Lotusphere® 2008

HND302

IBM Lotus Sametime Gateway – Setup and Administration

Chris Miller | Director of Messaging and Collaboration / Connectria

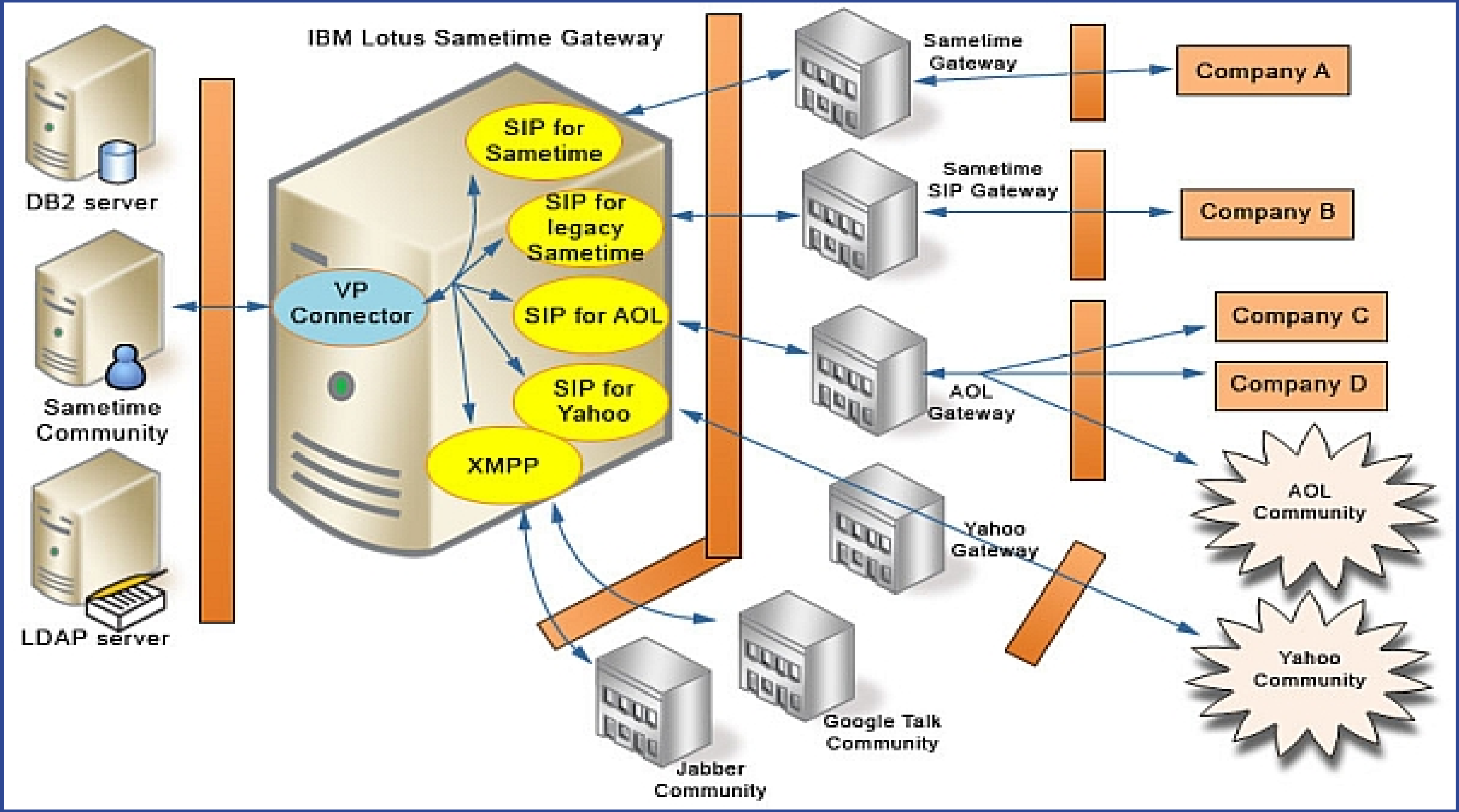
Troy Schoewe / Supervisor of Messaging / Connectria

Lotusphere 2008

The Agenda

- DB2 installation
- Sametime Gateway/WAS installation
  - Hardware and software talks
- Gateway configuration
- Network placement and architecture talks throughout
- Cross fingers here that you can write fast enough

Where You Will End UP



From the online IBM Lotus Sametime Gateway documentation

The DB2 Installation

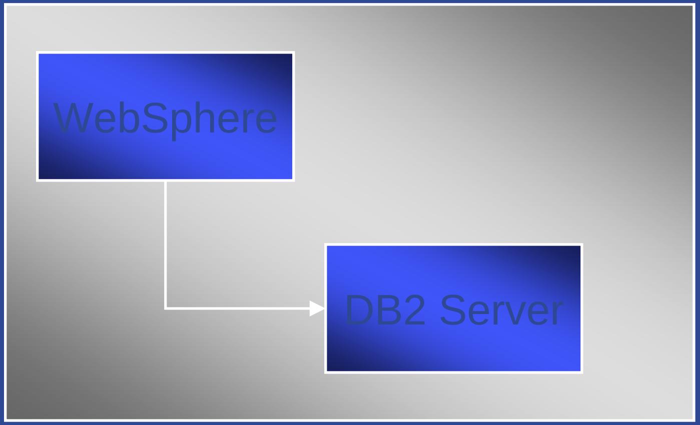
- We completed the DB2 software installation in advance to save time
  - Some reminders:

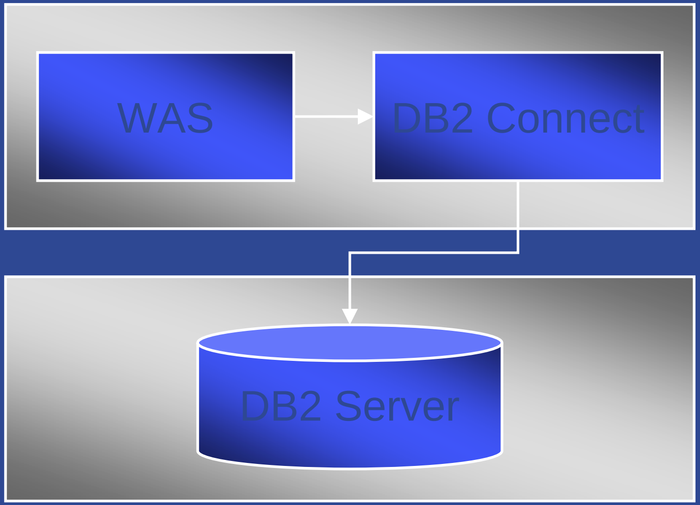
    - Do **NOT** use any of the restricted characters in the DB2 password
      - ;*!?"/<>|+&'`[]%^
      - Looks similar to a cartoon saying bad words, remember that
    - The DB2 admin account should have local administrator rights
    - Allow the installer to create any necessary local groups
    - Make life easier on yourself and do not install into Windows paths with spaces

Creating the DB2 Database for the Gateway

- This will create the tables and bufferpools that the gateway requires
  - Your server machine name should **not** be STGW
- You must unpack the Sametime Gateway installers to complete this task
  - So let’s move to that step and discuss some best practices while it works
- Navigate from a command prompt to the following directory:
  - ..\<sametime gateway install files>\database\db2
- Change to a DB2 command prompt
  - Db2cmd
- Run the following command to create the tables:
  - db2 –tvf createDb.sql (you may also append *>createDbout.txt* for output)

