3170 Live Communications Server: Under The Hood

Kieran McCorry
Principal Consultant
Hewlett-Packard

Agenda

- Microsoft's LCS Server Introduction
- An Introduction to SIP
- Client Configuration
- Installation Information
- LCS Home Server
- LCS Forwarding Proxy
- LCS Front End Server
- Topologies
- Message Logging
- Summary

Why Live Communications Server (LCS)?

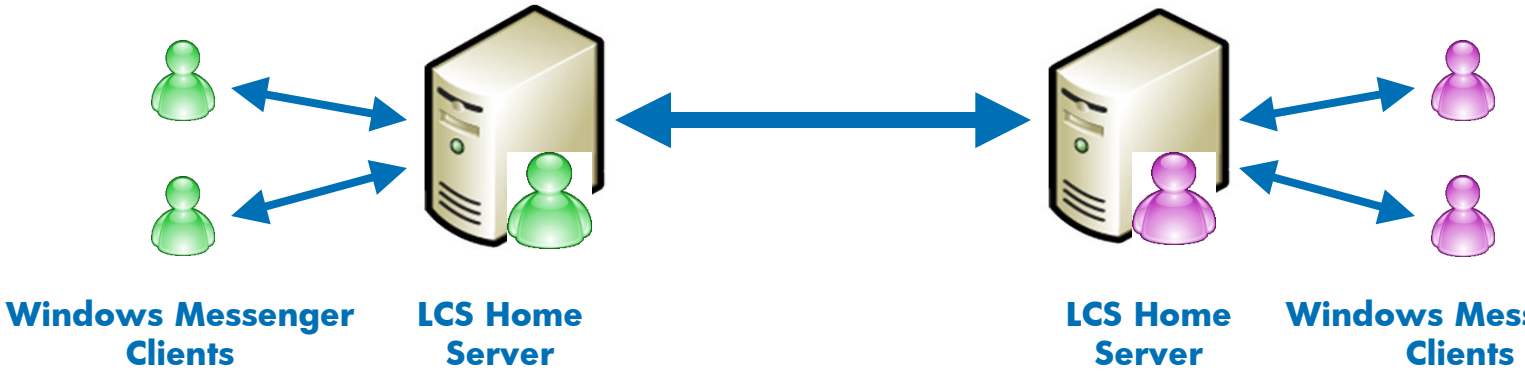
- Hybrid of traditional communications mechanisms
  - Telephone
  - E-Mail
- Presence functionality is arguably the most important feature
- Other considerations
  - Great for short, staccato information exchanges
  - Immediacy is a great benefit
    - But interruption is still a problem
    - Group threads non scalable over four participants
      - Multiple conversations swamp users

LCS Server Evolution

- Previously on Microsoft…
  - Exchange 2000 Instant Messaging Server
    - Text-based Instant Messaging (IM)
    - Used proprietary RVP protocol for IM
  - Exchange 2000 Conferencing Server provided support for
    - Audio/Video Conferencing
    - Application Sharing
    - H.323 and T.120 for AV and Application Sharing

LCS Server Architectural Fundamentals

- Windows Messenger Clients establish connection to LCS Server(s)
- LCS Server(s) performs several key functions:
  - Authenticates client connections with Active Directory
  - Maintains Presence information about Clients
  - Facilitates user-to-user communications
    - Either intra-server or inter-server



An Introduction to SIP

A Brief History of SIP

- Feb 1996: draft-ietf-mmusic-sip-00, 1 request type
- Dec 1996: draft-ietf-mmusic-sip-01, 2 request types
- Jan 1999: draft-ietf-mmusic-sip-12, 6 methods
- Mar 1999: RFC 2543 Session Initiation protocol (SIP)
  - 6 methods (153 page spec)
- Dec 2000: draft-ietf-sip-rfc2543bis-02
- 2001: New SIP Working Groups formed, including
  - SIMPLE
    - SIP Instant Messaging and Presence Leveraging Extensions
      -
- Jun 2002: RFC 3261 Session Initiation Protocol
- Jun 2002: RFC 3263 SIP: Locating SIP Servers
- Dec 2002: RFC 3428 SIP Extension for Instant Messaging

Client/Server Connections Using SIP

- SIP's only function is to set up a communications session
  - In this case between Client and Server, but also
  - Between servers
- Provide basic signaling between participants
- Define nature of the communication used within the session (use SDP, RFC 2327)
  - Media type (e.g., audio, video, etc.)
  - Transport protocol (e.g., RTP, RTSP, H.320)
  - Media format (e.g., H.261, MPEG)
- Use some other protocol for content delivery
  - RTP or RTSP
- Only exception is IM
  - Content is delivered in-band

Fundamental SIP Architectural Components

- SIP User Agent (UA)
  - SIP User Agent Client (UAC)
  - SIP User Agent Server (UAS)
- SIP Proxy Server
- SIP Redirection Server
- SIP Registrar

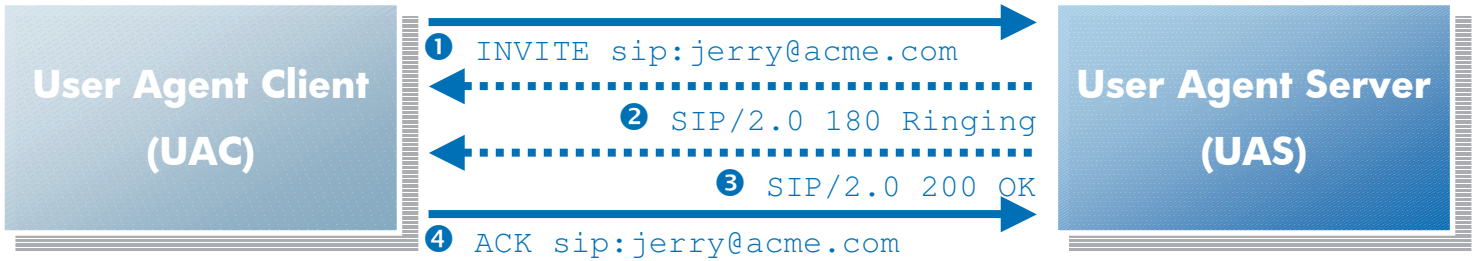
Basic SIP Methods

- INVITE
  - Issued by a UAC to establish a session
- ACK
  - Issued by a UAC to confirm session up
- OPTIONS
  - Allows a UAC to query another's capabilities (e.g., methods, content types, codecs, etc.)
- BYE
  - Terminates the entire session
- CANCEL
  - Cancels a transaction within the session
- REGISTER
  - Identifies a UAC contact information with a SIP Registrar

