

# OMNIMESSAGING

a multi media messaging solution

*OmniMessaging  
Functional Description  
Version 8.3*



# OmniMessaging Functional Description

<b>1</b>	<b>OMNIMESSAGING UMS SOLUTION OVERVIEW .....</b>	<b>6</b>
1.1	OMNIMMS .....	6
1.2	OMNIVOICE.....	7
1.3	OMNIVR .....	7
1.4	OMNIERS .....	7
1.5	OMNIMARKETING.....	8
1.6	ZLEMAIL ADAPTER.....	8
1.7	TARGET CUSTOMERS.....	9
<b>2</b>	<b>ADVANTAGES WITH THIS SOLUTION.....</b>	<b>9</b>
<b>3</b>	<b>BUILT WITH THE BEST TECHNOLOGY .....</b>	<b>9</b>
3.1	OPSOL OMNI MESSAGING SOFTWARE .....	9
3.2	HP OPEN CALL PLATFORM FOR VOICE COMPONENTS .....	10
3.3	HP NONSTOP SERVER FOR USER CONNECTION AND THE MESSAGE STORE.....	10
<b>4</b>	<b>TECHNOLOGY PROTECTION FOR THE FUTURE .....</b>	<b>10</b>
<b>5</b>	<b>OMNIMESSAGING MMS, EMAIL .....</b>	<b>11</b>
5.1.1	<i>Guaranteed Email server.....</i>	<i>11</i>
5.1.2	<i>Scalable Email server .....</i>	<i>12</i>
5.1.3	<i>Multi node growth.....</i>	<i>12</i>
5.1.4	<i>Open System with conformance to Standards .....</i>	<i>13</i>
5.1.5	<i>Production ready operational environment.....</i>	<i>13</i>
5.1.6	<i>SMSC .....</i>	<i>13</i>
5.1.7	<i>LDAP3 like directory.....</i>	<i>13</i>
5.1.8	<i>Web Portal Support.....</i>	<i>14</i>
<b>6</b>	<b>FUNCTIONAL OVERVIEW.....</b>	<b>14</b>
6.1	MAIN FUNCTIONS.....	14
6.2	PRODUCT FEATURES.....	15
6.2.1	<i>Mail Delivery.....</i>	<i>15</i>
6.2.2	<i>Configurable Limits .....</i>	<i>15</i>
6.2.3	<i>User Configuration .....</i>	<i>15</i>
6.2.4	<i>Mailbox Management.....</i>	<i>15</i>
6.2.5	<i>Security.....</i>	<i>16</i>
6.2.6	<i>Multi-Lingual Support .....</i>	<i>16</i>
6.2.7	<i>Interoperability.....</i>	<i>16</i>
<b>7</b>	<b>MOBILE OMNIMESSAGING FEATURES .....</b>	<b>17</b>
7.1	MMS - MULTI MEDIA MESSAGING SUPPORT.....	17
7.2	SMPP PROTOCOL SUPPORT.....	17
7.3	JAVA MOBILE CLIENT .....	17
7.4	BROWSER BASED CLIENTS.....	17
7.5	IMAP, POP, SMTP PROTOCOL SUPPORT.....	18
7.6	WAP SUPPORT .....	18
7.7	DEVICE TYPE RECOGNITION.....	18
7.8	CONFIGURABLE NOTIFICATION.....	18
7.9	ENTERPRISE MAILBOX.....	18
7.10	WORKGROUP MAILBOX.....	19
7.11	INFORMATION SUBSCRIPTION.....	19

# OmniMessaging Functional Description

7.12	MAILBOX SELF-MANAGEMENT .....	19
7.13	AUTO DOWNLOAD OR CONFIRMATION OPTION.....	19
7.14	BRANDING.....	19
7.15	NONSTOP RELIABILITY, SCALABILITY, AVAILABILITY.....	19
7.16	CARRIER GRADE PERFORMANCE.....	19
<b>8</b>	<b>MULTI-NODE ARCHITECTURE OVERVIEW.....</b>	<b>20</b>
8.1	OMNIMESSAGING MULTI NODE CHARACTERISTICS.....	20
<b>9</b>	<b>HP NONSTOP™ PLATFORM REQUIREMENTS .....</b>	<b>22</b>
9.1	SOFTWARE REQUIREMENTS.....	22
9.2	HARDWARE CONFIGURATION REQUIREMENTS .....	22
<b>10</b>	<b>OMNIMESSAGING COMPONENTS.....</b>	<b>23</b>
10.1	PROVISIONING SYSTEM – NAM, LISTENER, TRANSLATOR.....	24
10.1.1	Message Transfer Agent (MTA) .....	24
10.1.2	Message Store.....	25
10.1.3	Local Delivery Server (LDS) .....	25
10.1.4	Mailbox Maintenance Server (MBM) .....	25
10.1.5	Message Aging Server (MAS).....	26
10.1.6	Post Office Protocol version 3 (POP3) .....	26
10.1.7	Internet Message Access Protocol version 4 revision 1 (IMAP4) .....	26
10.1.8	ZLE Mail Adaptor.....	27
10.1.9	OmniMessaging Application Manager .....	27
10.1.10	Product Tracing Module .....	28
10.1.11	Queue Files .....	28
10.1.12	LDAP3 interface / Directory Server (optional) .....	29
10.1.13	Multi Node Directory Server.....	30
10.1.14	OpenSwitch.....	30
<b>11</b>	<b>OMNIMESSAGING FEATURES .....</b>	<b>32</b>
11.1	MAIL DELIVERY .....	32
11.1.1	Message Broadcasting.....	32
11.1.2	Mail User Redirection/Distribution Lists/Forwarding .....	32
11.1.3	Mail User Aliasing.....	32
11.1.4	Mail User Auto-Reply/Holiday Messaging .....	33
11.1.5	Configurable NDR Contents.....	33
11.1.6	Spam Checking.....	33
11.1.7	Pretension to Receive Spam .....	34
11.1.8	Relay Mail Blocking.....	34
11.1.9	Delivery Notification Interface.....	35
11.1.10	Virtual Domain Support .....	35
11.2	CONFIGURABLE LIMITS.....	36
11.2.1	Max Mailbox Size.....	36
11.2.2	Mailbox Size Threshold Warnings .....	36
11.2.3	Max Mailbox Messages .....	37
11.2.4	Max Message Retention Period.....	37
11.2.5	Max Local Message Size.....	38
11.2.6	Max Remote Message Size .....	38
11.2.7	Max Mailboxes Per User.....	38
11.2.8	Max Subscriptions Per User .....	38
11.3	USER CONFIGURATION.....	39
11.3.1	Service Package .....	39

# OmniMessaging Functional Description

11.3.2	Account Ownership .....	39
11.3.3	Mail Users .....	39
11.4	MAILBOX MANAGEMENT.....	40
11.4.1	Mailbox Sharing .....	40
11.4.2	Mailbox Maintenance By Administrator .....	40
11.4.3	Optional Message Aging.....	40
11.5	SECURITY.....	42
11.5.1	POP Before SMTP Authentication .....	42
11.5.2	Support for CRAM-MD5 Authentication Support .....	42
11.5.3	Configurable Max Login Attempts.....	42
11.5.4	Configurable Max Sessions Per User .....	42
11.5.5	Inactivity Timeout .....	42
11.5.6	Login Timeout.....	43
11.5.7	BCC Header Deletion.....	43
11.5.8	Quoted User Name in Local Language .....	43
11.5.9	Configurable Non-Delivery Report Messages.....	43
11.5.10	Optional IMAP Login Failure.....	44
11.5.11	Use of local HOST or DNS lookup for IP resolution.....	44
<b>12</b>	<b>APPENDIX - SYSTEM PARAMETERS .....</b>	<b>45</b>
<b>13</b>	<b>BILLING MODULE .....</b>	<b>48</b>
<b>14</b>	<b>VIRUS SCAN MODULE .....</b>	<b>49</b>
<b>15</b>	<b>PARENTAL CONTROL AND CONTENT ROUTER .....</b>	<b>50</b>
<b>16</b>	<b>ACH / EDI SUPPORT WITH DIGITAL SIGNATURES X.509 .....</b>	<b>51</b>
16.1	SECURE EMAIL IS DEFINED AS .....	51
16.2	SOME REQUIREMENTS FOR SECURE EMAIL.....	51
16.3	ENCRYPTED AND DIGITALLY SIGNED EMAILS.....	51
<b>17</b>	<b>DELIVER INVOICES, STATEMENTS VIA EMAIL .....</b>	<b>53</b>
<b>18</b>	<b>CONSOLIDATES USERS EMAIL ADDRESSES .....</b>	<b>54</b>
18.1	FEATURES .....	54
<b>19</b>	<b>VOICE MAIL SERVER .....</b>	<b>55</b>
19.1	RECORDING VOICE MESSAGES .....	55
19.2	RETRIEVING VOICE MESSAGES.....	55
19.3	DELETING VOICE MESSAGES.....	56
<b>20</b>	<b>OMNI IVR SOLUTION OVERVIEW .....</b>	<b>57</b>
<b>21</b>	<b>SOLUTION DETAILS .....</b>	<b>57</b>
21.1	PACKAGED IVR .....	57
21.2	PRE RECORDED PROMPTS .....	57
21.3	ADDING DYNAMIC CONTENT TO THE PROMPT .....	58
21.4	RETRY BUSY NUMBERS FOR OUTGOING CALLS .....	58
21.5	CONFIRMED DELIVERY .....	58
21.6	CALL REPORTING / AUDITING FACILITY .....	58
21.7	SCALING FOR VOLUMES .....	59
21.8	LOAD BALANCING.....	59

