private key decrypts data encrypted by the public key. (For a general explanation of how encryption works, see the *LDD Today* article, "[Using field encryption in applications](#).")

The TLS protocol is based on the Netscape Secure Socket Layer (SSL) 3.0 protocol to provide secure messaging. But like SIP, the TLS protocol is a standard developed by the IETF.

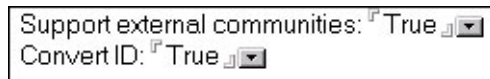
The Sametime SIP Gateway

You configure the Sametime SIP Gateway using four documents in the Sametime Configuration database: the CommunityGateway, the ExternCommunity, the CommunityConnector, and the CommunityConnectivity documents. These documents enable the connections to other SIP-enabled communities. You should set up the documents in the order that they appear here.

Instructions for creating and configuring the documents in the Sametime Configuration database are available in the [Sametime 3.0 Administrator's Guide](#).

The CommunityGateway document

The CommunityGateway document tells the SIP Gateway to translate Internet email addresses. The Sametime SIP Gateway identifies users by their Internet email addresses, for instance, John_Smith@acme.com. When you add users from another SIP-enabled community, you specify their Internet email addresses in your contact list. The SIP Gateway can translate email addresses using LDAP directories, but you can programmatically access other directories.



Support external communities: True
Convert ID: True

The Sametime SIP Gateway can translate internal user IDs to Internet email addresses for you. So when you send an instant message to another user outside your community, the gateway will translate your ID into your Internet email address for the recipient. To enable translation of email addresses, you only need to set the ConvertID field value in the CommunityGateway document to True.

The ExternCommunity document

The ExternCommunity document determines which SIP-enabled community the gateway connects to. In this document, you specify:

- The name of the SIP-enabled community
- The DNS domains of the community
- The DNS name of the SIP proxy server
- The port on which to connect to the SIP proxy server



Community Name:
Domains:
DNS:
Port:

You can use any name for the SIP-enabled community, but you may want to choose something descriptive. You can specify more than one domain for a single community and use the asterisk (*) wildcard to specify a domain name, for example, *.acme.com. Specifying the DNS name of the SIP proxy server is optional. If you don't provide one, the Sametime server performs a DNS lookup for the SIP proxy for the domains that you specified. If the Sametime server can't find the SIP proxy server, it attempts to connect to the domain using the port that you specify for the proxy server. The default port number is 5060, the same one used for the SIP Connector.

The CommunityConnector document

The CommunityConnector document controls the SIP Connector functions. In this document, you specify:

- The name and IP address of the SIP Connector machine

- The SIP Connector port
- The names of SIP-enabled communities to which the SIP Gateway connects

The name of the SIP Connector machine will be the same one you specify when you install the SIP Connector. Use the DNS name of the server on which you install the SIP Connector. By default, the SIP Connector port, on which the connector listens for connections, is 5060. The names of the SIP-enabled communities are the same ones that you specify in the ExternCommunity document.

Connector Name:	
IP:	
Port:	
Supported Communities:	

When you want to disable a connection to another SIP-enabled community, you only need to change the value of the "Support Communities" field in the CommunityConnector document to False. Setting the value to True enables the connection.

The CommunityConnectivity document

The CommunityConnectivity document sets the security for your community. In the ExternCommunity document, you specify which communities your users can communicate with, but in the CommunityConnectivity document, you can specify which SIP Connectors the Sametime server can connect with. You enter the IP addresses of the SIP Connector machines in the Community Trusted Ips field.

VPHMX_HOSTNAME	HTTP Tunneling Host Name	
VPHMX_PORT	HTTP Tunneling Port	80
VPHMX	Is HTTP Tunneling supported?	true
VPMX_HOSTNAME	Direct TCP Host Name	
VPMX_PORT	Direct TCP Port	1533
VPHTTSPMX_HOSTNAME	HTTPS Host Name	
VPHTTSPMX_PORT	HTTPS Port	
Community Trusted IPS		

The SIP Connector

Without the SIP Connector, the Sametime SIP Gateway can't function. The SIP Connector installation program is on the Sametime server CD. System requirements for the SIP Connector are the same as the requirements for the Sametime 3.0 server (see the [Sametime 3.0 Installation Guide](#)). When you install the SIP Connector, you provide two pieces of information: the installation path and the name of the Sametime SIP Gateway server to connect with. After you install the Connector, it's ready for use. You configure the Connector when creating the Sametime Configuration database documents for the SIP Gateway.