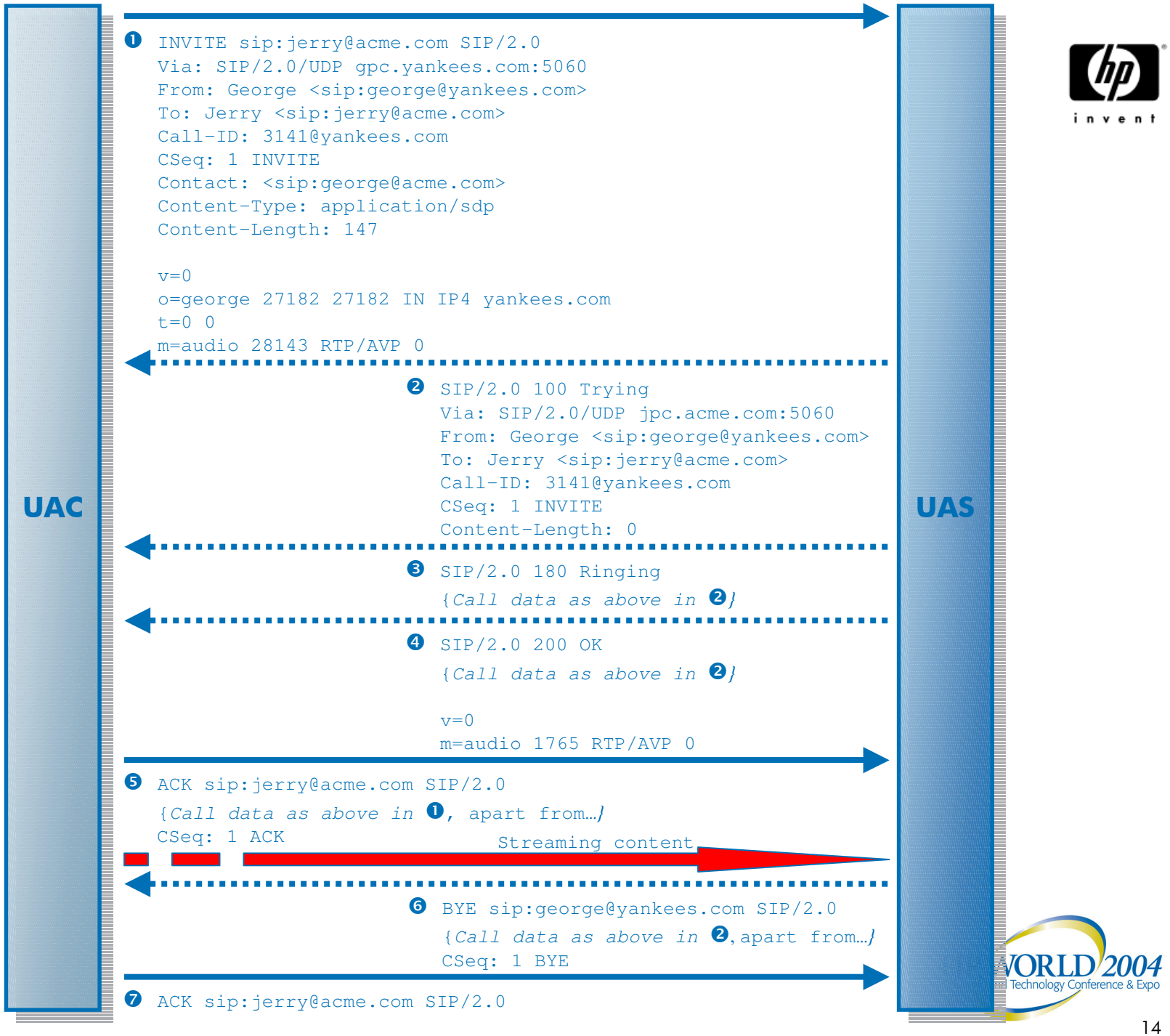
Basic SIP Protocol Packet

```
INVITE sip:jerry@acme.com SIP/2.0
Via: SIP/2.0/UDP gpc.yankees.com
From: George <sip:george@yankees.com>
To: Jerry <sip:jerry@acme.com>
Call-ID: 3141592654@yankees.com
Content-Type: application/sdp
Content-Length: 27182
CSeq: 1 INVITE
Subject: A show of numbers?
...
```

Basic SIP Client/Server Exchange



A Complete SIP Session


UAC
UAS
❶ INVITE sip:jerry@acme.com SIP/2.0
Via: SIP/2.0/UDP gpc.yankees.com:5060
From: George <sip:george@yankees.com>
To: Jerry <sip:jerry@acme.com>
Call-ID: 3141@yankees.com
CSeq: 1 INVITE
Contact: <sip:george@acme.com>
Content-Type: application/sdp
Content-Length: 147
v=0
o=george 27182 27182 IN IP4 yankees.com
t=0 0
m=audio 28143 RTP/AVP 0
❷ SIP/2.0 100 Trying
Via: SIP/2.0/UDP jpc.acme.com:5060
From: George <sip:george@yankees.com>
To: Jerry <sip:jerry@acme.com>
Call-ID: 3141@yankees.com
CSeq: 1 INVITE
Content-Length: 0
❸ SIP/2.0 180 Ringing
{Call data as above in ❷}
❹ SIP/2.0 200 OK
{Call data as above in ❷}
v=0
m=audio 1765 RTP/AVP 0
❺ ACK sip:jerry@acme.com SIP/2.0
{Call data as above in ❶, apart from…}
CSeq: 1 ACK
Streaming content
❻ BYE sip:george@yankees.com SIP/2.0
{Call data as above in ❷, apart from…}
CSeq: 1 BYE
❼ ACK sip:jerry@acme.com SIP/2.0

SIP Extensions for IM

```
MESSAGE sip:jerry@acme.com SIP/2.0
Via: SIP/2.0/UDP gpc.yankees.com
From: George <sip:george@yankees.com>
To: Jerry <sip:jerry@acme.com>
Call-ID: 3141592654@yankees.com
Content-Type: text/plain
Content-Length: 35
CSeq: 1 MESSAGE

This is some IM Text!!
```

SIP Extensions For Presence

```
SUBSCRIBE sip:jerry@acme.com SIP/2.0
Via: SIP/2.0/UDP gpc.yankees.com
From: George <sip:george@yankees.com>
To: Jerry <sip:jerry@acme.com>
Call-ID: 3141592654@yankees.com
CSeq: 1 SUBSCRIBE
Contact: <sip:george@yankees.com>
Content-Length: 0
```

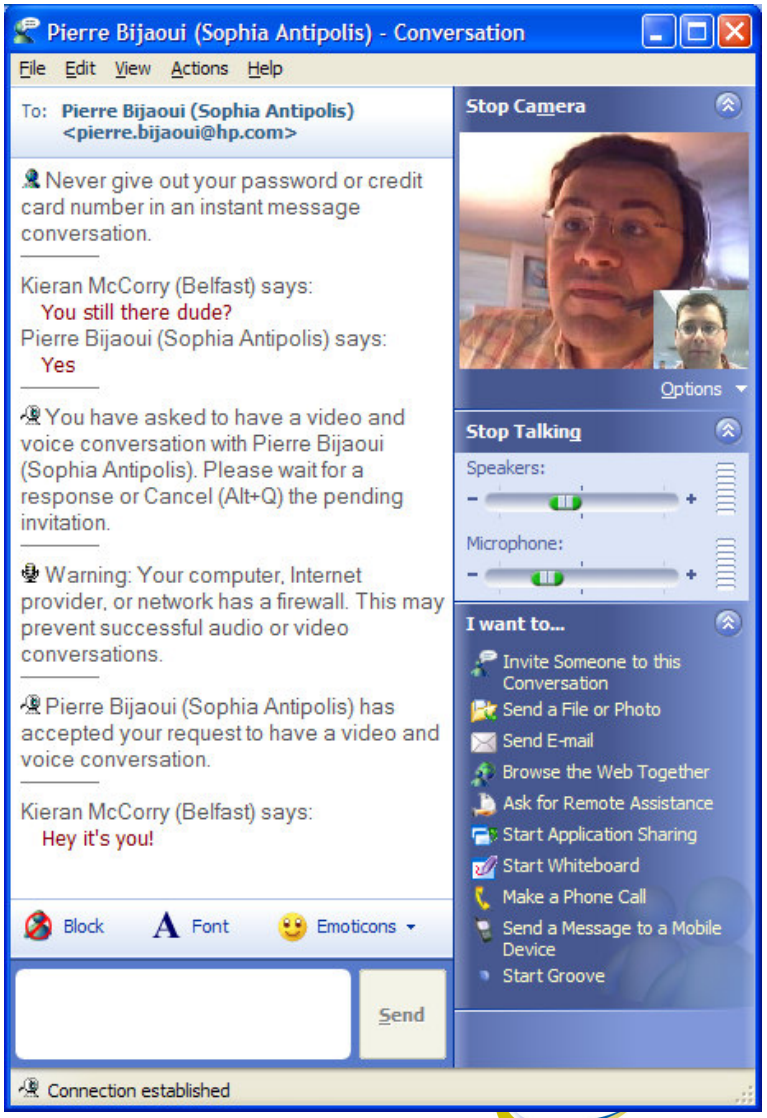
```
NOTIFY sip:george@yankees.com SIP/2.0
Via: SIP/2.0/UDP siprelay.acme.com
From: Jerry <sip:jerry@acme.com>
To: George <sip:george@yankees.com>
Call-ID: 3141592654@yankees.com
Content-Type: application/cpim-pidf+xml
Content-Length: 1673
CSeq: 1 NOTIFY

[PIDF Document]
```

Client Configuration

Client Connections

- Windows Messenger Client is very functional
  - Instant Messaging
  - Presence Notifications
  - File Transfer
  - Office Integration
  - Application Sharing
  - Audio/Video Communication