Deployment Options – Single Server





Single Server

- WebSphere / DB2 Server on the same machine

Split install

- WebSphere / DB2 Client on one machine
- DB2 server on a remote machine

Hardware Requirements for the Gateway

- The minimum hardware requirements match those of your standard WebSphere Application Server
  - Dual processor — 2GHz or better
  - 2GB of RAM on the low end
  - Disk requires 2GB for the media and 2GB for the Real-Time Collaboration (RTC) Gateway code
    - Bonus note — multiple gateway configurations require 5GB of space, plus 2GB for the media
- However, this does not take into account LDAP or DB2, however

Software Requirement Notes

- You can get the current version requirements here:
- These deserve special mention
  - Match the DB2 version exactly, do not attempt to get the “latest”
  - There are many supported LDAP directories, you simply must utilize the same one that your Sametime infrastructure points to
  - Get ready to obtain a trusted certificate
    - We will discuss your needs versus costs
  - Verify that you disable older SIP gateway installations when completed with the gateway install

Installing the Sametime Gateway (single server)

- Verify that DB2 is running at your installation at this point
- Unpack the Websphere files following the best practices we discussed a few minutes ago
- Navigate via file explorer (or command prompt for the old timers)
  - Launch *install.bat*
- Let’s walk through the wizard together…
- Get your pencils and pens ready for real-world installation brain dumping

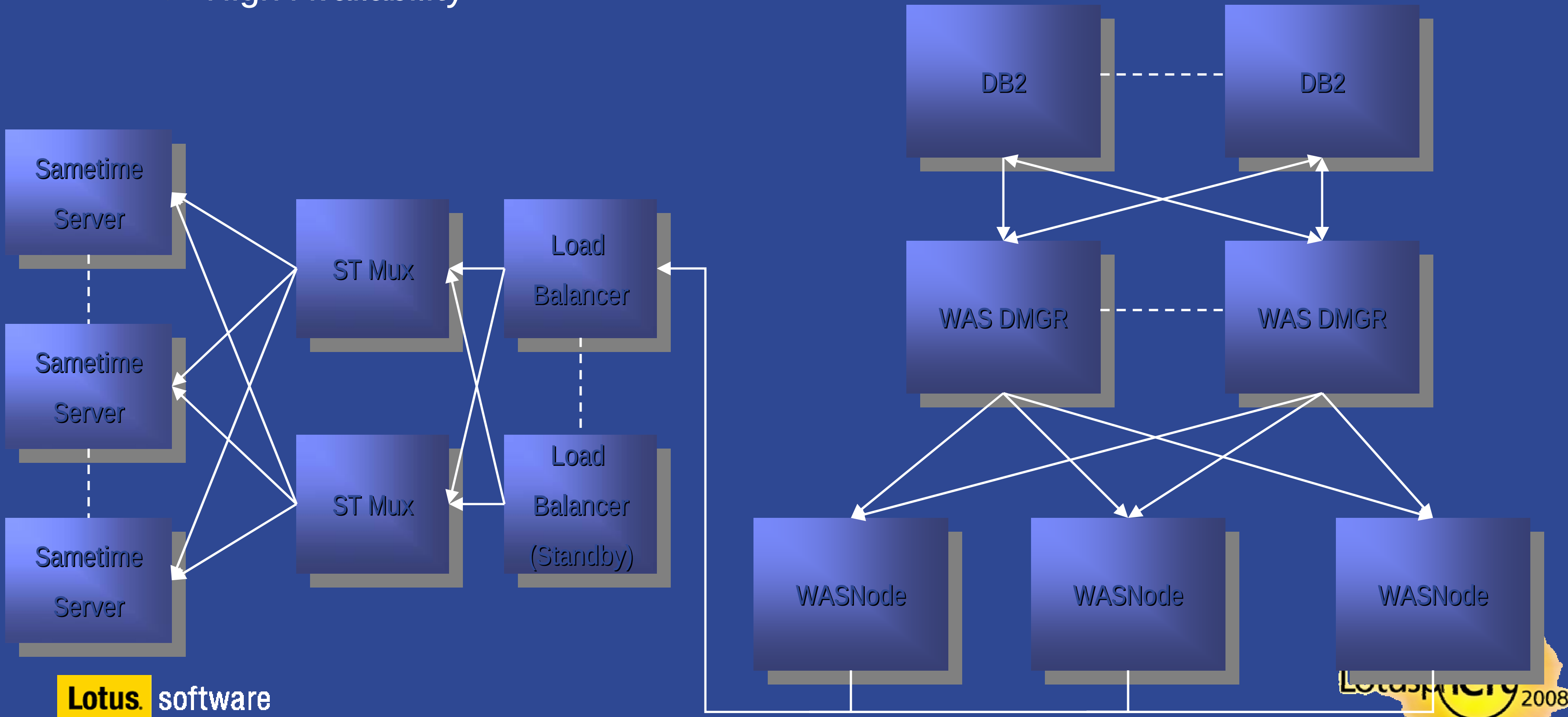
The IdoNotes Top 5 Gateway Questions

1) How many pieces of hardware do I need?
2) Can I use an existing DB2 installation in my enterprise?
3) How many users will ‘this’ architecture design support?
4) Where do I put the actual gateway in my network design
5) How do I get rid of all these NAT’s flying around?