# OmniMessaging Functional Description

21.9	FAULT TOLERANCE.....	59
<b>22</b>	<b>HARDWARE AND SOFTWARE COMPONENTS.....</b>	<b>59</b>
22.1	OMNI IVR CALL PROCESSING MODULE.....	60
22.2	OMNI IVR CALL CONTROL MODULE.....	60
22.3	CALL FLOW PROGRAMMING .....	61
22.4	REPORTS AND STATISTICS FOR IVR SERVERS .....	61
	REPORTS ON TIME INTERVALS AND SERVER TYPES.....	61
	STATS TABLE STRUCTURE .....	62
	OPTIONS FOR REPORTS .....	63
	AGENT STATISTICS AND REPORTS.....	64
	AGENT STATISTICS FOR PARTICULAR AGENT.....	65
	EMAILING AND DOWNLOADING OPTIONS FOR REPORTS .....	66
<b>23</b>	<b>ADDITIONAL FEATURES TO INCREASE REVENUE .....</b>	<b>67</b>
23.1	DELIVERING CONFIRMATIONS , NOTIFICATIONS VIA VOICE MESSAGES, EMAIL, FAX.....	67
23.2	SUPPORTED TOUCH POINTS .....	68
23.3	SENDING OUTBOUND FAXES.....	68

## 1 OmniMessaging UMS Solution Overview

Opsol's OmniMessaging provides email, voice mail, short messages and Multi Media Messages for mobile operators, fixed line Telcos, ISPs and the enterprise. Banks use OmniMessaging to send emails from their Tandem applications.

OmniMessaging is a high-performance messaging solution for environments that support tens of millions of subscribers. It provides an infrastructure for applications that need sophisticated intelligent messaging.

### Key benefits:

**Ready for the future**—offers a fully integrated universal mailbox that manages multimedia objects such as e-mail, voice, pictures, video, chat, and more

**Ease of use and implementation**—supports all industry standard protocols, wireless devices, desktop systems, standard Web browsers, and e-mail clients

**Reduces costs**—eliminates the need to purchase, support, and maintain large server farms; one system supports a million subscribers and multiple systems can be managed as a single system image (SSI) to support even larger loads

**Scales with market demand**—allows each message transfer agent (MTA) to support in excess of 100,000 active messages and up to 250 active connections; limited only by the number of processors and available disk space

**Expandable**—offers add-on applications such as OmniMessaging Portal for calendar sharing, instant messaging, meeting planning, to-do list creation, and more; and OmniMessaging ZLEMAIL Adapter to automatically send e-mail messages based on predefined business rules

### 1.1 OmniMMS



In July 2002, OmniMessaging went live at KDDI, the largest Telco in Japan to support 15 million subscribers for MMS services. OmniMessaging was selected to replace a SUN, OpenWave solution.

Opsol's OmniMessaging provides streaming multi media to cell phones and mobile devices. OmniMessaging is a complete Universal Messaging solution with support for MMS, email, Voice messages and SMS alerts. The application generates CDRs for billing, SNMP events to HP OpenView for manageability and Java based user provisioning. The portal interface supports Web Mail, e – groups and calendaring. It is little wonder then that OmniMessaging has been selected at KDDI for 15 million users and has been in production since July 2002.

# OmniMessaging Functional Description

OmniMessaging leverages the scalable HP *NonStop*™ platform so that extra capacity can be added as required: disks, processors and communications controllers can be added online, Message Store size is limited only by the size of the disk farm. Thus allowing Service Providers to cope with growth while the subscriber base is still connected.

<http://www.omnimms.com>

## 1.2 OmniVoice



OmniMessaging Voice Mail server is for Carriers and Mobile Operators supporting millions of voice mail boxes. Voice messages can be accessed via standard phones, mobile phones, email and MMS clients. The solution is completely integrated with the carriers Network Protocols to provide Intelligent Messaging Services.

The GUI enables easy customization of prompt menus so it is easy to replace existing aging Voice Mail servers with newer technologies and yet eliminate user retraining.

<http://www.omnimessaging.com/omnivoice.htm>

## 1.3 OmniIVR

The OmniMessaging IVR solution provides a complete IVR solution, including CTI, to support a call center integrated with NonStop Financial applications.

<http://www.omniivr.com>

## 1.4 OmniERS



OmniERS provides mass alarm notification for a government organization to warn the population in case of major emergencies or incidents like huge fires, poisonous gas clouds or terrorist attacks.

The OmniMessaging Emergency Response System for mass alarm notification reaches millions of citizens within minutes via cell phone, fixed line, email, SMS and fax in the event of an emergency.

# OmniMessaging Functional Description

The target group can be a single street, a neighborhood or even a city. Organizations can broadcast alarms to all households in a radius of 5 miles from the disaster. The OmniERS database contains names, addresses, contact numbers as well as geographical information and location details.

<http://www.omniers.com>

## 1.5 OmniMarketing



The OmniMessaging Campaign Manager provides customer care via email and voice touch points. The mass mailing, millions of mails per month, is driven based on business rules and integration with web, order entry and billing applications. The solution records each user interaction in the campaign to target the correct message. Automated processes cleanse the database of invalid emails or telephone numbers.

<http://www.omnimessaging.com>

## 1.6 ZLEMail Adapter



The OmniMessaging Zero Latency Enterprise email adapter is to enable NonStop Business applications to send and receive emails of Banking Statements, invoices, PDF files etc. You can also learn how the OmniMessaging IVR solution provides a complete IVR solution, including CTI, to support a call center integrated with NonStop Financial applications. Eliminate expensive leased lines by securely transporting EDI and Secure documents encrypted using 3DES and digital certificates over the internet.

The **EMS2CELL** feature allows customers to deliver EMS messages to support staff's cell phones with voice and SMS alerts.

The **Omni Secure Transport** provides encrypted file transfer using digital certificates.

<http://www.zlemail.com>

Opsol solutions are developed specifically to take advantage of the proven reliability, scalability, and manageability of the HP NonStop platform, OmniMessaging provides



# *OmniMessaging Functional Description*

the highest levels of availability, the lowest total cost of ownership, and adherence to open standards to integrate new applications and media formats.

## **1.7 Target Customers**

Federal—Real-time command and control (ZLE)

Federal—Real-time homeland security (ZLE)

Network and service providers

Telco— Telco

## **2 Advantages with this solution**

- 1) Low total cost of ownership
- 2) Detailed call accounting
- 3) Integrated CTI Pop Up screens thus allowing call agents to follow current procedures
- 4) Seamless integration in the existing network
- 5) No matter what happens ... the customer calls will get through
  - a. Route messages via either Call Center
  - b. Hardware and software/application fault tolerance (no single point of failure)
  - c. Availability 99.999 % as required for a emergency application
- 6) Scalability ... Even a minimal configuration can handle hundreds of simultaneous calls. The implementation will scale easily to handle higher volumes
- 7) Reduce risk ... by working with experienced enterprise partners
  - a. Large Telcos and Financial institutions rely on HP NonStop Servers for high availability
  - b. HP's Open Call Platform is used for hundreds of thousands of ports
  - c. Opsol software is deployed for Enterprise integration in some of the largest banks, stock exchanges and cellular network providers

## **3 Built with the best technology**

### **3.1 Opsol OmniMessaging software**

- Provides tight integration between "The Telco" business applications and the IVR touch point
- Real time access and updates to the data warehouse on the Tandem
- Integrated with "The Telco" architecture and Stand-In processing
- Load balancing across multiple HP Open Call IVR servers
- Automatic routing updates to handle IVR scheduled maintenance and upgrade
- High Availability algorithm to handle Network or IVR failures
- Deployed for 15 million cellular customers messaging needs and has unmatched load balancing and fast performance for millions of calls
- Includes the OmniIVR Business Modules, Control Modules and all communication modules

### **3.2 HP Open Call platform for Voice components**

- Large number of ports supported in a single server
- Fewer servers to manage and hence costs less as it needs less operators
- Fewer servers and hence reduces server footprint, data center costs for air conditioning etc
- Complete IVR functionality
- Industry standard IVR cards for call handling and DTMF signaling
- Long term investment protection as additional features like Software DSP for Speech Recognition, VOIP etc can be added
- Deployed at some of the largest Telcos and Call Centers
- Hosts the OmniIVR Control Modules

### **3.3 HP NonStop server for user connection and the Message Store**

- Scalable, reliable, 99.999% uptime
- Currently provides Stand-In capability to all touch points including the IVR touch point
- Hosts the "The Telco" Operational Data Store
- Communicates in real time with other applications
- Deployed at some of the largest Telcos, Banks, Stock Exchanges and Card Switches
- Hosts the OmniIVR Business Modules

## **4 Technology protection for the future**

The solution is built on open technologies and additional modules can be purchased or added to add new functionality such as Voice XML, Speech Recognition etc

## **5 OmniMessaging MMS, Email**

Opsol's OmniMessaging provides an industrial-strength messaging solution suitable for electronic commerce and e-mail service providers, which demand scalability, reliability, and high-performance message backbones. OmniMessaging exploits the unique ability of HP NonStop™ systems to provide the most reliable email server in the world. OmniMessaging is reliable (99.999%), scalable and secure.

This document is a functional description of the OmniMessaging solution.