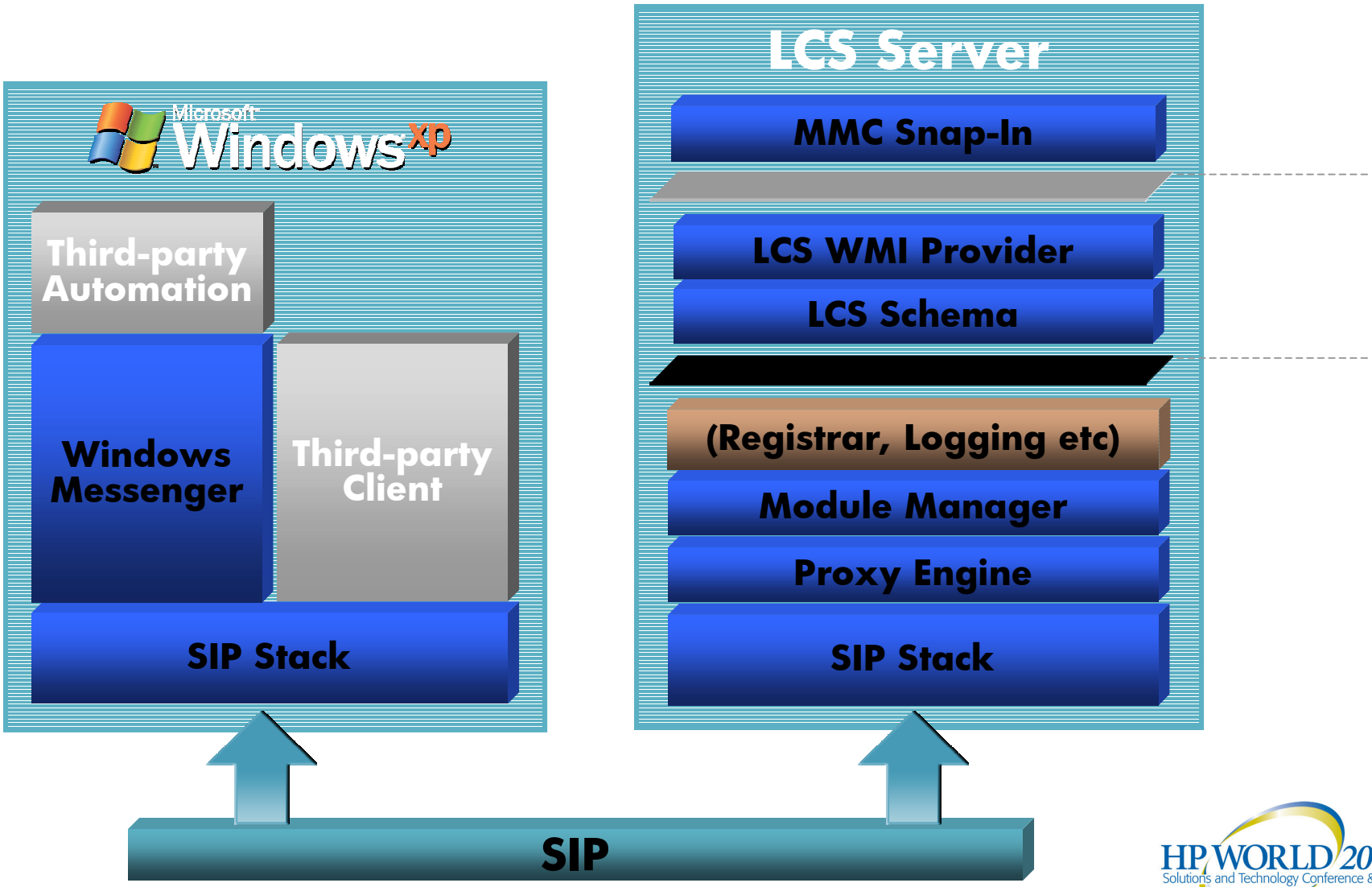


Windows Messenger 5.0 Client

- Triple Stack Client
  - MSN
  - Exchange IM
  - LCS Service
- Richest Experience on Windows XP Platform

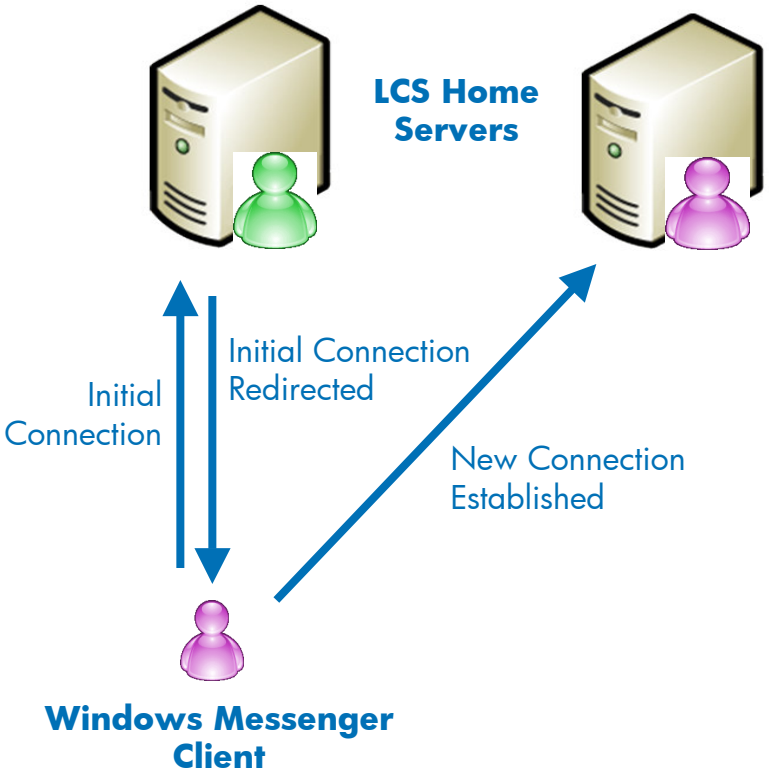
Feature / Platform	IM	Voice	Presence	File Transfer	Acoustic Echo Cancellation	Video	White board	App Sharing
Windows XP	✓	✓	✓	✓	✓	✓	✓	✓
Windows 2000	✓	✓	✓	✓	✗	✗	✗	✗

Client/Server Architecture



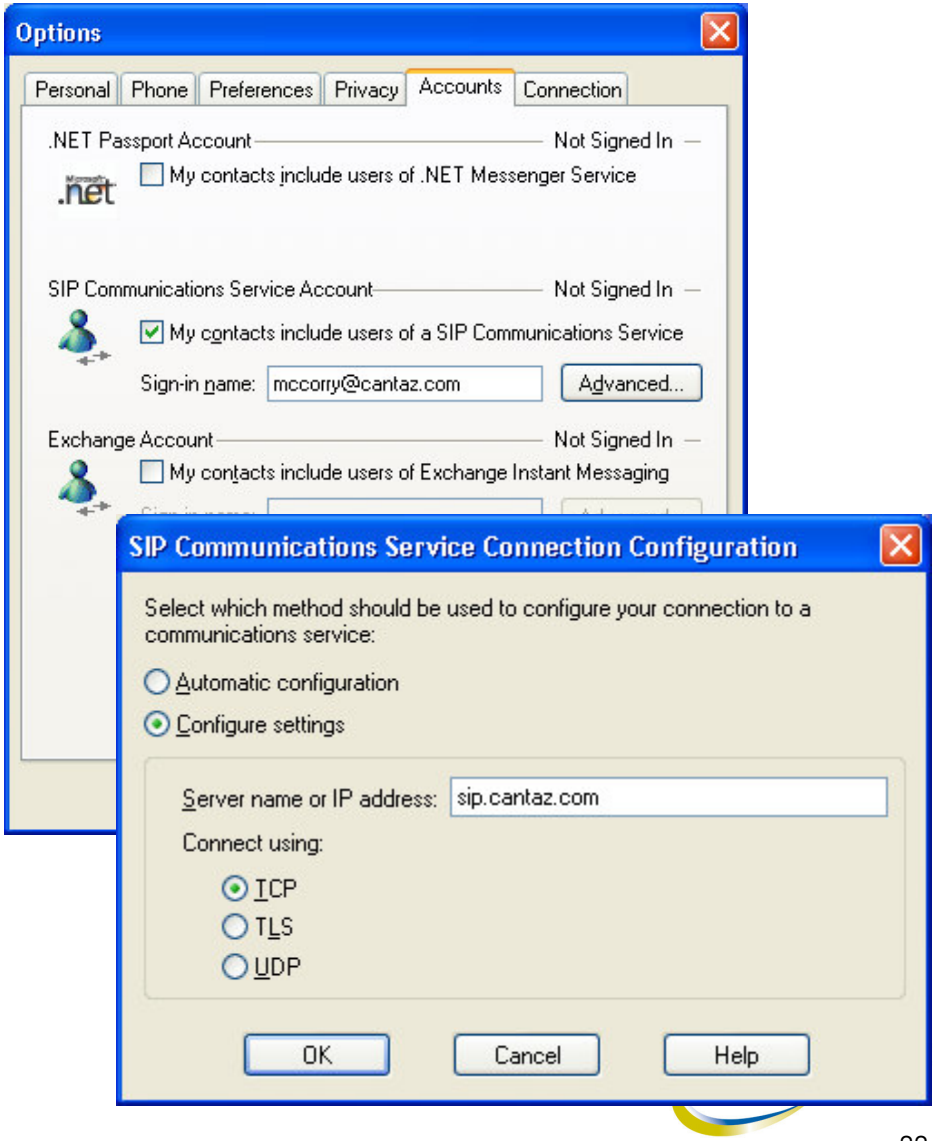
Client Connections

- Connections from Client to Server established over
  - SIP (TCP)
    - C/S: [>1024]→5060
      - Cannot be locked down
    - S/C: 5060←[>1024]
  - SSL/TLS
    - C/S: [>1024]→5061
      - Note: can also use 443
- No server support for SIP (UDP)
  - But client supports this mechanism for interoperability
- Home Server will REDIRECT client connections to other servers if client not homed on the local Home Server