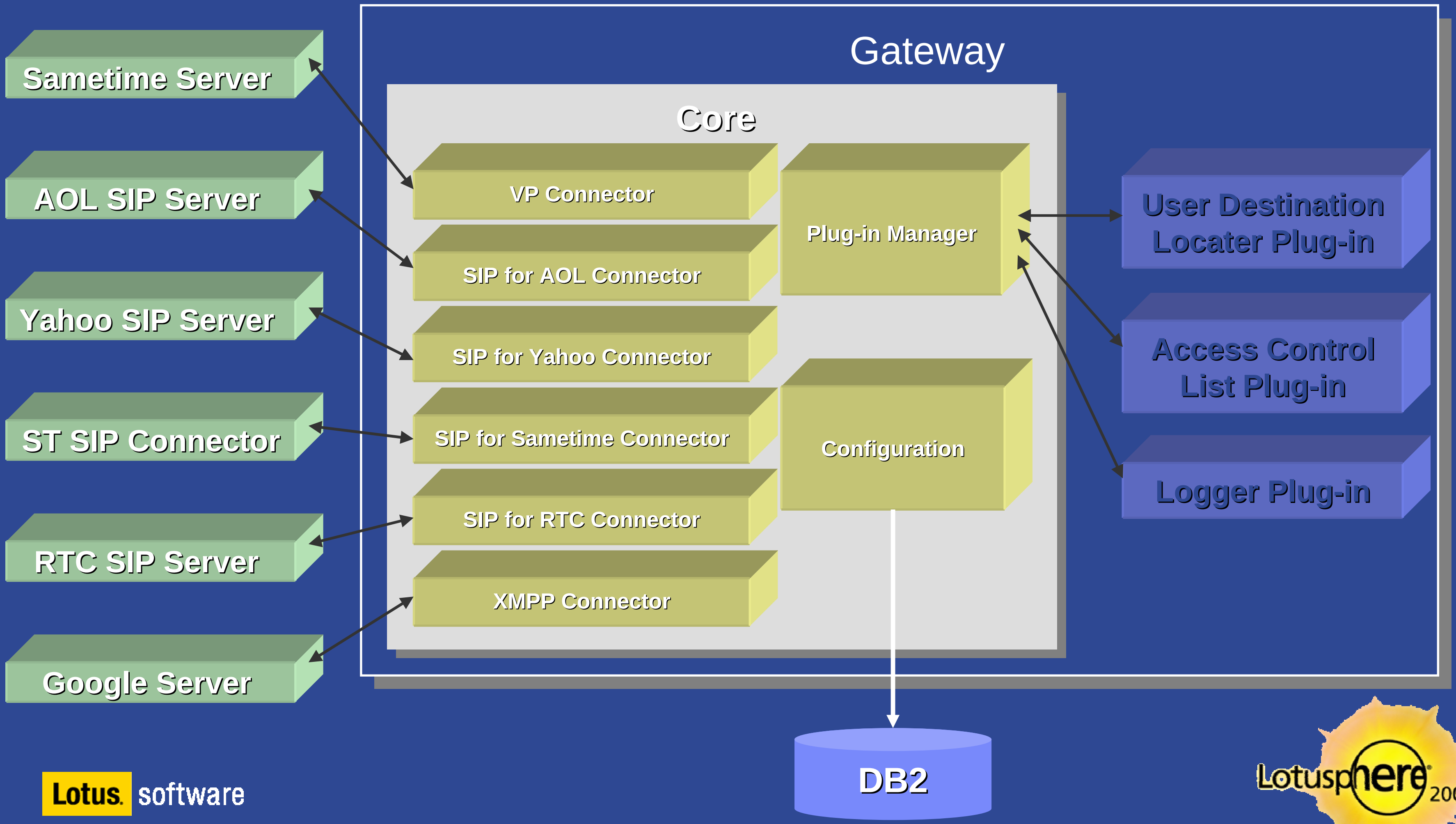
Deployment Options – Clustered Options

Sametime Gateway Deployment Configurations

- WebSphere Clustered Configuration
  - High Availability



Sametime Gateway Architecture (from IBM TechTalk)



Lotus. software

Lotusphere 2008

The Sametime Gateway in My Network

- The gateway is not fond of:
  - NAT
  - lots of firewalls
  - Numerous DMZ zones
  - and other network issues called “*network administrators*”

- Let’s break them down some more...

DNS

- DNS naming is one of the most important first steps
  - Do **<u>NOT</u>** utilize STGW as your machine or DNS name
  - Think of something portable
  - Aliases are fine, portability is important
- DNS must both be a normal A record and SRV entries
  - Guaranteed more than half of you have network adminsitrators that have never seen or implemented a SRV entry
- The gateway must not only resolve for external companies but must be able to look up proper DNS entries for other hosts

A Proper SRV Lookup Example

- > set class=ANY
- > set type=SRV
- > _xmpp-server._tcp.imcontrol.com
- Server: dns-rs1
  - Address: 12.127.17.71
  - Non-authoritative answer:
  - _xmpp-server._tcp.imcontrol.connectria.com
    - SRV service location:
      - priority = 5
      - weight = 0
      - port = 5269svr hostname = imcontrol.connectria.com
  - You must have a SRV entry for <u>**each**</u> domain you support for mail that would show in the LDAP source

LDAP Rules and Regulations

- The Sametime Gateway must utilize the same directory as your Sametime environment we connect to
  - Scenario 1: Sametime uses the Domino Directory natively
  - Scenario 2: Sametime uses the Domino Directory via LDAP
  - Scenario 3: Sametime uses a remote LDAP source

- The result of all of the above is the same. The Sametime Gateway **must** point to that same directory source via LDAP
  - Authenticated connections are preferred

Launching Your Server

- First step – starting the gateway
  - Let me teach you a couple little knowledge nuggets about a common mistake
- Once the gateway obtains a process id and is open for business, we may proceed
- Launch your Internet browser and head to the Integrated Solutions Console (ISC from here on)
  - http://server.acme.com:9060/ibm/console

Configuring LDAP Manually

- The ISC will be where we maintain the majority of further configurations today
- Navigate to the following:
  - Security > Secure administration, applications and infrastructure from the menu
  - Verify that both *Enable administrative security* and *Enable application security* are selected
  - Set as current
  - Configure
  - Add base entry to the realm
  - Add repository
    - You make up some logical name at this point, just make sure it is unique
  - Let's walk through the remainder of the fields together

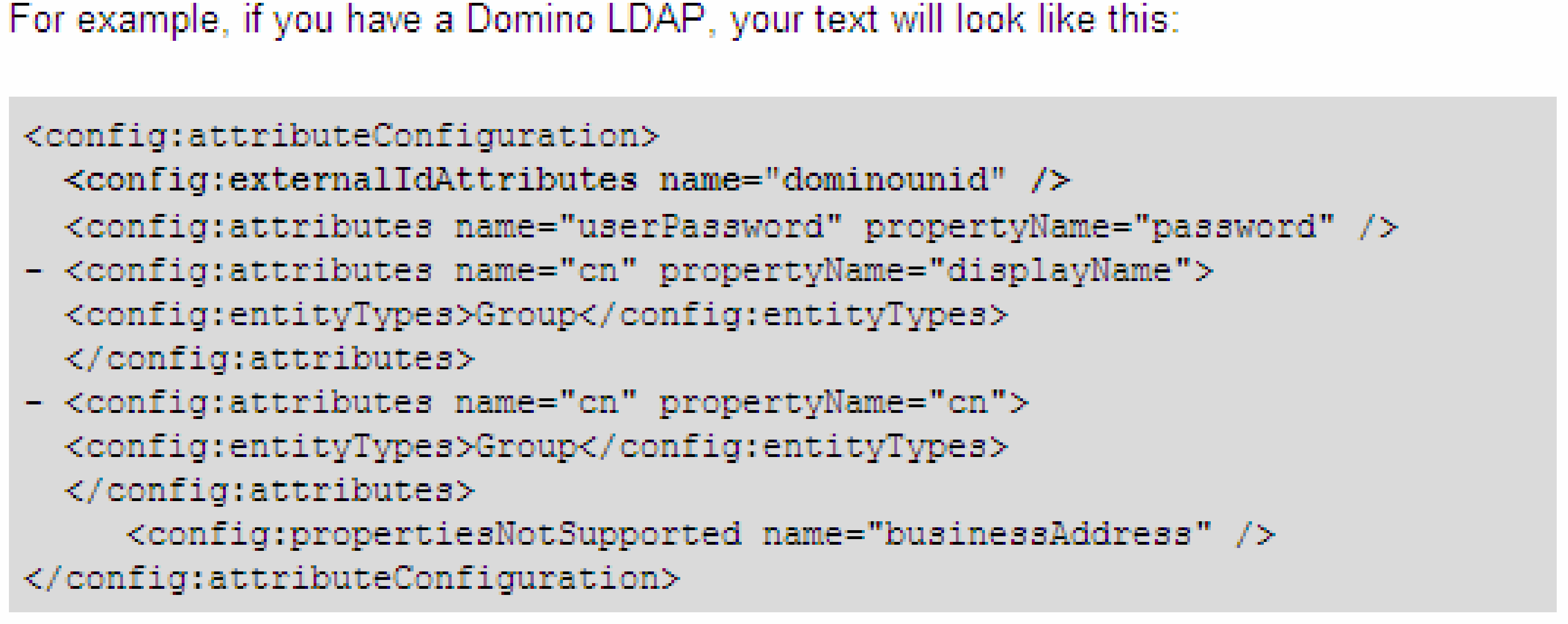
Finalizing the LDAP configuration manually

- Now that we have done the remainder of the settings, *Apply* and then *Save*
- In *Distinguished name of a base entry that uniquely...* field
  - o=defaultWIMLDAPBasedRealm
  - While Lotus now allows alternate names here, stick with the standards
- In *Distinguished name of a base entry in ...* field
  - Leave blank to start at the root of your LDAP directory
  - Insert *dc=xxx, dc=com* , let's discuss the key reasons

Oh, you didn’t think that was it did you?