OmniMessaging provides the following general functions:

- SMTP messaging over a TCP/IP network
- POP3, IMAP4 Protocol support
- SMPP3.4 support for SMS, OTA for cellular services
- Store-and-forward for Internet or local intranet messaging services

### **5.1.1 Guaranteed Email server**

OmniMessaging is the world most reliable email messaging server. It provides reliability in the following ways:

- Built on a NonStop™ fault-tolerant platform thus providing high system availability.
- Uses NonStop™ Transaction Manager/MP (TM/MP) to safeguard data integrity.
- Uses NonStop™ Transaction Services/MP (TS/MP) to provide process persistence.
- Provides automatic retries of delivery when recoverable failures occur. After the maximum number of retries are attempted, OmniMessaging generates NDR's (Non-Delivery Reports).

Once OmniMessaging accepts responsibility for a message, it ensures that the message is not lost. OmniMessaging safely stores all incoming messages on disk and then acknowledges the message. Once OmniMessaging accepts responsibility for the message it is never lost. OmniMessaging will deliver the message to its local users or forward the message to a remote MTA for remote users. If the remote MTA is unavailable, OmniMessaging will continue to retry delivery for a configurable period. In the event that the message still cannot be delivered then OmniMessaging will return a Non Delivery Report to the

# *OmniMessaging Functional Description*

originator. If delivery of the NDR fails then the message is forwarded to an administrative mailbox and sends an alarm to the system console.

## 5.1.2 Scalable Email server

OmniMessaging provides scalability in the following ways:

- OmniMessaging components and processes can run in different processors on the same physical node. In addition you can cluster multiple nodes in a Multi node cluster to grow to a maximum of 4096 processors.
- OmniMessaging runs on a NonStop™ System, where one can easily add disks, communication controllers, and processors as needed. One can easily configure OmniMessaging components for additional traffic by using OmniMessaging management applications and other standard tools. All of this can be done online with no outage or impact to the application. A small two cpu starter system for 100,000 subscribers can grow to a large 4080 cpu system for millions of subscribers with zero application outage.

## 5.1.3 Multi node growth

OmniMessaging in a multi node NonStop™ environment is designed to:

- Provide 24\*7 service availability during planned and unplanned node outages (constant application availability).
- Provide scalability – that is to handle subscriber growth with more accounts and data flow beyond the limits of a single node system, typically 1 million subscribers.
- To maintain a level of service even during hardware failures e.g. failures on Network Transport, Database, CPU or even a complete node.
- To provide the capability to upgrade a single node (SYSGEN) with no loss of service to the subscribers.
- To maintain service during an OmniMessaging upgrade into new MS format.
- To migrate users successfully from one node to another for load balancing across the entire system.

The above list highlights that the network external to the NonStop™ Himalayas must not be Node dependent in that, in the event of a Node being unavailable then another Node must be accessible via the IP network.

# *OmniMessaging Functional Description*

## 5.1.4 Open System with conformance to Standards

OmniMessaging uses and complies with Requests For Comments (RFCs), which are Internet standards used by the Internet community that apply to SMTP, MIME, TCP/IP, and DNS, among others.

## 5.1.5 Production ready operational environment

OmniMessaging provides the following features that are essential to a commercial environment:

- Detailed accounting and operational events.
- Support for large data-stream transfers; for example, bulk Electronic Data Interchange (EDI) transactions and multimedia data.
- SNMP Alarms and alerts to SNMP managers.
- Performance instrumentation to feed performance monitors in real time.
- X.400 support for application integration
- ZLE adaptors to integrate application on the NonStop™ platform. OmniMessaging provides adaptors and interfaces for external applications to generate mail, provision users, billing etc.

## 5.1.6 SMSC

- Fully functional SMSC package (add on)
- Notifications to Cell Phones, IPAQ
- WAP support

## 5.1.7 LDAP3 like directory

IMAP, POP, SMTP servers running on multiple physical nodes query the directory server for user information. The directory server accesses its User Database and obtains information such as home location, user profile and subscription attributes.

NSK-LDAP V2.0 is the OPENLDAP V2.0.12 port to the OSS environment. This software enables multiple LDAP servers on a system. Each cpu can have a LDAP server for load balancing and for fault tolerance.

NSK-LDAP V2.0 is complete. It includes all of the libraries and tools need to use the LDAP server or to do programing. The LDAP software uses the Berkely DB 1.85 for its database access and includes encryption (SSL/TLS) based on NSK-SSL. LDAP V2.0 support LDAP protocols V2.0 and V3.0 and user defined schema's.

NSK-LDAP V2.0 scales using the Parallel TCPIP product. With Parallel TCPIP, you can have as many instances of the LDAP server as required. NSK-LDAP V2.0 also works with standard TCPIP.

# *OmniMessaging Functional Description*

SQL back-end, SASL, and replication support will be included in the next update. If you require SSL, you will need NSK-SSL for private key, certificate request and key generation.

Features:

Single threaded versions of the LDAP server.

Test Suite included for install validation of LDAP server.

LDIF tools - data conversion tools for use with slapd

LDAP gateways - finger, gopher, email to LDAP gateways

LDAP tools - A collection of command line LDAP utility programs

## 5.1.8 Web Portal Support

- Browser client
- Contacts
- Branding

# 6 Functional Overview

## 6.1 Main Functions

The OmniMessaging product provides the following specific functions:

- A Message Transfer Agent (MTA) to route messages over the Internet using SMTP. For information about the OmniMessaging MTA, see section 10.1.1 Message Transfer Agent (MTA).
- A Post Office Protocol Version 3 (POP3) server, which allows remote mail clients to download mail from their NonStop™ Kernel mailboxes. For information about the OmniMessaging POP3 server, see section 10.1.6 Post Office Protocol version 3 (POP3).
- An Internet Message Access Protocol Version 4 (IMAP4) server, which allows remote mail clients to access and manage mail in their NonStop™ Kernel mailboxes. For information about the OmniMessaging IMAP4 server, see 10.1.7 Internet Message Access Protocol version 4 revision 1 (IMAP4).
- Wireless protocols to support efficient cellular messaging with SMSC gateways.
- ZLE Mail Adaptor for NonStop™ based applications and applications on other platforms
- Host-based mailboxes for storing a variety of messages (fax, text e-mail, documents, video clips, and so on).

# *OmniMessaging Functional Description*

- Facilities for configuration, management, accounting and statistical information.

## **6.2 Product Features**

Some of the product features are documented in this section

### **6.2.1 Mail Delivery**

- Message Broadcasting
- Mail User Redirection (to local or remote mail addresses)
- Mail User Forwarding (to local or remote mail addresses)
- Mail User Aliasing (to local or remote mail addresses)
- Mail User Auto-Reply/Holiday Messaging
- Content of NDR Configurable (Include Message/Include Header/Do Not Include Message)
- Spam Checking – Blacklisting at IP, Domain and From Address Levels
- Relay Mail Blocking (Subnet and White list checking for Relay Authorization)
- Delivery Notification Interface
- Virtual Domain Support

### **6.2.2 Configurable Limits**

- Mailbox Size
- Mailbox Size Threshold Warnings
- Max Message Retention Period
- Max Local Message Size
- Max Remote Message Size

### **6.2.3 User Configuration**

- Service Package Definition
- Account Ownership
- Mail Users

### **6.2.4 Mailbox Management**

- Mailbox Sharing
- Mailbox Maintenance By Administrator
- Optional Message Ageing

# *OmniMessaging Functional Description*

## 6.2.5 Security

- POP Before SMTP Authentication
- CRAM-MD5 Authentication
- Configurable Max Login Attempts
- Configurable Max Sessions Per User
- Configurable Inactivity Timeout
- Configurable Login Timeout
- Encrypted passwords on the network
- Access Control Lists on data files
- BCC Header Deletion

## 6.2.6 Multi-Lingual Support

- Quoted User Name Support
- Configurable Non-Delivery Report Messages

## 6.2.7 Interoperability

- Optional IMAP Login Failure Tagged Response
- Use of local HOST or DNS lookup for IP resolution



## **7 Mobile OmniMessaging Features**

(To purchase this additional module please contact your HP Sales Representative)

### **7.1 MMS - Multi Media Messaging support**

The OmniMessaging solution includes a Multi Media Messaging server to provide text and graphics to a cell phone. Opsol provides the MMS server over two protocols. We use the Mobile IMAP protocol for speed, small cell phone footprint and conformance to standard protocols. Or the customer can choose the WAP protocol if they have a significant WAP investment.

In both cases the user has a universal mailbox and can access it via cellular phones, email clients etc.

### **7.2 SMPP Protocol support**

The SMS Adaptor is based on the SMPP 3.4 specification and supports any SMPP3.4 compliant SMS center. The gateway is integrated with OmniMessaging and delivers a notification for new mail via the SMS protocol. The notification contains the URL to download the complete message, attachment or graphic to the users PDA. This feature is useful in confirming a download for pricing reasons etc.

Short Message Service (SMS) is the ability to send and receive text messages to and from mobile phones. The text can comprise of words, numbers, or an alphanumeric combination. Each short message can be up to 160 characters in length. Newer standards are emerging that support larger message sizes. Often SMS Mobile Terminate Services are offered along with voice mail notifications, which account for the vast majority of SMS traffic on the network.

### **7.3 Java Mobile Client**

The Mobile OmniMessaging client has a small footprint and is optimized for the Mobile IMAP protocol. The client is written in Java and can be easily deployed across different cellular phone models, PDAs etc.