Client Connection Configuration

- From the Messenger Client
  - Options\Accounts
    - Enter your SIP sign-in name
  - Advanced
    - Select the Connection mechanism
      - TCP or TLS
      - Add the Fully Qualified Domain Name of the server running LCS
    - Connections can be made automatically
      - Requires infrastructure configuration to allow clients to automatically connect to a SIP server without entering any SIP server information on the client



Automatic Client Configuration

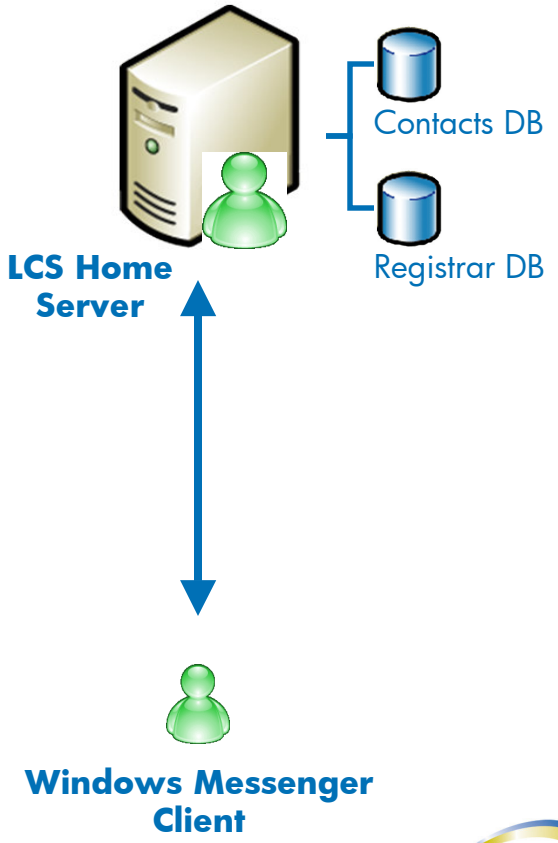
- Configure DNS Service Location (SRV) Resource Record (RR)
  - _sip._tcp.<domain.com>
  - _sip._tls.<domain.com>
  - e.g.,
    - _sip._tcp.cantaz.com
- SRV Record maps to the SIP Server Fully Qualified Domain Name
- When client set to automatic configuration, discovery order is
  - TCP, then
  - TLS

Connection Authentication

- Client must typically specify three authentication items
  - SIP sign-in name
  - Windows Domain and Username
  - Windows password
- SIP sign-in name is checked against the SIP Registrar Database
  - Ensure sign-in valid
- Windows credentials checked against Global Catalog server

Client Contacts and Home Server Databases

- Home Server uses MSDE to store information in two databases
  - Contact Information
  - Registrar Information
    - Presence state of 'homed' clients
- Upon client connection
  - Server contacts downloaded to client cache
  - Using MSDE allows for fast access
- Thus Contacts 'roam' with clients



Maintaining Contacts

- User may search the Active Directory to add contacts to their Contacts List
- Users' 'searchability' from the Active Directory can also be controlled using ACLs
  - Administrator controlled
  - Set from AD Users and Computers OU Security tab
    - Enable or Disable
      - ReadRTCUserSearchPropertySet
  - Property can be set on an OU and inherited
    - Not applicable to groups

Group Policy

- Group Policy
  - GP Templates can be used to control the feature set made available to Windows Messenger users

Installation Information

Installation Information

- LCS only supported on Windows Server 2003
- Can exist in native mode domains within Windows 2000 DCs
  - Hardware Recommendations
    - 1GHz P4 or higher
    - 512MB memory or higher
    - 'Suitable' IO configurations
- Installation performs schema modifications
  - Requires Schema Admin permissions
- LCSService Account created at installation
  - Member of RTCHSDomainService
  - Special account created under which the RTC Service is run
- LCSDomainServerAdmins Group created at installation
  - Server administrators can administer all settings on a server
  - Can move users from server to server
- LCSDomainUserAdmins
  - Manage all user settings for a user
    - Change SIP URI, add/remove entries from block/allow list

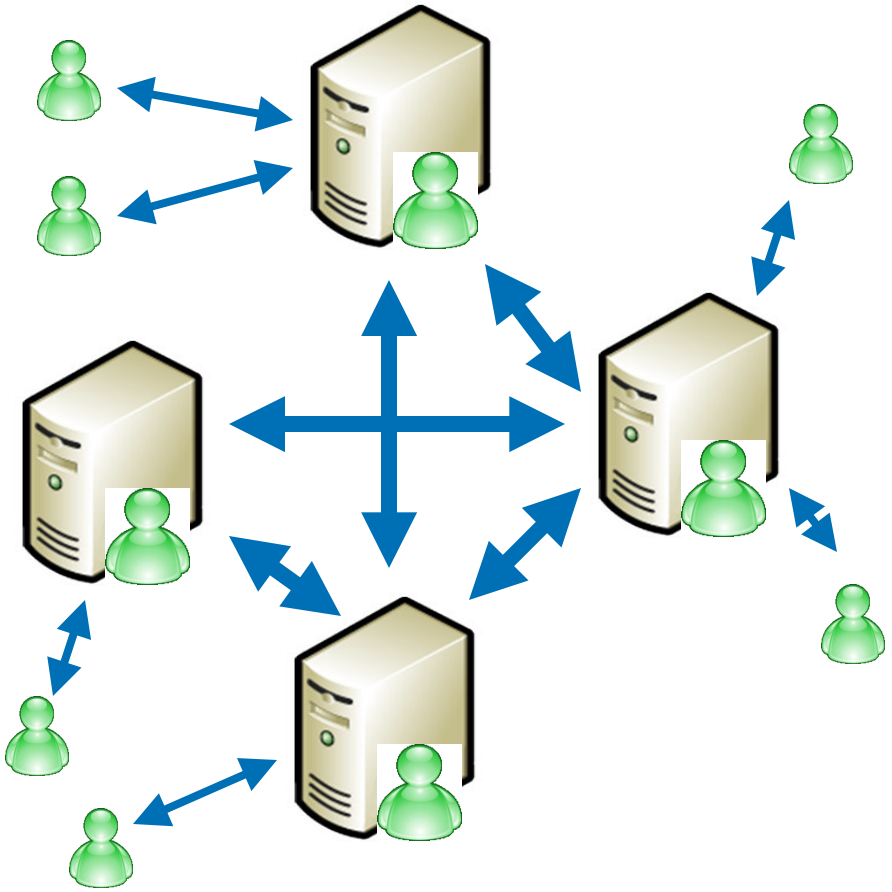
LCS Home Server

LCS Server Functions

- Server Roles
  - Home Server
  - Forwarding Proxy
  - Front End Server
- These roles may be combined so that a single server performs multiple roles
- You must also provide Active Directory GCs/DCs for
  - Configuration information
  - User Authentication
- DC/GC discovered by normal Windows Site Discovery process
- LCS Servers can utilize a variety of other technologies
  - Active Directory
  - SQL Server

LCS Home Servers

- Home Servers
  - Act as a rendezvous point for IM communications
    - Users are 'homed' on a Home Server
  - Communicate with each other in a peer-to-peer fashion
    - No hub-and-spoke
  - All inter-server communication is with Mutual TLS connections
  - Support in the region of 10000 users per Home Server