- Websphere never allows for you to not edit a text entry
- Make your life simple here and cut and paste where possible
- Open the following location and file:
  - <app server root>\profiles\RTCGW_Profile \config\cells\ *<cell_name>*\wim\config\wimconfig.xml
- Find this section:
  - <config:attributeConfiguration>
- Add the following line:
  - <config:externalIdAttributes name="dominounid"/> right above password
  - **SPECIAL NOTE**: The Domino LDAP source **must** be 6.5.4 or higher

Sample Wimconfig.xml



For example, if you have a Domino LDAP, your text will look like this:

```
<config:attributeConfiguration>
  <config:externalIdAttributes name="dominounid" />
  <config:attributes name="userPassword" propertyName="password" />
- <config:attributes name="cn" propertyName="displayName">
  <config:entityTypes>Group</config:entityTypes>
  </config:attributes>
- <config:attributes name="cn" propertyName="cn">
  <config:entityTypes>Group</config:entityTypes>
  </config:attributes>
     <config:propertiesNotSupported name="businessAddress" />
</config:attributeConfiguration>
```

The Sametime Gateway Has A Habit

- The habit is called ‘stop and restart’ for changes
- If you left your command prompt open, then you are one step ahead
- Stop and restart your gateways
- Log back into the ISC and navigate to:
  - Users and Groups > Manage Users
  - Click *Search*
    - If you receive **no** results **stop** as the remainder of the steps will be a waste of your energy if no directory may be reached
    - Let’s discuss some common issues at this point with LDAP connectivity
- If we are successful let’s move on

Enabling the Secure Login manually

- Copy the *rtcgw_vmm.jacl* file from the following:
  - <sametime gateway root>/config/adminscripts/
- To the following location:
  - <app server root>/bin
- Open “or use” your command prompt and navigate to the bin directory above
  - wsadmin -username *username* -password *password* -f rtcgw_vmm.jacl
  - The username is what we created when we installed the gateway and the password we assigned during creation
- Restart your gateways

Preparing Sametime for the Gateway

- There are a few steps required, let’s see if you catch the missing one:
  - On your Sametime server(s), open **stconfig.nsf** and edit the Community Connectivity document to trust the IP address of the gateway
    - In version 7.0 and previous, you actually need to create a Community Gateway document and accept all the defaults as True
    - Run away from this option and get moving to 7.5.x or 8.0
  - Disable any previous SIP gateway connectivity
  - Configure the necessary policies to allow users to add external contacts
  - Restart the entire Domino/Sametime server to pick up all the changes

Ways to Stop and Start the Gateway

- Stopping the gateway from the profile bin allows two ways to do the manual stops and starts
  - 1. Wait for the prompt that pops up
  - 2. stopServer.bat RTCGWServer -username *username* -password *password* startServer.bat RTCGWServer with the names from above

- You may also list the gateway as a service
  - However it does not always properly shut down on Windows and a server restart may be necessary
  - IBM technote #1267202 has the necessary steps
    - .WASService -add "SametimeGateway" -serverName RTCGWServer -profilePath "[Path To Profile Directory]" -startType automatic
    - Note: Do not use spaces in the service name in Windows or it will not start

Connecting the Gateway to Your Sametime Server

1. From the Integrated Solutions Console (of course)
   - Real-Time Collaboration Gateway → Communities
   - Select New and enter a name that defines the community
   - Select Local as the community type (since it is your Sametime community you are adding)
   - Domains must include the Fully Qualified Domain Name (FQDN) of your SIP naming
     - This might be multiple local domain names
   - Set the translation protocol to VP
   - Provide the hostname of the Sametime server
     - FQDN of the server, not the Notes name
   - Click OK and restart as you would expect

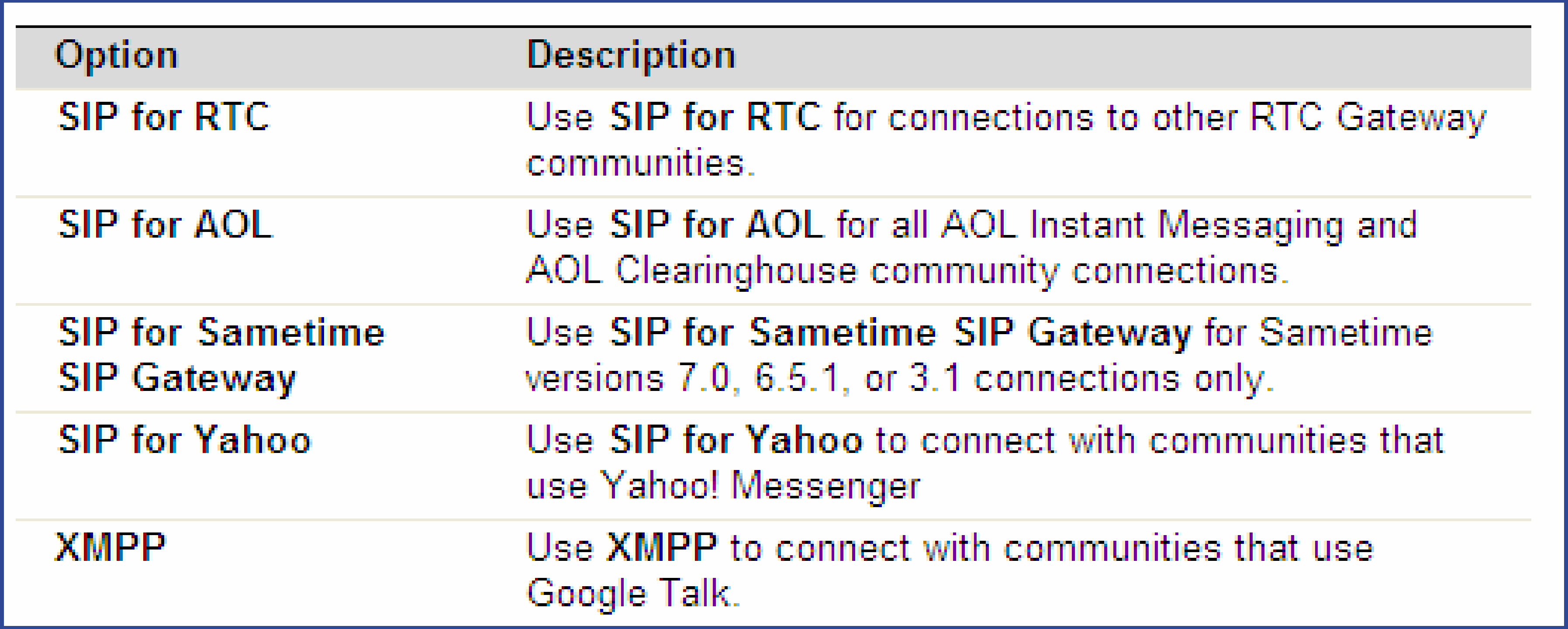
Adding External Communities

- Next, we are moving to external, instead of local, communities. However, you must assign local users or no one can access this new external community.