### **7.4 Browser Based clients**

Mobile OmniMessaging supports standard browser (e.g. Microsoft Explorer) based clients using the WAP protocol. The users access the OmniMessaging server using the link <http://www.zlemail.com>. This allows users to read, create emails in their regular inbox. The WAP Gateway and protocols are provided by the Cellular Network Provider.

# *OmniMessaging Functional Description*

## **7.5 IMAP, POP, SMTP Protocol support**

Users can access the OmniMessaging server using standard email clients (e.g. Microsoft Outlook Express, Netscape). The user configures zlemail.com as their SMTP server, IMAP server or POP server. Requests come in to the OmniMessaging server as standard TCPIP requests. The wireless access is provided by the Cellular Network Provider.

## **7.6 WAP Support**

OmniMessaging users can provision themselves and also alter their settings using the WAP interface. Thus a user can register/de-register himself from a service using the WAP interface. In addition, once registered the user can change his personal settings using the WAP interface. These include functionalities like - change password, adding an alias, setting forwarding or autoreply features, altering his personal autoreply messages etc.

## **7.7 Device type recognition**

OmniMessaging users can configure the device type associated with an email address. As a result OmniMessaging is able to intelligently route messages to the devices using the appropriate protocols. E.g. we would use the SMPP protocol to deliver a message to a Cellular Phone, or an SMS notification to an IPAQ. The graphic images can be reformatted based on the device display type. Hence JPG images are delivered to phones that support JPG and GIF images are delivered to phones that support GIF images.

## **7.8 Configurable Notification**

Users can send Notification ("New Mail") messages to Cellular Phones, IPAQ PDA, Palm PDAs, wireless Laptops, Pager Devices etc. Notification is enabled and configured by the user. Configuration options include the subject length of the message, content size, delivery mechanism etc. All of these attributes are stored in the User Profile.

## **7.9 Enterprise Mailbox**

ISPs can offer group mailboxes to corporate customers on a group-sharing basis. Enterprise mailbox service is for middle/small enterprise, this kind of company has the need of exchanging information on internet, but the common free internet mailbox can not meet their requirement of high speed, security, stable and independence, and installation of own mail server will cost too much and pay more O&M cost, so they need service provider to provide mailbox rental service.

Corporate customers can use this feature to have their own group of mailboxes, with specific configurable properties and their own administrators. These customers can also have their own branding and customized Webmail.

# *OmniMessaging Functional Description*

## **7.10 Workgroup Mailbox**

ISPs can offer workgroup mailboxes to corporate and individual customers on a group-sharing basis.

A workgroup mailbox is similar to the concept of E-groups or knowledge sharing groups. Hence a member can subscribe to these groups, and exchange mails with members of the workgroup.

## **7.11 Information Subscription**

Users can subscribe to Subscriptions or information based on their requirements. Notification is enabled and configured by the user, and they can configure to receive it in suitable devices. All of these attributes are stored in the User Profile.

## **7.12 Mailbox Self-Management**

Users can configure their own set of rules for mailbox management. Thus a user can decide whether to have old messages deleted based on date, or messages deleted on read/unread status or any other rule. Thus the user can ensure that if the mailbox-quota is exceeded the mail-delivery does not get affected.

## **7.13 Auto download or confirmation option**

OmniMessaging supports auto download of the emails to cellular devices so that the event of receiving an email is automatic. On the other hand if the Service Provider would like to charge based on data transfer then only the header is displayed and the user confirms each download.

## **7.14 Branding**

The OmniMessaging Web Mail client can be branded by the customer. We provide the source code to our Web Client.

## **7.15 NonStop Reliability, Scalability, Availability**

OmniMessaging is built to run on HP NonStop™ servers. NonStop™ servers are used to run Financial networks, Stock Exchanges, Banks and now OmniMessaging brings the same reliability, scalability and availability to Wireless email and messaging.

## **7.16 Carrier Grade Performance**

OmniMessaging has optimized protocols and databases to support fast and guaranteed message delivery to Mobile Devices.

## **8 Multi-Node Architecture Overview**

In a multi-node OmniMessaging system; the message store is partitioned into several HP NonStop™ nodes. The pop/imap/smtp request from outside can come to a server at any node. The recipient server will make sure that the message retrieval/storage occurs in the message store on the primary node that is assigned to the user/submission-address transparent to the client, whenever the primary node is up.

For high availability, each user/submission-address is assigned one primary node and two or more backup-nodes. If the primary node is down, the client should be able to use the OmniMessaging system. New messages can be sent or stored. The older messages will be inaccessible. Once the primary node is up all (new and old) messages will be accessible.

A particular node can be brought down by the operator; this is termed as scheduled outage. A node could go down due other reasons; this is termed as unscheduled outage. Once a node is down the action taken by the OmniMessaging system remains same as that in the case of scheduled outage.

### **8.1 OmniMessaging Multi Node characteristics**

1. OmniMessaging Node: NonStop™ node with OmniMessaging software.
2. OmniMessaging users are distributed across the nodes.
3. Multiple OmniMessaging Pathmons can be started on a single OmniMessaging node.
4. The OmniMessaging Message Store is shared by all the OmniMessaging Pathmons.
5. The OmniMessaging application components are exact replicas on each node.
6. Some data is replicated across the OmniMessaging instances. This information is used to route the user to his home node.

## *OmniMessaging Functional Description*

7. The permanent storage for a user is always on his home node. Intermediate storage for new mails is provided on backup nodes. After maintenance of the users primary node is complete, the users mails will be transferred to the original home node. This action is scheduled by the operator.

## **9 HP NonStop™ Platform Requirements**

### **9.1 Software Requirements**

The OmniMessaging product runs on the NonStop™ platform (K1000 plus) with the NonStop™ Kernel operating system version D47 or G06 and above. You must be connected to a TCP/IP network (Internet or local intranet) with access to a DNS server.

NonStop™ Kernel Operating System G06.14 Currently certified

T9551 TCP/IP

T9631 EMS collector

T9632 EMS distributor

T9153 NonStop™ TS/MP

T9066 NonStop™ TM/MP (TMF)

T9193 NonStop™ SQL (only the run-time license)

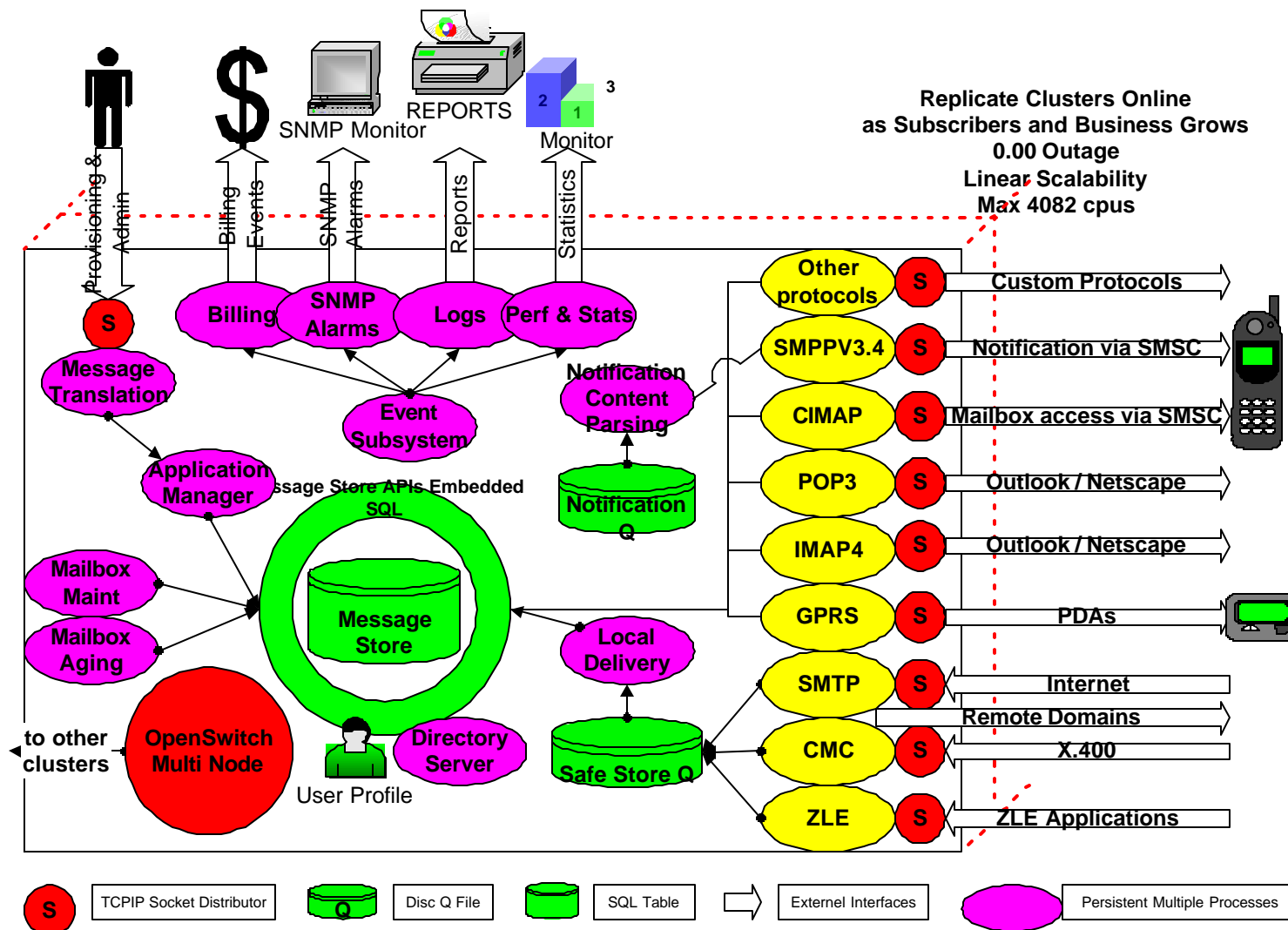
Please refer to the NonStop™ manuals for installation and configuration information.