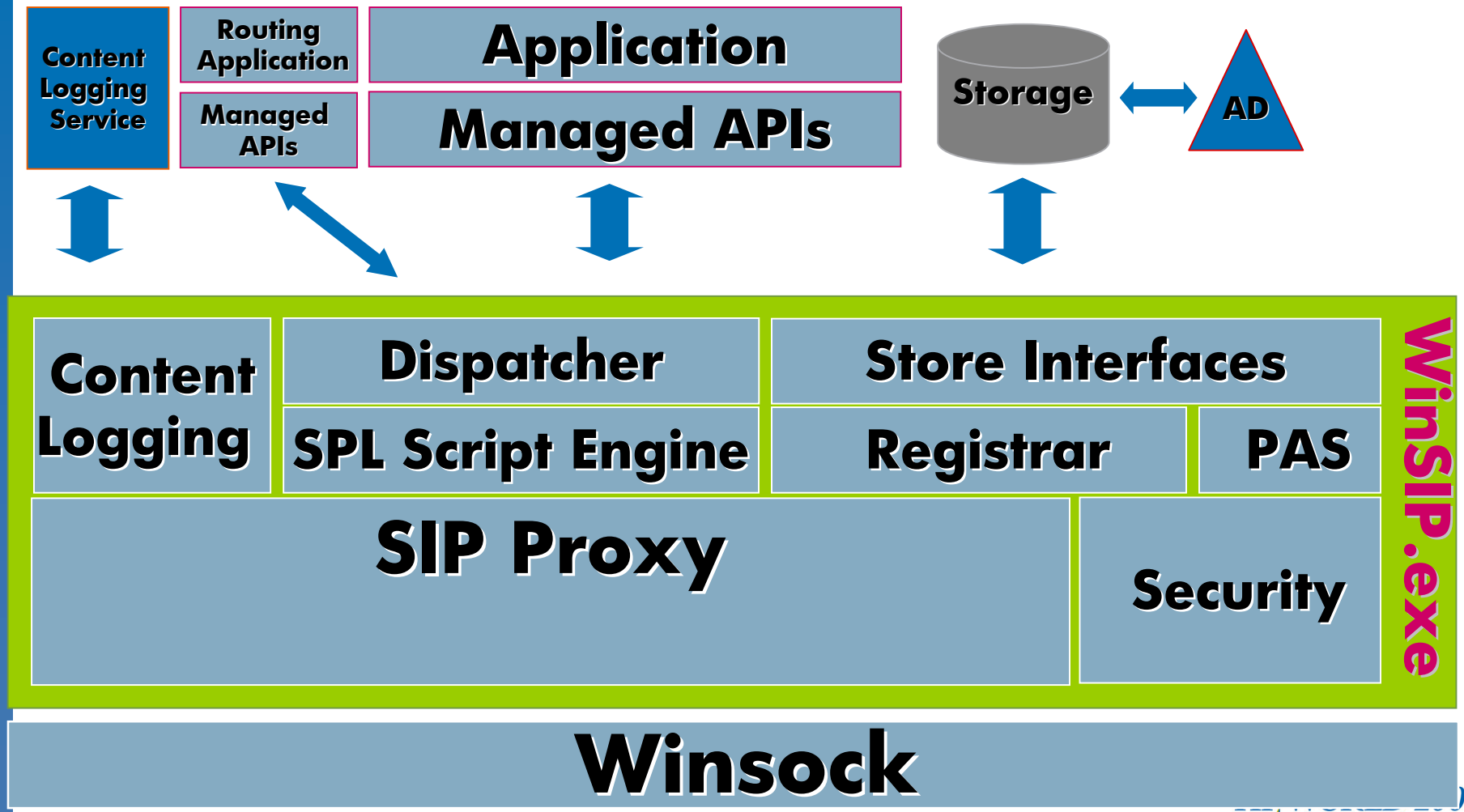
Home Servers and Mutual TLS

- All inter-server traffic uses Mutual TLS, therefore
  - Each HS must have a certificate that can be used as both
    - Server Certificate
    - Client Certificate
  - Within an enterprise use a common PKI infrastructure
    - Servers should trust each others' CA and a common CA
- The certificate names must much the server names
  - Take care planning all naming structures in advance.

LCS Home Server Components

- Main Components
  - SIP Proxy
  - SIP Registrar
  - Presence Agent Server (PAS)
  - Store
- Other Components
  - Content Logging Functions
  - Customization/Extendibility

Home Server Architecture



Home Server Component Descriptions 1 of 3

- SIP Proxy
  - Performs routing functions
  - Uses route header in SIP packets
  - AD lookups used for destination SIP URIs
    - Used to send an IM
  - Static routing used for originator SIP URIs (optional)
    - Used to connect a client to a specific Home Server
    - User information held in AD will override
- Security
  - User authentication using either Kerberos or NTLM
  - Client/Server authentication over SSL/TLS
  - Server/Server authentication over Mutual TLS

Home Server Component Descriptions 2 of 3

- SIP Registrar
  - Maintains mapping table of SIP URIs to endpoint addresses
    - i.e., knows 'where' a user is logged in
- PAS
  - Maintains contacts, active subscriptions, presence information, ACLs for users, pending subscriptions
    - For the local user
    - Subscriptions to other users' presence is maintained by remote Home Server
- Store
  - Instantiation of presence information above
  - User Information
    - LCS enabled/disabled status, SIP URI, Home Server attributes, etc.
      - Held locally so that AD not queried continually; better performance
      - Downloaded synch from AD

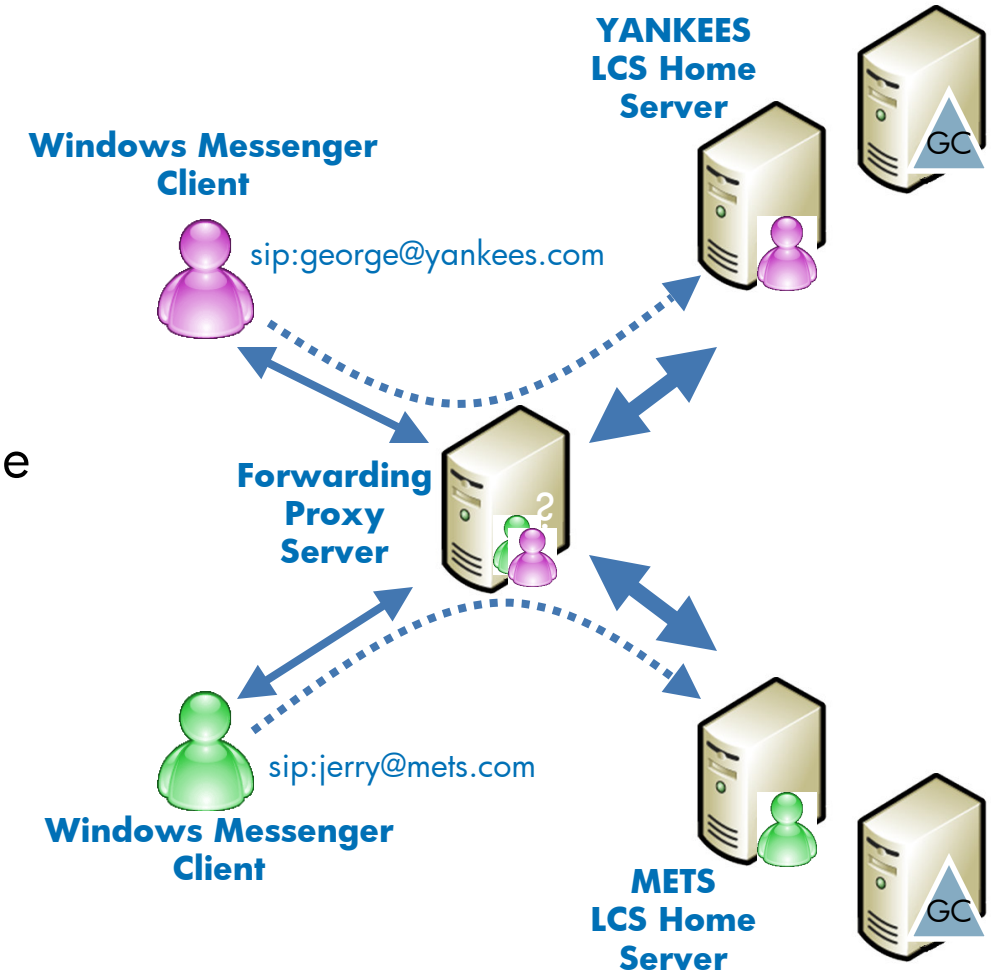
Home Server Component Descriptions 3 of 3

- Server APIs
  - Allows LCS-integrated applications to run on server
  - Separate process space per application
- SIP Programming Language (SPL)
  - Runs in-proc
  - Subset of C#
  - Functions for filtering and routing