1. Be sure you have completed the steps on Slide 25 to add Sametime to the Sametime Gateway.
2. This is done in the same place in the Integrated Solutions Console.
   - Note: To connect to AOL, AIM, ICQ, or iChat communities, use these domains:
     - aol.net, corp.aol.com, or aol.com (for AIM or AOL users)
     - iqc.com (for ICQ users)
     - mac.com (for iChat users)

Adding External Communities (cont.)

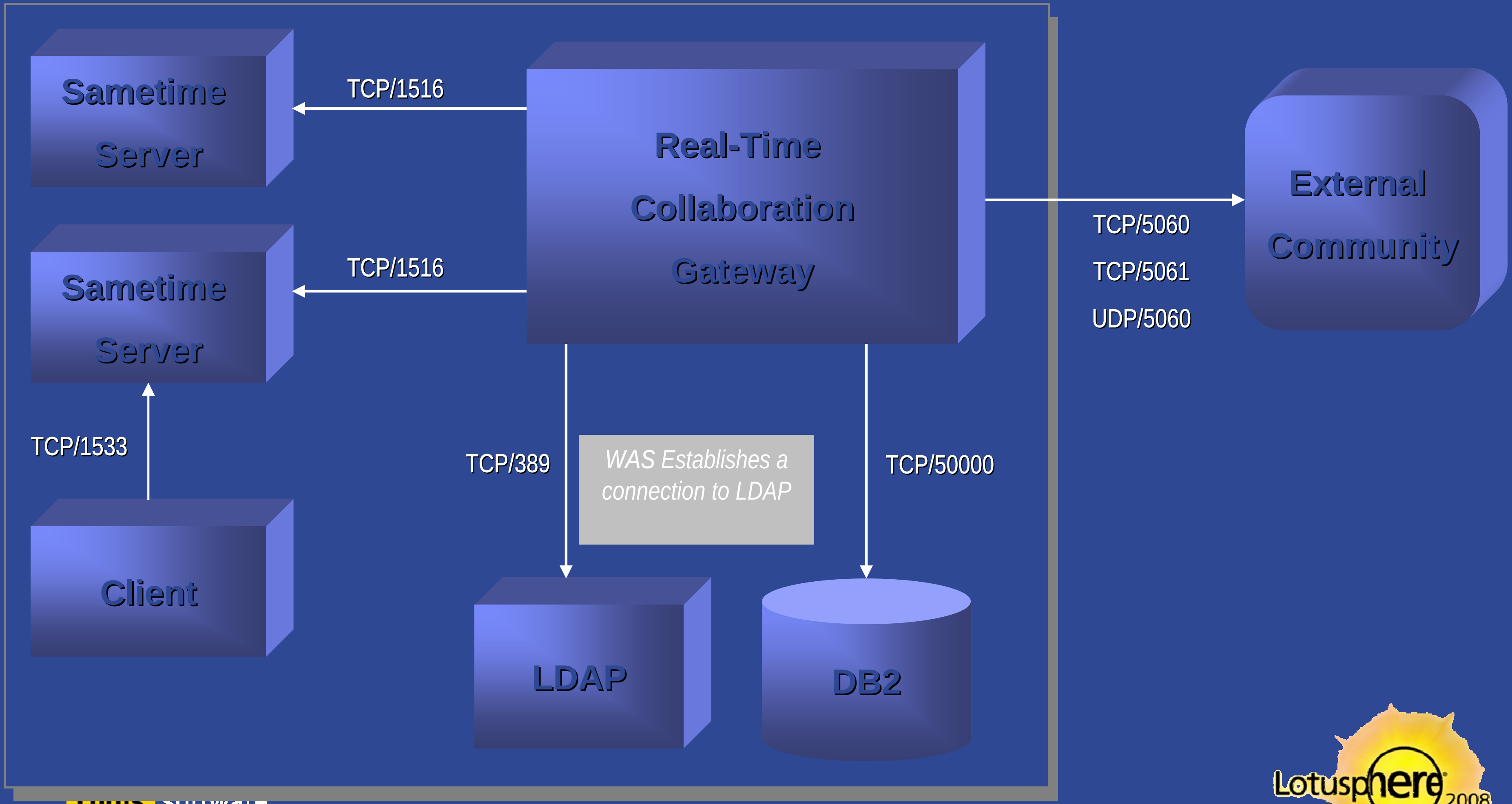
3. Select a translation protocol



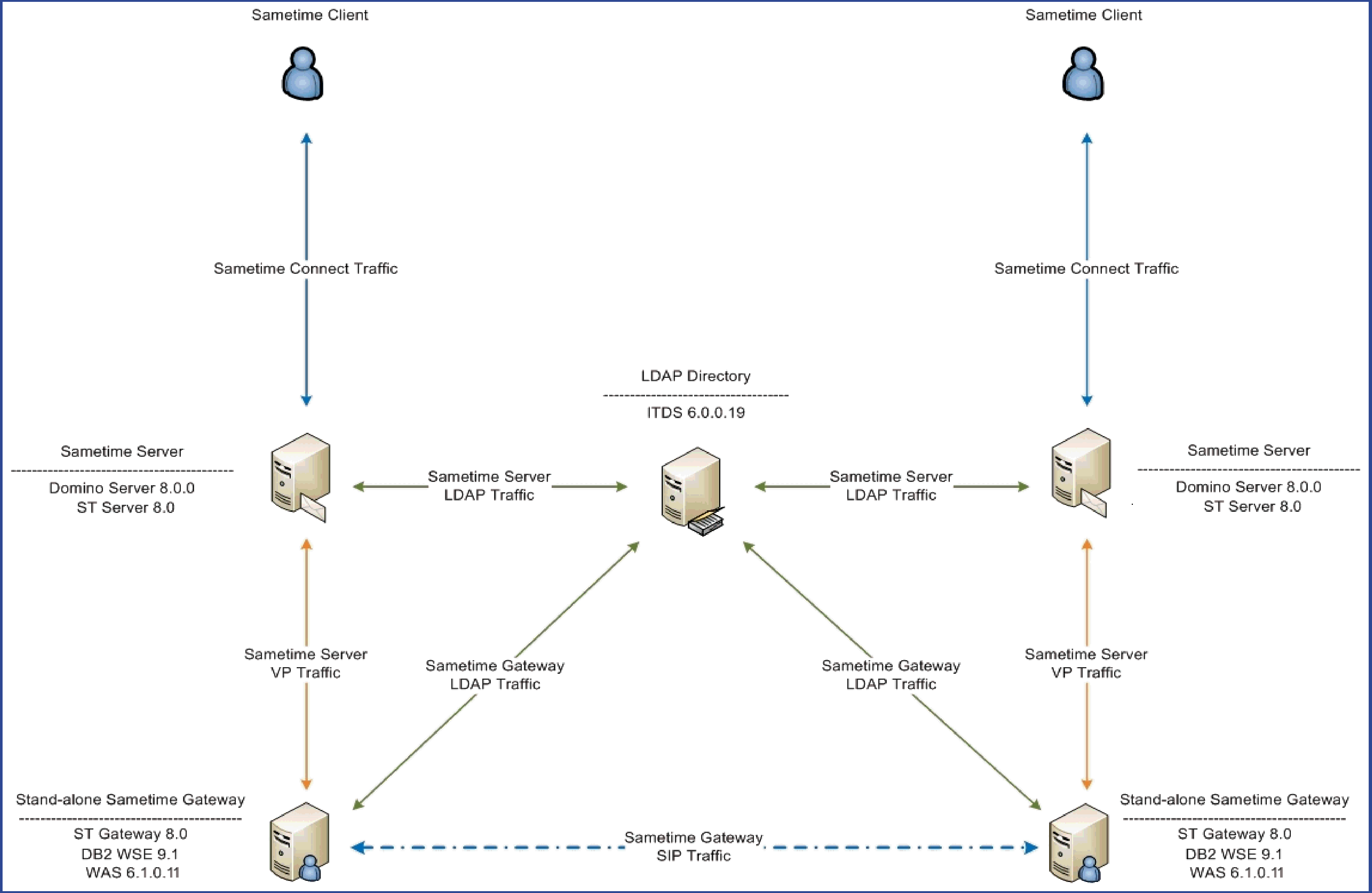
Option	Description
SIP for RTC	Use **SIP for RTC** for connections to other RTC Gateway communities.
SIP for AOL	Use **SIP for AOL** for all AOL Instant Messaging and AOL Clearinghouse community connections.
SIP for Sametime SIP Gateway	Use **SIP for Sametime SIP Gateway** for Sametime versions 7.0, 6.5.1, or 3.1 connections only.
SIP for Yahoo	Use **SIP for Yahoo** to connect with communities that use Yahoo! Messenger
XMPP	Use **XMPP** to connect with communities that use Google Talk.