### **9.2 Hardware Configuration Requirements**

(see attached HP NonStop™ Performance Report for system sizing)

## 10 OmniMessaging Components

## OmniMessaging(tm) Architecture on Compaq NonStop(tm) Himalaya servers



## **10.1 Provisioning System – NAM, Listener, Translator**

Users are provisioned on the system using the provisioning server. The following method can be three interfaces

- Java Provisioning client – PC based. The Java Administrator Client allows an Administrator to manage the entire configuration of the OmniMessaging application. It is portable and can execute on any system that supports Java. It is used to add domains, users, blacklists etc. For details refer to the OmniMessaging Java Provisioning Client Manual.
- Provisioning batch load – Server based. This method is ideal to migrate a large number of users in a short time. 10,000 users can be provisioned per hour. We export the user information from the existing email server and transform the data to the OmniMessaging format. This batch load is then provided to the Provisioning Server. Following that the emails are migrated from the old system to the OmniMessaging system. With this approach we can migrate 100,000 users within a weekend. This method is used by our Professional Services Team.
- Custom built provisioning using Message Store API interface. This method is used by accounts that have special provisioning needs. This method is not normally used as all features are provided via the Provisioning system.

In a Multi Node environment the Provisioning server will populate the address book and make corresponding entries on all nodes to support a large multi node cluster.

### **10.1.1 Message Transfer Agent (MTA)**

The OmniMessaging MTA consists of receiving MTA, sending MTA and distributor NonStop™ TS/MP server classes. NonStop™ TS/MP software provides management of the NonStop™ TS/MP processes by means of the PATHMON process. There can be multiple MTA and distributor processes.

The distributor process allows for monitoring of multiple local IP addresses.

Each MTA process instance implements SMTP functionality and interacts with ZLEMAIL ADAPTER gateway applications.

When a receiving MTA process is started, the MTA process registers itself with the distributor process. When the distributor process receives a message from TCP/IP, it uses an internal scheme to distribute requests to an MTA process registered with the distributor process.



# *OmniMessaging Functional Description*

When a receiving MTA process receives a message that needs to be sent to a remote domain it passes this message to a sending MTA process to be relayed on.

Since neither the distributor nor the receiving MTA use **Pathsend** for dynamic load balancing, you must add additional receiving and sending MTA processes (using the OmniMessaging Application Manager) to increase the number of MTA server-class processes for increasing loads.

## 10.1.2 Message Store

A Local Delivery Server (LDS) enters the messages into the MS and the MBM and MAS processes maintain the messages.

You configure the LDS and MBM and MAS as NonStop™ TS/MP processes running under the control of a PATHMON process.

## 10.1.3 Local Delivery Server (LDS)

The LDS is configured as a static NonStop™ TS/MP process. It may have multiple server classes, and each server class may have multiple processes. If needed, the operator may configure multiple LDS NonStop™ TS/MP server classes and start and stop the classes based on local-message load.

The process's tasks are the following:

- get local messages from the OmniMessaging MTA
- store messages in the MS
- explode redirection lists
- enforce quotas
- generate non delivery reports and vacation messages

The LDS process does not analyse or decode message content.

If all recipients are invalid, the message is rejected, and a non-delivery report is sent to the originator via the MTA. If the message contains both valid and invalid recipients, the LDS generates non-delivery reports for the invalid recipients (one report for each message). OmniMessaging allows the configuration of whether the whole message, the headers or no message content is returned in a non-delivery report.

## 10.1.4 Mailbox Maintenance Server (MBM)

The MBM performs deferred cleanup activities for ensuring that all MS operations complete successfully, and that the database remains in a logically consistent state.

Each MBM process is a static NonStop™ TS/MP process that runs as a background task. It deletes messages, mailbox folders, namespaces, submission addresses, domains, user entries and accounts from the MS as requested by the Provisioning, MAS, POP3, IMAP4, LDS and MTA Servers. MBM functions are determined by queue entries.

# *OmniMessaging Functional Description*

If the delete operation fails, the MBM retries the failed operation as specified in the Max retry count entry. If retries are exhausted, the record is written to the MBM backup queue.

The MBM will reschedule a message delete until all sessions that have the mailbox selected are aware that the message has been expunged. The MBM will reschedule a mailbox delete until there are no sessions that have the mailbox selected.

The MBM process also cleans up orphaned sessions that result from unexpected OmniMessaging process terminations.

## 10.1.5 Message Aging Server (MAS)

The MAS deletes messages older than a period specified for each mailbox. A system wide default maximum age can also be specified.

Each MAS process is a static NonStop™ TS/MP process that runs as a background task. Each MAS server class accepts key range parameters so that a number of them can run in parallel across particular physical partitions.

## 10.1.6 Post Office Protocol version 3 (POP3)

OmniMessaging provides host-based mailboxes for OmniMessaging users. OmniMessaging supports the standard POP3 protocol to allow users to access their mailboxes remotely from desktop mail clients. Users can establish connections to their mailboxes, count the messages in their inboxes, retrieve messages to local storage, and delete messages from host-based mailboxes.

OmniMessaging POP3 includes POP3 server and distributor processes.

You configure the POP3 server and distributor as NonStop™ TS/MP processes running under control of a PATHMON process.

POP3 is an **Internet Protocol (IP)** for remote mailbox access; its specifications are documented in RFC 1939 (for more information, see [RFC 1939—Post Office Protocol—Version 3](#)).

Initially, the server host starts the POP3 service by monitoring TCP port 110. When a client host establishes a TCP connection with the server host, the POP3 server sends a greeting. The client and POP3 server then exchange commands and responses until the connection is closed or aborted.

## 10.1.7 Internet Message Access Protocol version 4 revision 1 (IMAP4)

OmniMessaging provides host-based mailboxes for OmniMessaging users. OmniMessaging supports the standard IMAP4 protocol to allow users to access their mailboxes remotely from desktop mail clients. IMAP4 varies from POP3 in providing management functions for the mail to remain centrally stored in OmniMessaging.

OmniMessaging IMAP4 includes IMAP4 server and distributor processes.

You configure the IMAP4 server and distributor as NonStop™ TS/MP processes running under control of a PATHMON process.

# OmniMessaging Functional Description

IMAP4 is an **Internet Protocol (IP)** for remote mailbox access; its specifications are documented in RFC 2060 (for more information, see [RFC 2060—Internet Message Access Protocol - version 4rev1](#)).

Initially, the server host starts the IMAP4 service by monitoring TCP port 143. When a client host establishes a TCP connection with the server host, the IMAP4 server sends a greeting. The client and IMAP4 server then exchange commands and responses until the connection is closed or aborted.

## 10.1.8 ZLE Mail Adaptor

A ZLE Adaptor is provided to email enable applications. Applications can send email messages to internet users via the ZLE Adaptor. The Adaptor can be invoked by applications on the platform as well as applications off the platform. The adaptor supports a simple input buffer. Applications on the NonStop™ platform can invoke the ZLE Adaptor via a simple server class send. Applications from an NT or UNIX platform can invoke the adaptor using a socket interface.

## 10.1.9 OmniMessaging Application Manager

The OmniMessaging Application Manager receives requests from users, currently via the Java Administrator client, to monitor various performance indicators of OmniMessaging resources and to query the system configuration.

This interface is also used to start and stop traces for troubleshooting and to turn accounting events on or off.

The Application Manager has the capability to display statistical information relating to the live OmniMessaging environment. During the lifetime of each server process, statistical information is accumulated within the server's memory as each new message is processed. The information gathered varies depending on each server class – the following is a summary of statistical information provided by the main servers:

POP and IMAP servers:

- # of openers
- # of current sessions
- # of connections accepted
- # of connections rejected
- Shortest connect time
- Longest connect time
- # of invalid commands
- # of messages sent
- # of messages deleted
- Size of largest message
- Size of smallest message

# *OmniMessaging Functional Description*

Message Transfer Agent servers (MTA):

- # of current incoming sessions
- # of current outgoing sessions
- Send Q length
- # of incoming sessions
- # of messages received
- # of receive recipients
- # of outgoing sessions
- # of messages sent
- # of send recipients

Local Delivery Server (LDS):

- # of messages stored
- # of messages rejected
- # of messages w/NDRs
- # of messages recipients
- # of messages invalid recipient
- # of messages exploded recipients
- # of messages sent
- # of messages Quota violations
- Largest MSG (bytes)
- Max local recipients/MSG

## 10.1.10 Product Tracing Module

OmniMessaging provides tracing for troubleshooting. You can configure the trace option to turn on or off selected functional-component trace logs. This requires special attributes and call Opsol for details.