LCS Forwarding Proxy

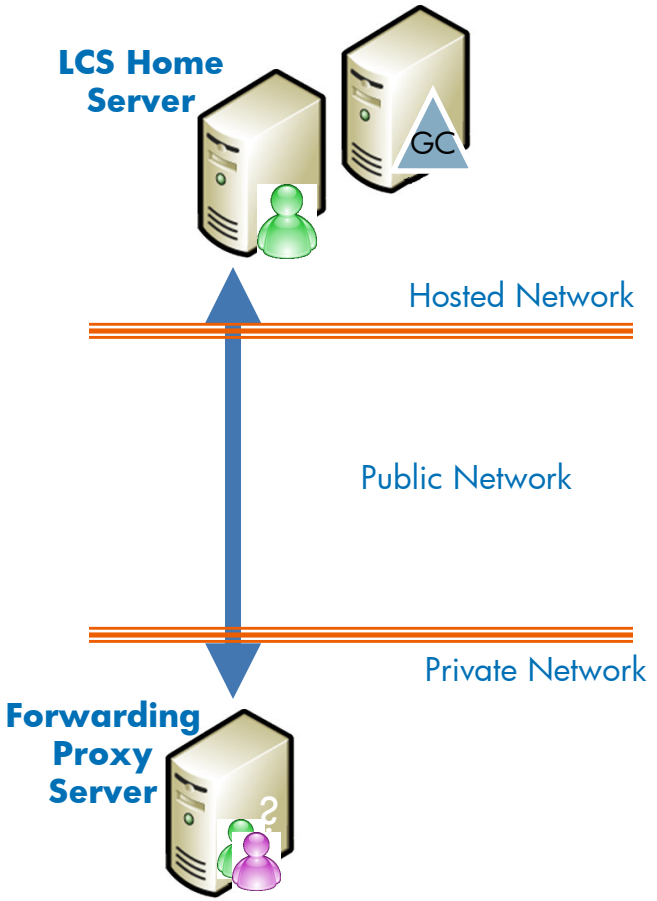
LCS Forwarding Proxy

- Acts solely as a relay for SIP messages
- Inspects the originator SIP URI
  - decides how to route this connection request to a Home Server
  - Uses static routing table
- Performs no authentication
- Forwarding Proxy
  - ALWAYS proxies
  - NEVER redirects



Forwarding Proxy Topology Example

- Forwarding Proxy Server useful
  - when internal clients will connect to external service
  - TCP client connections will traverse internal firewalls
    - Use Mutual TLS between Forwarding Proxy and Home Server
      - No need to deal with ephemeral ports

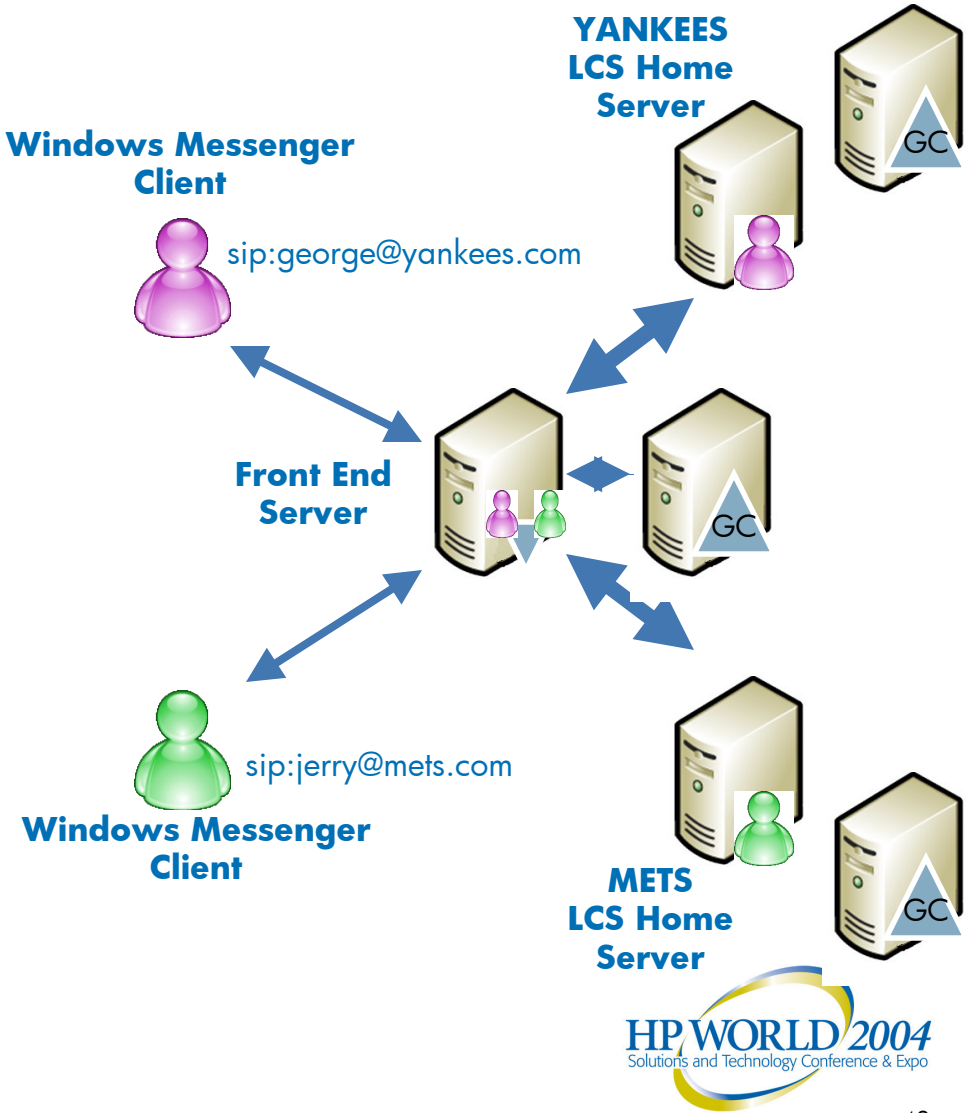


Windows Messenger Client

LCS Front End Server

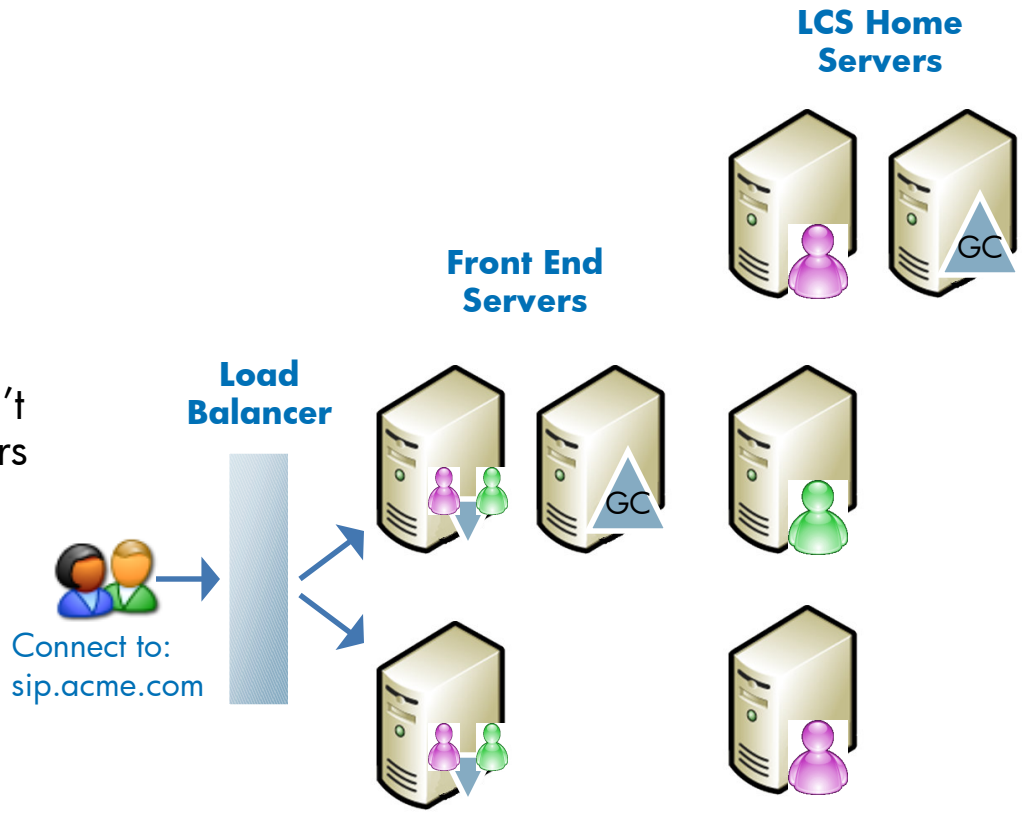
LCS Front End Server

- Effectively a Home Server that does not 'home' any users
- Inspects the originator SIP URI
  - decides how to route this connection request to a Home Server
  - Queries Active Directory to determine Home Server for originator
- Authenticates the originator
- Front End Server will
  - Proxy or Redirect connections
    - Determined by configuration on the server