Where We Stand At This Point In the Install

Sametime Gateway



An Alternate Look



Registering Sametime with AOL

- You need to register your Sametime Gateway server with AOL Public IM Services
    - As described on Slide 29, you download the form from IBM
    - You’ll need your Passport ID and organization site number
- Submit the online form
- Wait about seven days for an email confirming your acceptance into the connection

Registering Sametime with AOL (cont.)

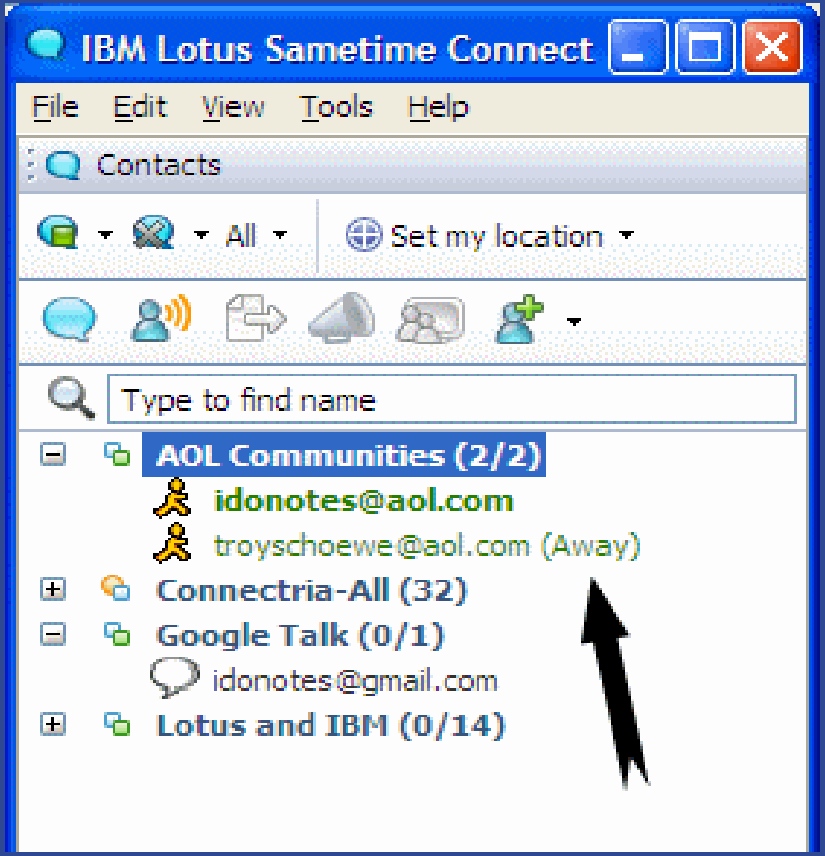
1. Download the AOL/Yahoo Provisioning Form from:
   - http://www.ibm.com/software/lotus/sametime/federation

2. Complete the required information
   - Gateway name — The name of the Lotus Sametime Gateway server in your environment.
   - Gateway hostname —The hostname of the Lotus Sametime Gateway server. The hostname is used to direct instant messages to your community.
   - Provider name — AOL.
   - Contact email — The email address of your organization’s contact, such as the Lotus Sametime administrator, who will receive email notification of provisioning events.
   - Domain names — One or more domains for your Lotus Sametime servers. Include domains of all Lotus Sametime users in your community.

Adding the AOL Clearinghouse

- Much like adding communities previously
  - Community type is Clearinghouse
  - Choose SIP for AOL as the protocol
    - sip.oscar.aol.com is the hostname for connectivity
  - TLS is required
  - Assign users that can use the connection

What Does the Client See?



AOL Communities (2/2)

idonotes@aol.com

troyschoewe@aol.com (Away)

Connectria-All (32)

Google Talk (0/1)