## 10.1.11 Queue Files

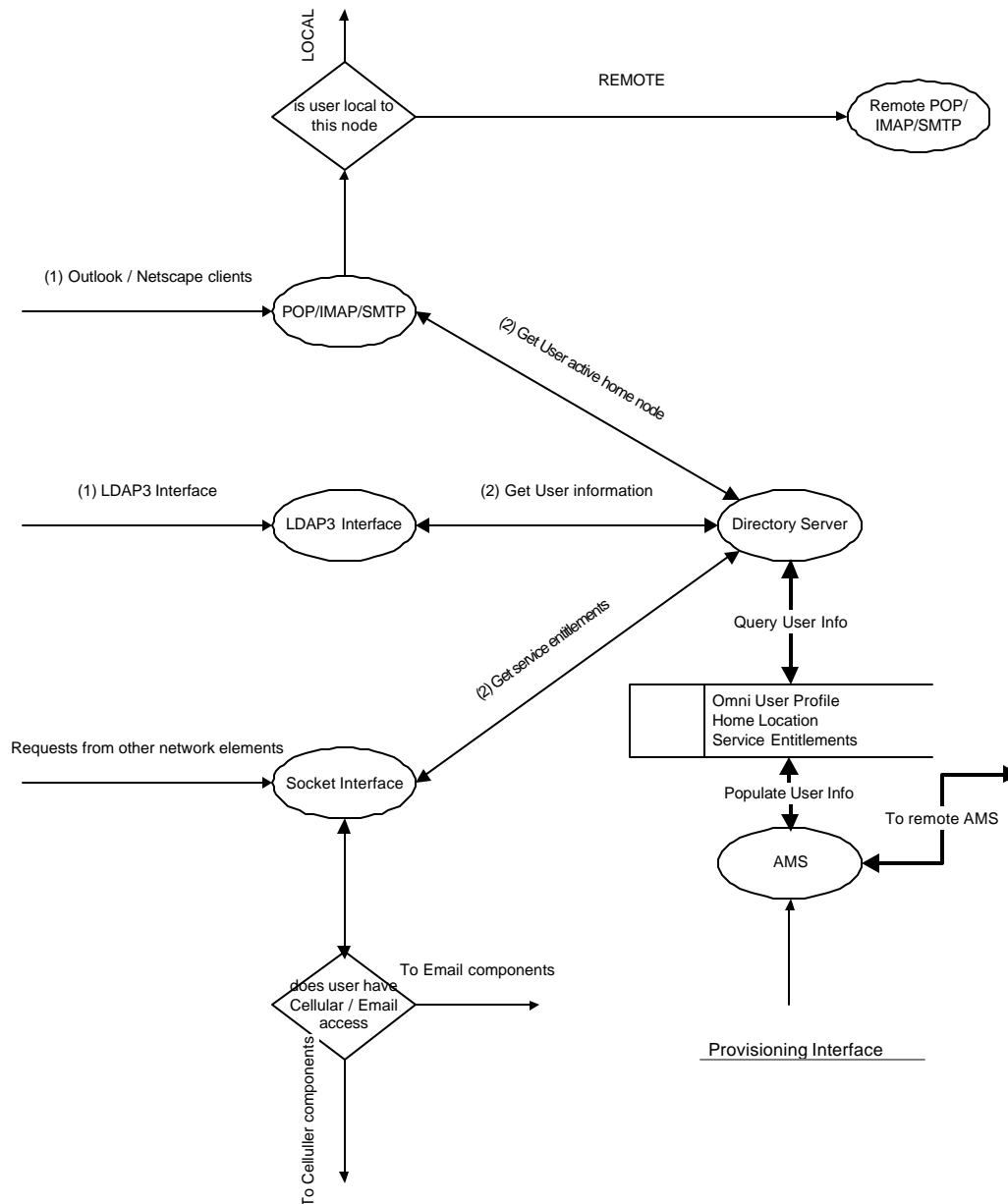
OmniMessaging makes extensive use of standard HP NonStop Queue files. The use of queue files enables greater load balancing between server processes. For example the MTA process creates a queue file entry to trigger the local delivery of messages by the LDS process. OmniMessaging has the flexibility to be configured to have many server processes de-queueing records from a single queue file.

## OmniMessaging Functional Description

### 10.1.12 LDAP3 interface / Directory Server (optional)

The Directory Server provides user information for local OmniMessaging components via the Server class send APIs. Applications on other platforms desiring access to the OmniMessaging User profile can use a socket interface or an LDAP3 interface. The Directory Server runs as a NonStop™ TSMP Server class for persistence and scalability.

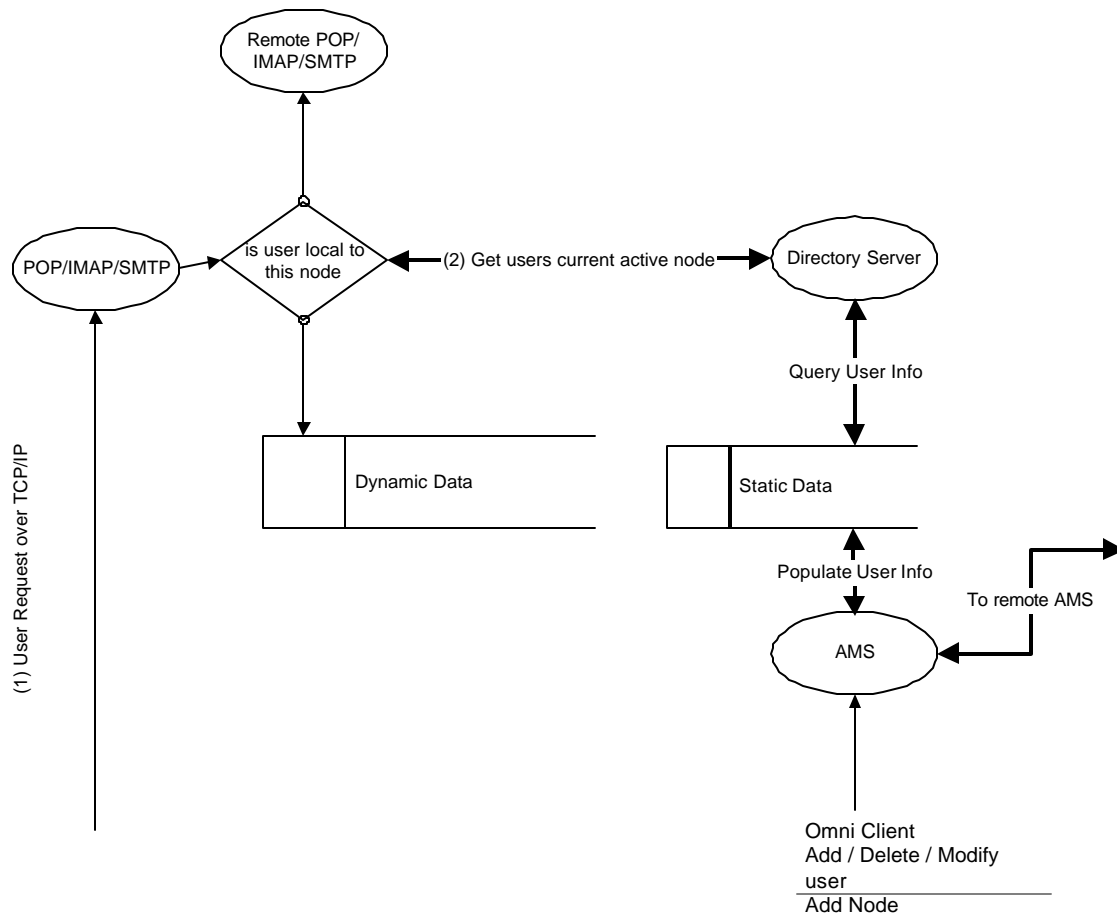
The figure below describes the flow for the directory server.



# OmniMessaging Functional Description

## 10.1.13 Multi Node Directory Server

The Directory server runs as a TSMP server class. The input is an email address (submission address) or User Name and the output is the users home node and backup node instances. A Programmatic Interface is provided for custom applications attempting to use the Directory Server.



## 10.1.14 OpenSwitch

OpenSwitch monitors the nodes in the OmniMessaging multi node environment. The OpenSwitch considers a node down if it loses all its connections to the OpenSwitch on the other node. OpenSwitch uses Expand and \$receive for all its communications.

The POP, IMAP, SMTP servers register with the OpenSwitch on the local node. The POP, IMAP, SMTP servers wishing to communicate with a remote node will query the OpenSwitch for their counterparts process names on the other nodes. The OpenSwitch will return the home nodes process name if the home node is

## *OmniMessaging Functional Description*

up or the backup nodes process name if the home node is down. We currently support 2 backup nodes.

A Programmatic Interface is provided for custom applications that need to use the OpenSwitch.

## **11 OMNIMESSAGING FEATURES**

### **11.1 Mail Delivery**

#### **11.1.1 Message Broadcasting**

Message Broadcast is a mechanism that will allow a message to be delivered to ALL recipients at a given domain. An administrator sending a message to a special submission address triggers the process. OmniMessaging automatically expands the recipient list to include all users in the domain. Built in checks prevent this procedure from being abused by hackers.

#### **11.1.2 Mail User Redirection/Distribution Lists/Forwarding**

OmniMessaging can be configured to redirect mail directed to one particular address to one or more other addresses. OmniMessaging handles Distribution lists as a type of redirection.

The following facilities are provided: -

- Option to save or discard the redirected message in the target mailbox for the original recipient (normally discarded for distribution lists)
- Configuration of multiple remote or local redirection addresses (or distribution list addresses)
- Loop detection (prevents mails being forever redirected)
- Configurable Reverse Path Address – On generation of redirected messages for a message sent to a redirected/distribution list address, the recipient for any NDRs can be configured to be:-
  - the original sender of the message
  - the current path, either redirected/distribution or original recipient
  - a nominated address (External Maintainer)
  - NULL, to indicate that the no NDR should be sent.