LCS Front End Server Topology

- In Front End Server environment
  - Namespaces are normalized
    - No need to specify server specific SIP URIs
      - Or have server specific connections
      - (although technically this isn't needed anyhow since servers will redirect intrinsically)
  - All client configurations should point to the Front End Server
    - If you have multiple Front End Servers consider
      - Hardware Load Balancing, or
      - Round Robin DNS

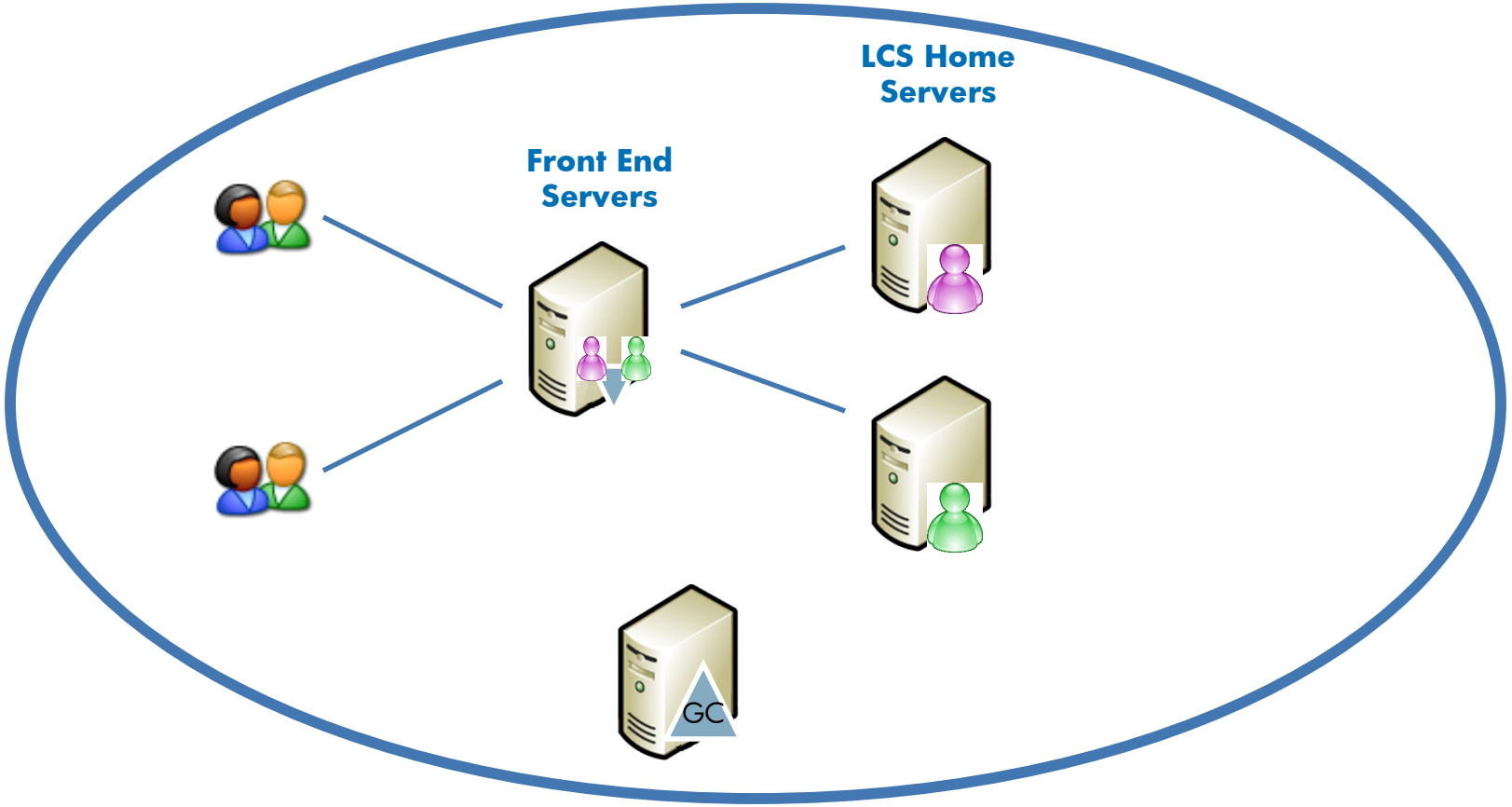


Topologies

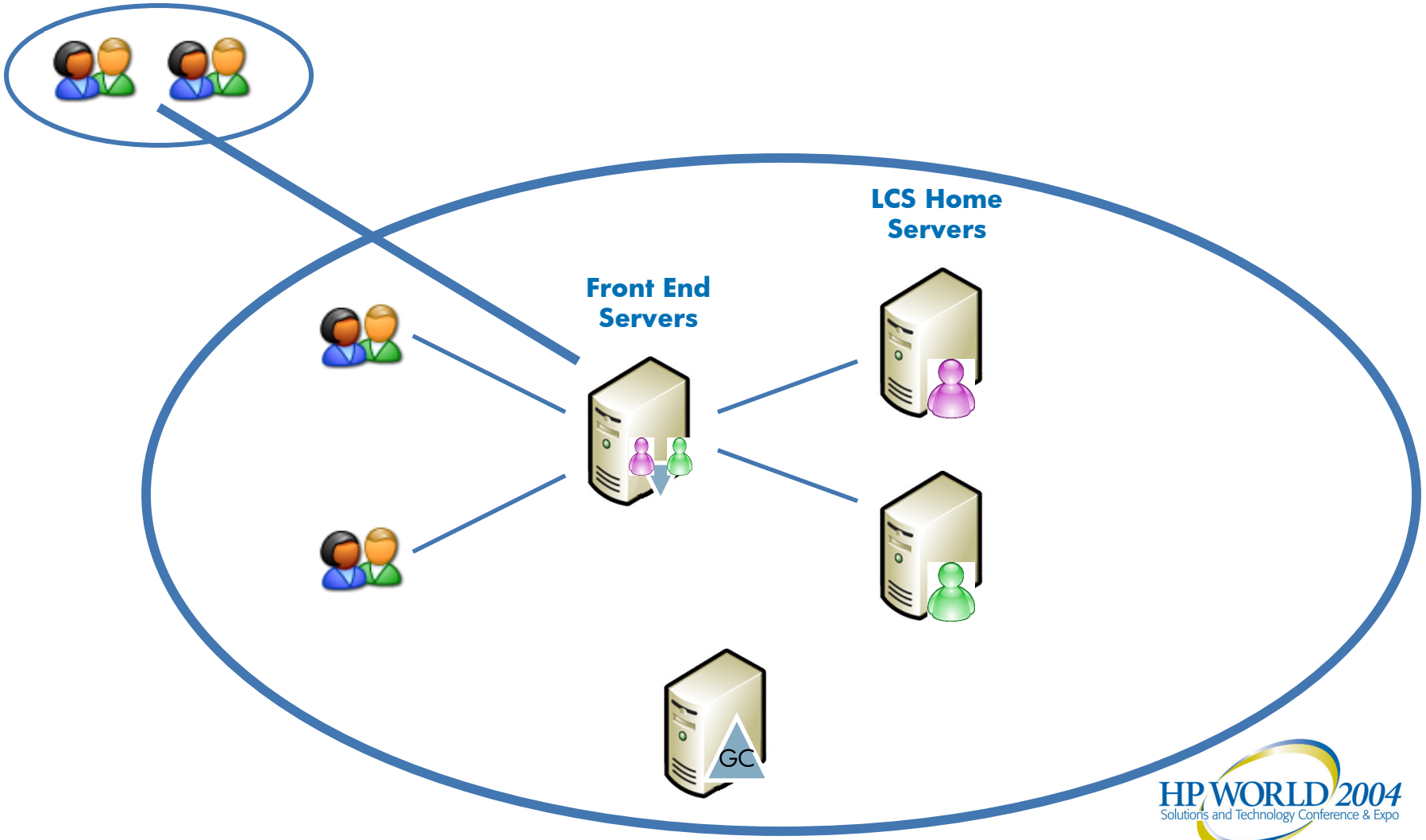
Deployment Topologies

- Home servers are connected peer-to-peer
  - There is not hub-and-spoke topology for routing at the backbone
    - Routing is only done from a client connection perspective
  - Hierarchy is enforced from a connectivity perspective using Forwarding Proxy or Front End Server servers
- For Remote Office deployments
  - For fewer than 100 clients consider a remote connection
- For multi site topologies
  - Clients should connect to localized Front End Servers
  - Consider configuration of multiple SIP SRV records
- For multi forest deployments
  - Ensure appropriate trusts between forest
    - Kerberos cross-forest trust on pure Windows 2003 domains
    - NTLM with Windows 2000/NT4 DCs
  - Synchronize use information using some form of dir synch tool