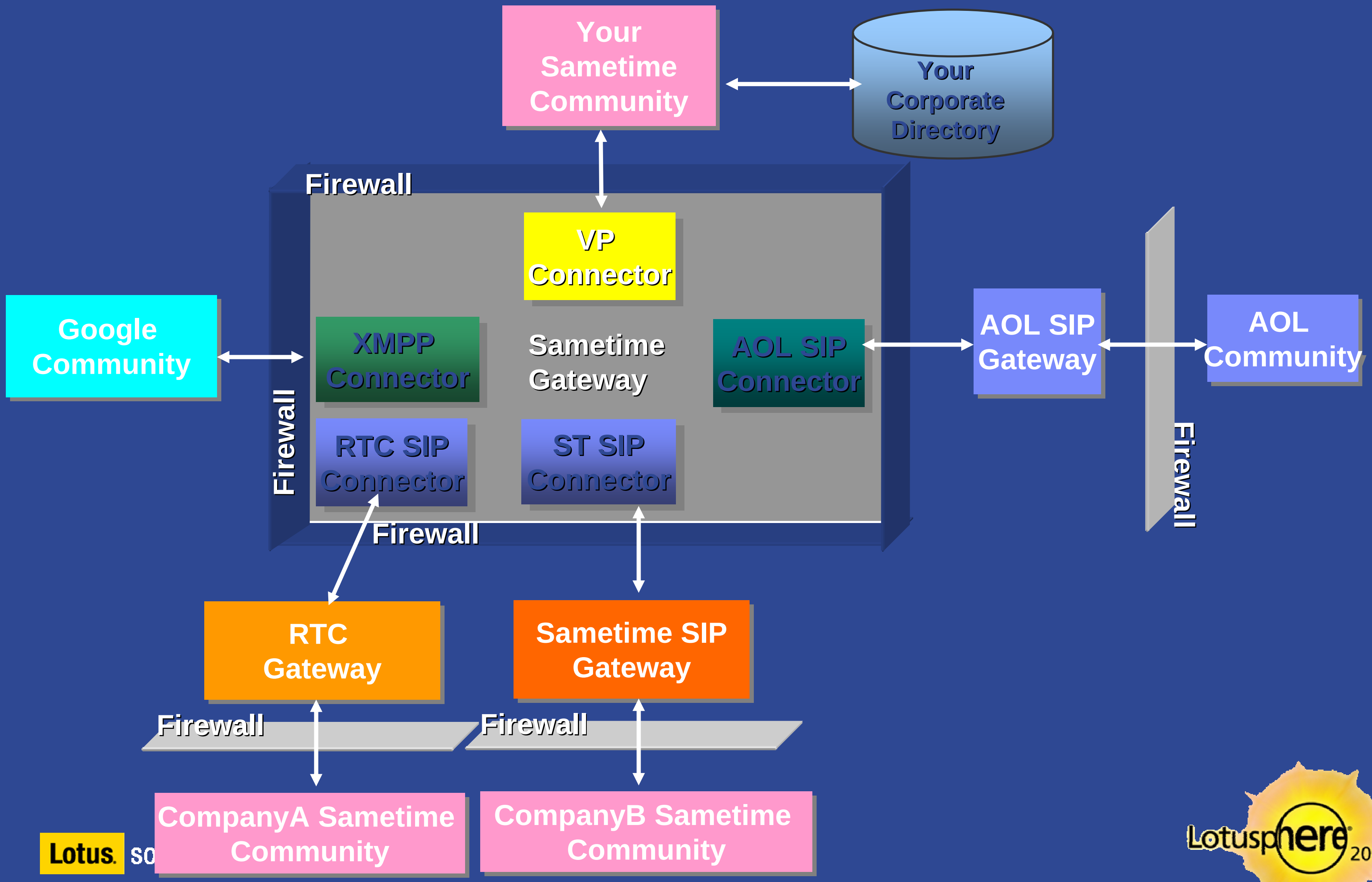
idonotes@gmail.com

Lotus and IBM (0/14)

Connecting to Google Talk

- Google Talk uses Extensible Messaging and Presence Protocol (XMPP)
- It uses built-in encryption
- Requires a DNS Service Record (SRV) published to DNS
  - SRV entry must be made
- Note that Google Talk currently only supports a single Sametime Gateway server — no clusters

Where We Stand in the Install Process Now



Your Sametime Community

Your Corporate Directory

Firewall

VP Connector

Google Community

XMPP Connector

Sametime Gateway

AOL SIP Connector

AOL SIP Gateway

AOL Community

Firewall

Firewall

RTC SIP Connector

ST SIP Connector

Firewall

RTC Gateway

Sametime SIP Gateway

Firewall

Firewall

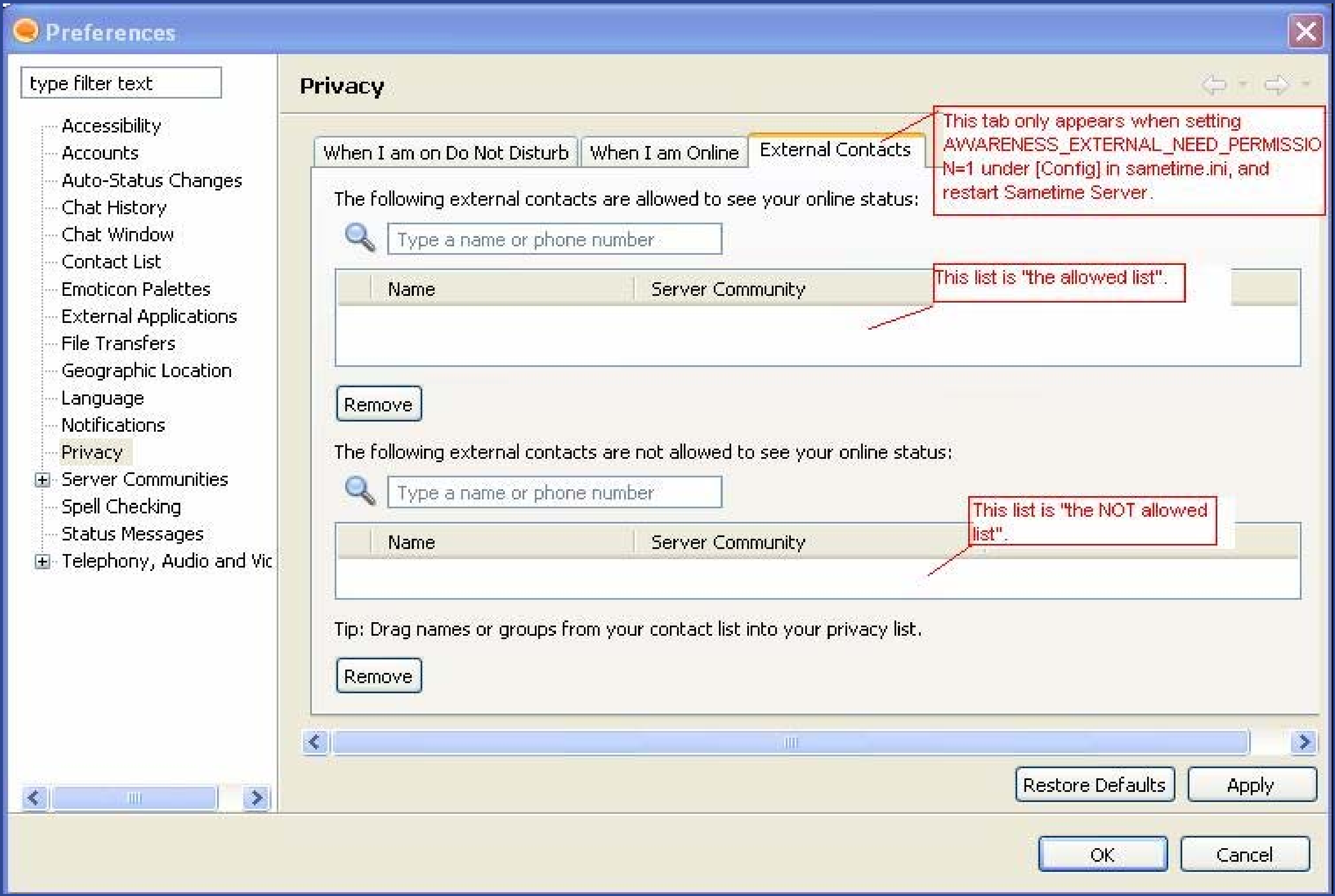
CompanyA Sametime Community

CompanyB Sametime Community

A Bonus Feature

- Requiring external users to request permission to see online status
  - This feature was introduced after many requests to hide your status from external users
  - ;Sametime.ini
  - [Config]
  - AWARENESS_EXTERNAL_NEED_PERMISSION=1
- This feature seems to work well with Sametime to Sametime connections through the gateway, but still is spotty in gateway to the public providers

What the End User Sees in the Client



This tab only appears when setting AWARENESS_EXTERNAL_NEED_PERMISSION=1 under [Config] in sametime.ini, and restart Sametime Server.