For distribution lists, NDRs will normally not be sent or will be sent to a nominated address, e.g. the distribution list administrator. For normal redirection, including aliases, any NDRs are normally configured to be sent to the original sender of the message.

#### **11.1.3 Mail User Aliasing**

This is another type of redirection. Normally with aliases the mail is redirected to a single address and the mail is not saved at the original targeted mail address. The Reverse Path Type would normally be set to the original sender of the message.



# *OmniMessaging Functional Description*

## 11.1.4 Mail User Auto-Reply/Holiday Messaging

OmniMessaging can be configured to send auto-reply messages sent to a particular mail address. The following facilities are provided: -

- Configurable date/time period for auto-reply activation for a mail address
- Configurable subject line and mail text for auto-reply mail for a mail address
- Option to keep the original message in the auto-reply mail for a mail address
- Option to keep or discard a message received during an auto-reply period for a mail address
- Configurable time interval between auto-reply messages being sent to a particular mail address. Auto-reply messages are sent in response to messages being received while auto-reply is active for the recipient address. However, after one auto-reply message has been sent in response to a mail received from a particular address, no more auto-replies will be sent in response to any more mails sent from that same address until a configured time interval has expired since the first one was sent (AUTOREPLY\_INTERVAL System Parameter).
- An AUTOREPLY message can be setup to include the original message in the reply. It is also possible to restrict the content of the original message to the headers only by activating the NDR\_INCLUDE\_ONLY\_HEADERS System Parameter.

## 11.1.5 Configurable NDR Contents

As well as the subject and text of Non-delivery reports being configurable (see 11.5.9), whether the original message is attached to an NDR is also configurable. This can be configured differently for NDRs being delivered locally and NDRs being delivered externally.

For NDR messages sent externally, the NDR\_RELAY\_INCLUDE\_ORIG\_MSG System Parameter indicates whether the original message should be included or not.

For NDR messages destined for local users, the NDR\_INCLUDE\_ORIG\_MSG Domain Parameter indicates whether the original message should be included or not.

Further more, if an NDR is to include the original message, it is possible to restrict the content of the original message to the headers only, i.e. the message text and any attachments will not be included (NDR\_INCLUDE\_ONLY\_HEADERS System Parameter).

## 11.1.6 Spam Checking

OmniMessaging allows the following types of Blacklisting:-

- IP Address of the sending MTA

## *OmniMessaging Functional Description*

- Domain of sending MTA
- SMTP From Address

Each of the above can be blacklisted at the following levels:-

- System Level
- Domain Level (the local recipient's domain)

Finally the system also allows SMTP From Address blacklisting at mailbox level.

Domain Level and Mailbox Level spam checking can be activated or inactivated via system parameters (DOMAIN\_LEVEL\_SPAM\_CHECKING, MAILBOX\_LEVEL\_SPAM\_CHECKING)

### 11.1.7 Pretension to Receive Spam

OmniMessaging by default rejects mail from blacklisted IP addresses, domains or From Addresses. By enabling the Pretension flag the message is accepted but later discarded. This feature does not allow the sender to know that the mail is being rejected.

### 11.1.8 Relay Mail Blocking

When a message is received from an SMTP session with a recipient address that is not local, then the message has to be passed out to a remote MTA. This is relaying.

Within OmniMessaging relaying is allowed in the following cases:-

- the SMTP session has been authenticated via the SMTP auth extension
- the SMTP session is from a local client (see subnet checking below)
- POP Before SMTP is active and the SMTP client has already logged in via POP or IMAP
- Whitelist Checking is enabled AND the domain for the recipient address is present on the System Relay Whitelist table

N.B. If Whitelist Checking is not enabled, and the SMTP session does not satisfy one of the first three criteria above, relaying is not allowed for the session.

This Whitelist Checking is configurable on the MTA Send servers (NSIM-X-CHECK-SYSRDTB server parameter).

Subnet checking is carried out against the IP address of the remote SMTP client. If the check acknowledges that the client IP address is local, then relaying is allowed.

# *OmniMessaging Functional Description*

## 11.1.9 Delivery Notification Interface

OmniMessaging provides an optional delivery notification interface. This facility can be activated via a Service Package level parameter (DELIVERY\_NOTIFICATION).

If Delivery Notification is active, all the following types of mail arriving at a local address's target mailbox, will cause a record to be written to a special Delivery Notification queue file:-

- Messages sent straight to recipient address
- Messages sent to Distribution Lists / Aliases and then forwarded to recipient address
- Non Delivery Reports
- Quota Warnings

Each queue file entry holds the following information:-

- SMTP Address
- UID
- Message Size

The Queue File can be used by external systems, e.g. to notify mobile phone customers that messages are in their mailbox.

## 11.1.10 Virtual Domain Support

Supporting virtual domains, in the simplest terms, means a single OmniMessaging instance appears to its users and the outside world as multiple systems while to the system operators it is a single instance. This feature allows the system administrator to configure multiple domains on a single IP address.

One result of this is that submission addresses in one domain may be reused in another domain and represent different addresses e.g. ([fred@doamin1.com](mailto:fred@doamin1.com), [fred@domain2.com](mailto:fred@domain2.com)).

Each virtual domain has its own postmaster and administrator.

All virtual domains share a common message store (data base and discs used to store message files).

## **11.2 Configurable Limits**

### **11.2.1 Max Mailbox Size**

Max Mailbox Size limits are configurable at the following levels which are listed in order of usage, i.e. if the Mailbox Root level value is specified then it is used, otherwise the Service Package level value is used, and so on:-

- Mailbox Root
- Service Package
- System

Within an IMAP session, if an Append or Copy command causes the mailbox size limit to be exceeded, then the mail will not be delivered to the targeted mailbox and a NO response will be returned indicating to the user that the size limit has been exceeded.

If a mail arrives via an SMTP session, which causes the target mailbox size limit to be exceeded, then the mail will not be delivered to the recipient, but instead an NDR "Mailbox Full" mail is returned to the sender. Also, periodically, mail received by a full mailbox will cause a warning mail to be delivered to the recipient mailbox indicating the mailbox is full. The minimum interval between warnings generated in this way is equal to a configurable time interval (WARN\_MAIL\_SEND\_INTERVAL system parameter).

It is possible to set the limits at each level to indicate no limit.

The mailbox size for mailbox size limit checking is calculated as the total of the size of all mailboxes below a root mailbox.

### **11.2.2 Mailbox Size Threshold Warnings**

Mailbox Size Thresholds are configurable at the following levels which are listed in order of usage, i.e. if the Mailbox Root level value is specified then it is used, otherwise the Service Package level value is used, and so on:-

- Mailbox Root
- Service Package
- System

The Mailbox Size Threshold parameter holds a percentage value. The Threshold size is calculated using this percentage and the Max Mailbox Size. The total size of all mailboxes below a root mailbox is compared against the calculated threshold size.

Within an IMAP session, if an Append or Copy command causes a mailbox size threshold to be exceeded, then the mail will be successfully delivered to the mailbox but the OK response will warn the user that the threshold has been exceeded and will indicate the percentage full.

If a mail arrives via an SMTP session, which causes the target mailbox size threshold to be exceeded, then the mail is delivered successfully. However,

## *OmniMessaging Functional Description*

periodically, a warning mail, indicating the mailbox is almost full with the percentage full, is also delivered to the recipient mailbox.

Only one warning, either in response to an IMAP Append or Copy command warning or in response to an SMTP mail, will be generated within a configurable time period (WARN\_MAIL\_SEND\_INTERVAL system parameter).

It is possible to set the limits at each level to indicate no limit.

Again the mailbox size used for checking is the total of the size of all mailboxes below a root mailbox.

### 11.2.3 Max Mailbox Messages

The maximum number of messages that can be in all mailboxes below a root mailbox is configurable at the following levels which are listed in order of usage, i.e. if the Mailbox Root level value is specified then it is used, otherwise the Service Package level value is used, and so on:-

- Mailbox Root
- Service Package
- System

Within an IMAP session, if an Append or Copy command causes the maximum number of mailbox messages to be exceeded, then the mail will not be delivered to the targeted mailbox and a NO response will be returned indicating to the user that the max mailbox message number limit has been exceeded.

If a mail arrives via an SMTP session, which causes the maximum number of messages for the mailbox hierarchy to be exceeded, then the mail will not be delivered to the recipient, but instead an NDR "Mailbox Full" mail is returned to the sender. Also, periodically, mail received by such a mailbox will cause a warning mail to be delivered to the recipient mailbox indicating the mailbox is full. The minimum interval between warnings generated in this way is equal to a configurable time interval (WARN\_MAIL\_SEND\_INTERVAL system parameter).

It is possible to set the limits at each level to indicate no limit.

The total number of mailbox messages for checking against the max mailbox messages limit is calculated as the total number of messages in each of the mailboxes below the root mailbox.

### 11.2.4 Max Message Retention Period

A maximum Message Retention Period is configurable at the following levels which are listed in order of usage, i.e. if the Mailbox Root level value is specified then it is used, otherwise the Service Package level value is used, and so on:-

- Mailbox Root
- Service Package
- System

# *OmniMessaging Functional Description*

The Message Aging Server (MAS) uses this value to ascertain when messages can be deleted out of mailboxes.

It is possible to set this limit to indicate that messages should be retained indefinitely.