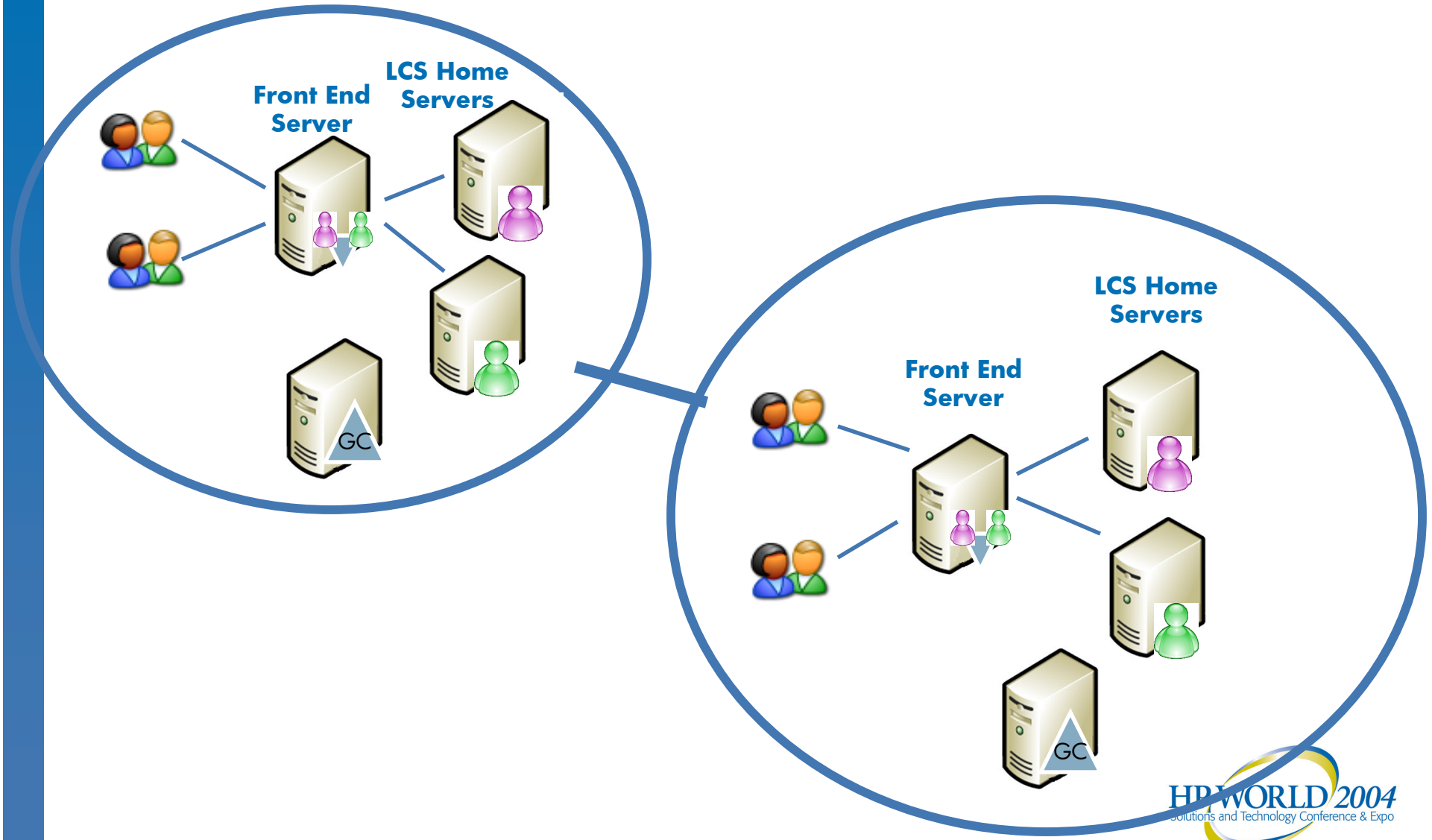
Single Site Topology



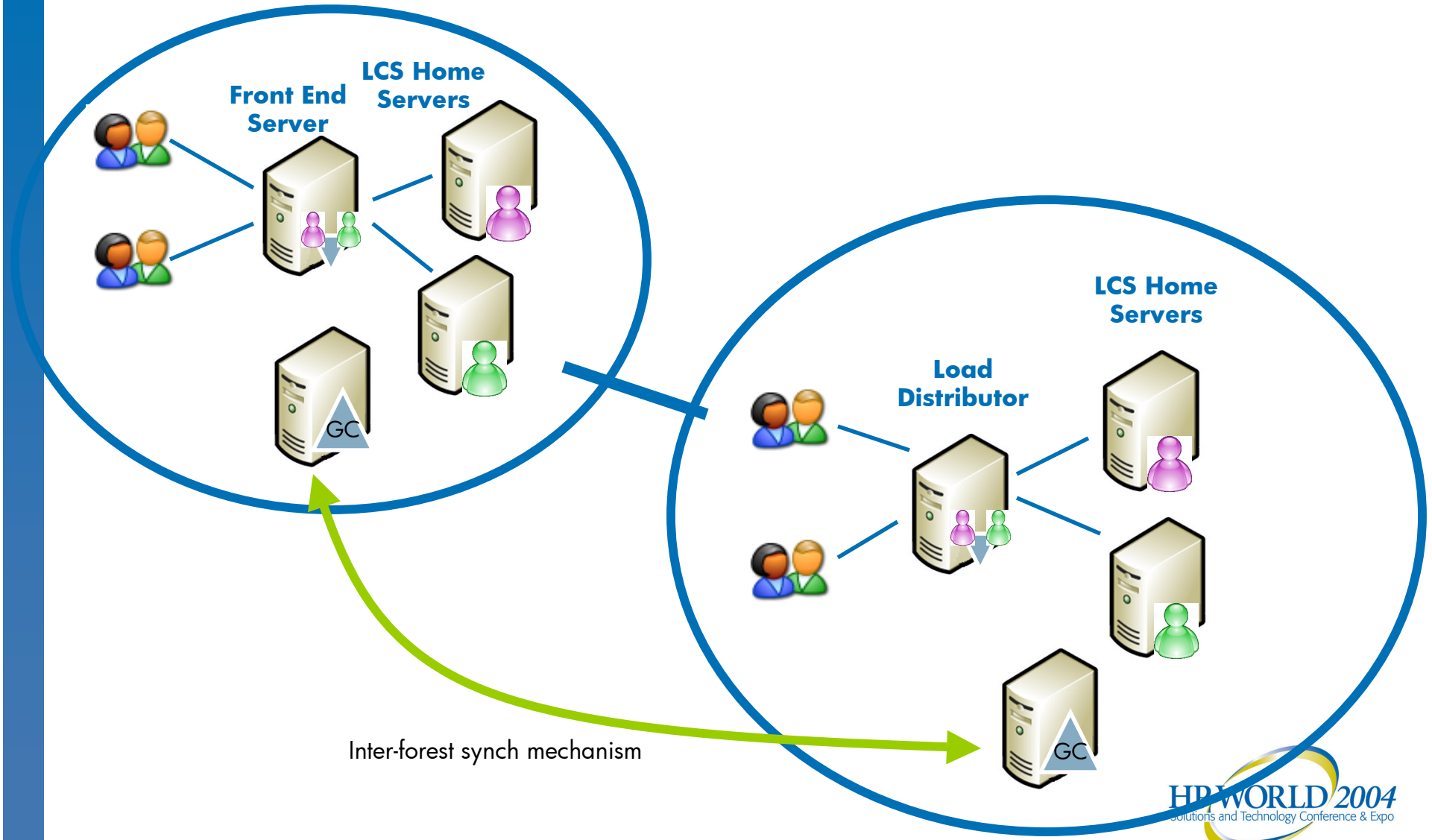
Remote Office Topology



Multi Site Topology



Multi Forest Topology



Message Logging

Message Logging Component

- Requires
  - Message Queuing Service (install from Control Panel)
  - SQL Server 2000 SP3 (or higher)
- Two component parts
  - IM Archiving Service
  - IM Archiving Agent
- Recommend installation of Archiving Service and SQL on a dedicated system
  - Agent is installed on potentially multiple servers
    - Consider installation on Front End Server or Forwarding Proxy servers
- Following information is logged per message
  - From, To, Time, Message (content)

Summary

Summary

- Support up to 10000 users per server
- All inter-server communication is over Mutual TLS
- Forwarding Proxy servers useful especially in hosted or firewall environments
- Front End Servers useful for normalized namespaces
- Multi Forest operation is straightforward but requires inter-forest trusts and a dir synch solution
- Implement Message Logging using a separate system with agents on critical IM systems

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP

RECOMMENDED TRAINING VENUE FOR THE

HP Certified Professional