You can install the SIP Connector either on your Sametime 3.0 server or on a separate machine. However, it's best to install the SIP Connector on a separate machine for a couple of reasons:

- If you are connecting to communities through the Internet, the SIP Connector needs to reside outside of your company's firewall. Installing the Connector on a Sametime server means having both of them outside the protection of your firewall.
- For performance reasons, you may want to install the SIP Connector separately. If you expect heavy traffic between or among your SIP-enabled communities, installing the SIP Connector and Sametime server on the same machine degrades performance.

The SIP Connector performs the following tasks for the gateway:

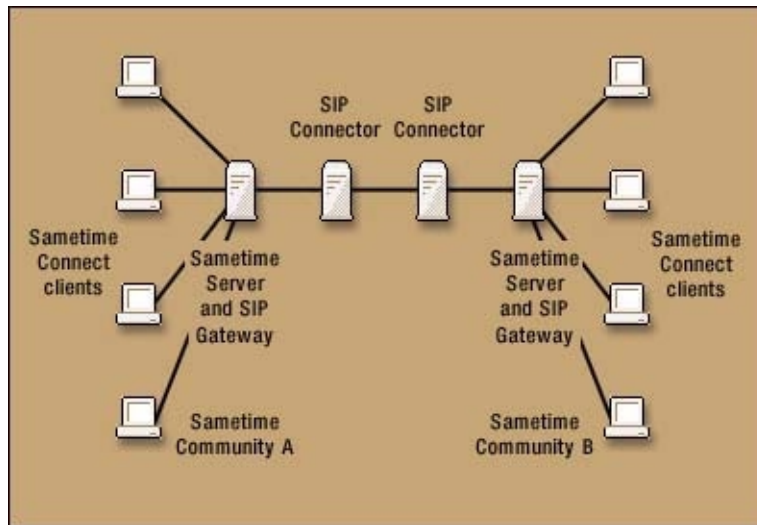
- It receives and parses outgoing messages from the gateway.
- It connects to either another SIP Connector or to an SIP proxy server in the other community.
- It parses and delivers incoming messages to the gateway.

The SIP Connector can connect with external SIP-enabled communities through the Internet, so it must be available beyond your organization's firewall, while still connecting to your Sametime server inside the firewall. You can also install the SIP Connector on an intranet machine with a network connection with the Sametime server.

When designing your architecture, you have several options:

- One SIP Connector, one SIP Gateway
You can dedicate one SIP Connector to service one SIP Gateway in your community.
- One SIP Connector, more than one SIP Gateway
You can use one SIP Connector to service more than one Sametime SIP Gateway in your community.
- More than one SIP Connector, one or more SIP Gateways
If you have a lot of traffic, you can install multiple connectors for load balancing. Having more than one connector also provides back up if one SIP Connector fails.

Remember that you can designate more than one external SIP-enabled community for a single SIP Connector. The following diagram shows a basic one SIP Gateway, one SIP connector topology.



Sametime clients and directories

The Sametime SIP Gateway connects only with other SIP-enabled communities. Those communities do not include clients and servers. While there are SIP clients available today, you cannot use those clients to connect with your SIP-enabled community.

You need the Sametime Connect client to connect to other SIP-enabled Sametime communities. While the Sametime 3.0 server is SIP-enabled, the Sametime Connect 3.0 client is not. With the Sametime Connect client and the SIP Gateway in place, you can do the following:

- See who is online or offline in the SIP-enabled community (they can also see you)
- Add users from another SIP-enabled community to your Sametime Connect contact list
- Initiate one-to-one instant messaging sessions with users of another SIP-enabled community
- Use Sametime Connect privacy features to prevent others from seeing your online status (while still seeing theirs)

Your SIP-enabled community cannot access the directory of another SIP-enabled community. So when adding external users to your contact list, you need to know their Internet email addresses. The Session Initiation Protocol does not provide rules for directories. If you want to connect directories in separate SIP-enabled communities, you can use other protocols like LDAP. This may be useful if you are connecting more than one SIP-enabled community within the same organization.

SIPing ahead

Sametime 3.0 contains the initial implementation of SIP, supporting presence and instant messaging across SIP-enabled communities. In the future, you can expect audio and video conferencing support as well for these communities. And as more instant messaging vendors, like AOL and Microsoft, embrace SIP, you can broaden your community connections even further.