The following external contacts are allowed to see your online status:

Type a name or phone number

This list is "the allowed list".

The following external contacts are not allowed to see your online status:

Type a name or phone number

This list is "the NOT allowed list".

Tip: Drag names or groups from your contact list into your privacy list.

Extending the Gateway with Message Handlers

- You can extend the Sametime Gateway by adding a message handler
  - It can perform instant message spam filtering (SPIM), virus checking, additional logging, additional protocol translators
- A message handler must be added as a J2EE application to WebSphere first
  - Then you use the Sametime Gateway console to manage the properties
- Third-party vendors can utilize the Sametime Gateway API to build additional functionality
- As of this writing, there are no message handlers available from IBM or its partners

Assigning Users

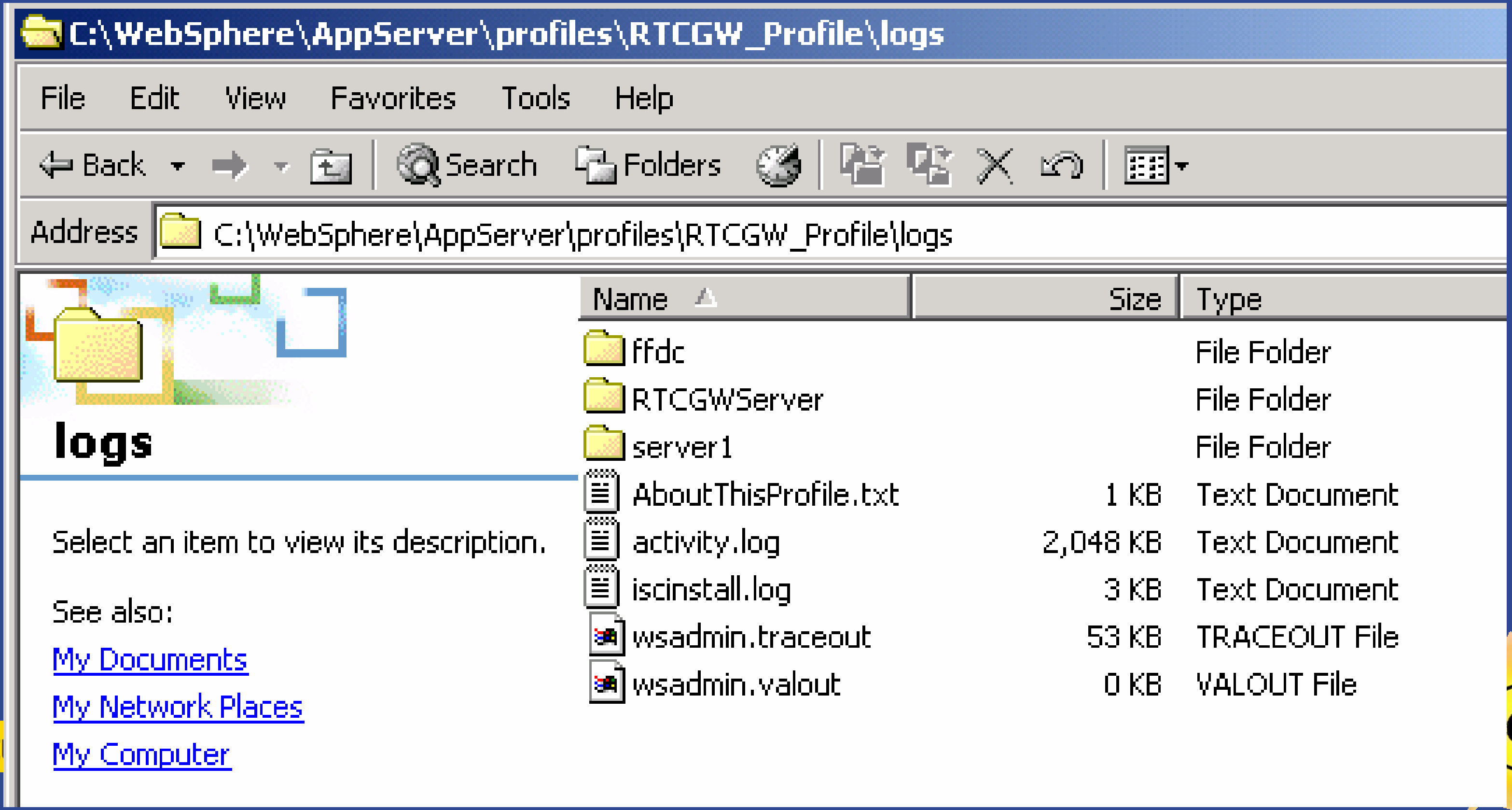
- I already mentioned that you need to assign users to each connection, but you have some options
  - Determine if you want to assign equal access to the community for everyone or set access for each user.
  - Keep in mind we are talking about internal community assignment only. External users will see the gateway after an internal user subscribes to the external service.
  - Groups, of course, can be used here.
- You can also use the Find Users tool to see who is assigned to which connection

Managing User Access Properties

- Maximum sessions — global setting
  - This will control the maximum number of connections to the entire gateway, not just a particular service
  - There is also a per community setting
- Blacklist domains
  - Use FQDN or IP addresses separated by a comma, semicolon, or space
  - Wildcards using an asterisk in the left-most subdomain position are allowed
- Session timeout per community
  - 60 minutes of inactivity is default
- Subscription timeouts both global and community
  - Applies to presence capability

Logging and Tracing Enablement

- Basic logging is enabled by default
- Traces are logged to [WASAppServer]\profiles\RTCGW_Profile\logs



C:\WebSphere\AppServer\profiles\RTCGW_Profile\logs

C:\WebSphere\AppServer\profiles\RTCGW_Profile\logs

logs

Select an item to view its description.

See also:

My Documents

My Network Places

My Computer

Name	Size	Type
ffdc		File Folder
RTCGWServer		File Folder
server1		File Folder
AboutThisProfile.txt	1 KB	Text Document
activity.log	2,048 KB	Text Document
iscinstall.log	3 KB	Text Document
wsadmin.traceout	53 KB	TRACEOUT File
wsadmin.valout	0 KB	VALOUT File

Troubleshooting (as in the Wild Wild West)

- IBM Trace and Request Analyzer for WAS
  - http://www.alphaworks.ibm.com/tech/trace

- Performance Monitoring Infrastructure (PMI)
  - Built into the Websphere Administration Console (ISC)
  - Monitoring and Tuning -> Performance Monitor Infrastructure -> RTCGWServer
    - Or SametimeGateway
  - Click Custom and then Apply and Save. Then enter custom again
  - Open the Runtime tab and enable the Sametime Gateway stats you wish

  - Click Monitoring and Tuning -> Performance Viewer -> Current Activity
  - Performance Viewer page, click RTCGWServer -> Performance Modules
  - Start logging and issue a subscribe request

This is us!

How to contact:
Chris Miller
IdoNotes@IdoNotes.com
Blogging at http://www.IdoNotes.com
Podcasts on iTunes and the blog site
IdoNotes on all your IM frequencies
IdoNotes on Twitter

How to contact:
Troy Schoewe
troy@connectria.com
Troyschoewe on AOL