## 11.2.5 Max Local Message Size

Max Local Message Size is configurable at the following levels which are listed in order of usage, i.e. if the Mailbox Root level value is specified then it is used, otherwise the Service Package level value is used, and so on:-

- Mailbox Root
- Service Package
- System

Within an IMAP session, if an Append or Copy command results in an attempt to append or copy a message that exceeds the local message size for the target mailbox, then the mail will not be delivered and a NO response will be returned indicating to the user that the message size limit has been exceeded.

If a mail arrives via an SMTP session, which exceeds the message size limit for the target mailbox, then the mail will not be delivered to the recipient, and instead an NDR "Message Too Large" mail is returned to the sender.

It is possible to set the limits at each level to indicate no limit.

N.B. the Max Local Message Size at system level is also used by the MTA to check the size of incoming mail destined for local addresses. The MTA will reject messages exceeding this value during an SMTP session.

## 11.2.6 Max Remote Message Size

The MTA uses the Max Remote Message Size limit to check the size of incoming mail destined for remote recipients. If the incoming mail is too large, the mail is rejected within the SMTP session with an appropriate response.

## 11.2.7 Max Mailboxes Per User

Creation of mailboxes during an IMAP session for a particular user is prohibited once the user has reached the system limit. The user can start creating mailboxes again once one or more mailboxes have been deleted.

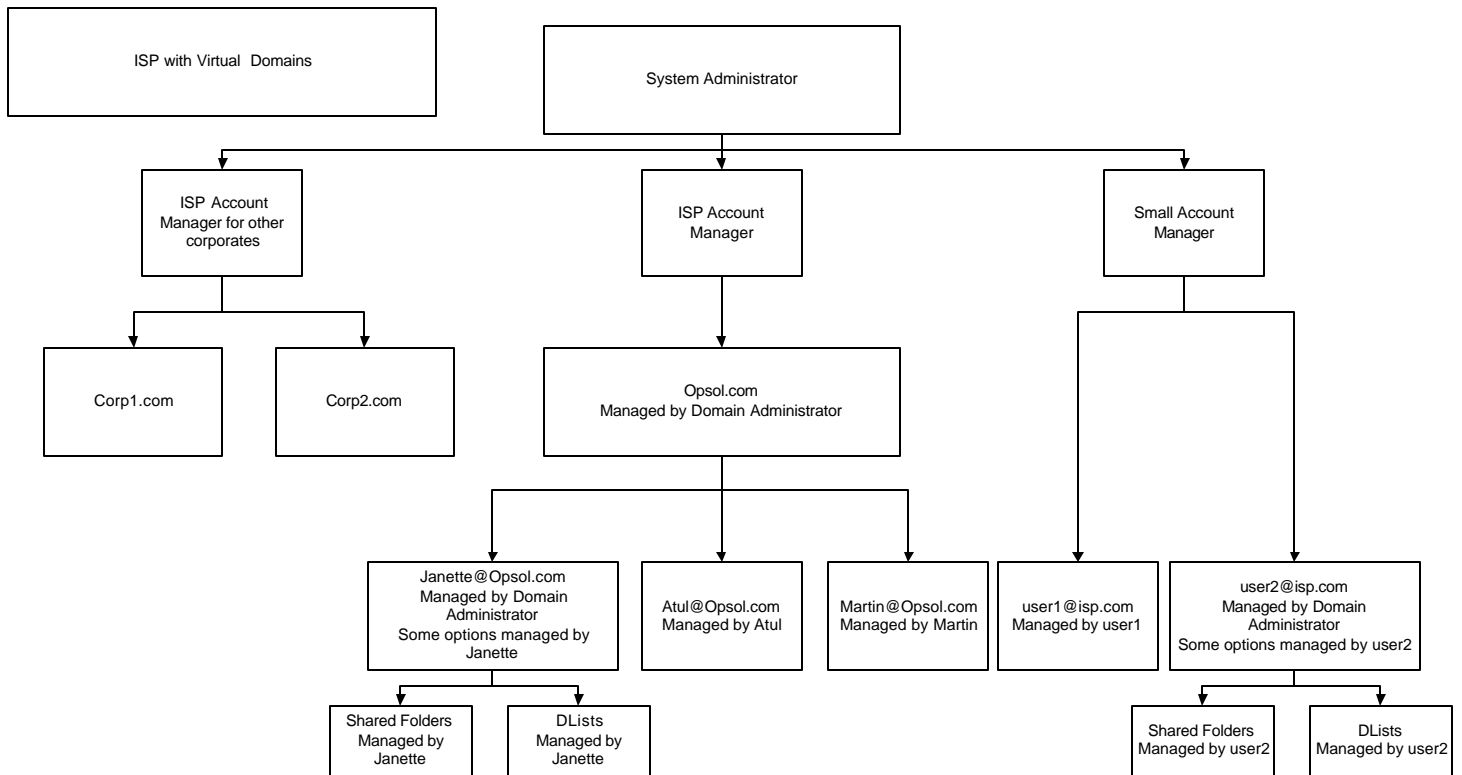
The total of all mailboxes below the users root mailbox is compared against the MAX\_MBOX\_PER\_USER system parameter.

## 11.2.8 Max Subscriptions Per User

Addition of new subscriptions via the IMAP SUBSCRIBE command during an IMAP session for a particular user is prohibited once the user has reached the system limit (MAX\_SUBSCRIPTION\_PER\_USER system parameter). The user can start adding more subscriptions again once one or more subscriptions have been deleted via the IMAP UNSUBSCRIBE command.

# OmniMessaging Functional Description

## 11.3 User Configuration



### 11.3.1 Service Package

A Service Package defines a packaged set of services for customers. An email provider may decide to offer customers differing levels of service depending on their status. For example Gold customers may be permitted larger mailbox and message sizes than say silver customers.

ASPs can also use the Service Package entity as a means of providing email services to ISPs and other companies. Attributes held at service package level permit an ASP to limit the number of domains, users and mail addresses their customers can define.

### 11.3.2 Account Ownership

OmniMessaging uses an account id to define a set of login users, domains and namespaces configured for a particular provisioning system account. A textual Id is provided as a means of linking the account with an external provisioning system.

### 11.3.3 Mail Users

The information held at user level permits individuals to login and authenticate themselves. OmniMessaging allows a user to be configured as either a POP3

# *OmniMessaging Functional Description*

or IMAP4 protocol user or both. The Login User Name is a unique string that should not be confused with the submission address. A Submission address defines the local part of the email address (i.e. person's name or job role 'sales', 'personnel' etc) and links this to the domain name.

OmniMessaging uses the Login User Name to denote ownership of mailboxes. A user can thereby have many mailboxes and many submission addresses for mail delivery.

In the event that a customer abuses the service, or has not kept up with payment, they can be suspended at user level. Mail retrieval and delivery is not permitted whilst they are in a suspended state, although existing mailbox content is retained should their status be re-activated.

## **11.4 Mailbox Management**

### **11.4.1 Mailbox Sharing**

OmniMessaging provides the means for sharing mailboxes. Mailbox Access can be set up to provide the following levels of access:-

LOOKUP	Mailbox is visible to LIST command
READ	Can SELECT, FETCH from, SEARCH and COPY from the mailbox
SEEN	Can STORE SEEN flag
WRITE	Can STORE flags (other than SEEN and DELETED)
INSERT	Can APPEND and COPY to the mailbox
CREATE	Can CREATE new sub-mailboxes
DELETE	Can STORE DELETED flag for messages in EXPUNGE from and DELETE and RENAME the mailbox (RENAME also requires that the user has CREATE access for the parent of the new mailbox)

Access to a mailbox can be by user or can be global. Mailbox information for a user is used first. If no such information exists, then, if global access information is stored for the mailbox, then this is used.

Any mailbox created will inherit the Mailbox Access Levels of its parent.

When a new user is created, the user's INBOX is automatically set up with full access rights for the user.

### **11.4.2 Mailbox Maintenance By Administrator**

The MSGMAINT server provides an administrator with a means of viewing messages for a particular user and mailbox. It allows the user to view details of the messages (UID, Size and Date Received) and select messages to be deleted or moved.

### **11.4.3 Optional Message Aging**

The Messaging Ageing Server (MAS) can be used to delete messages older than a particular time period. This time period is configurable via the NSIM-DEFAULT-AGEING-PERIOD server parameter on the MAS Server.



## *OmniMessaging Functional Description*

The MAS server can be configured to delete messages on a per user basis with the following options

Messages older than a certain period

Maximum number of messages in a mailbox

Mailbox size exceeded

# *OmniMessaging Functional Description*

## **11.5 Security**

### **11.5.1 POP Before SMTP Authentication**

OmniMessaging provides support for POP Before SMTP Authentication. This is an optional facility that is activated or deactivated by the POP\_BEFORE\_SMTP system parameter.

If active, this facility only authorises SMTP sessions for which one of the following is true:-

- There is a current POP or IMAP session in existence from the same IP address
- There has been a POP or IMAP session from the same IP address within a configured time period (POP\_BEFORE\_SMTP\_PERIOD system parameter)

If neither of the above criteria is met, the session is terminated.

### **11.5.2 Support for CRAM-MD5 Authentication Support**

OmniMessaging has the capability to support the transmission of passwords via plain text and via the use of an algorithm. This feature is implemented using standard protocol commands.

The OmniMessaging IMAP server supports CRAM-MD5 authorisation via the AUTHENTICATE command, whilst the POP server uses the APOP command.

### **11.5.3 Configurable Max Login Attempts**

OmniMessaging allows the configuration of a maximum number of failed logins for a valid user (MAX\_LOGIN\_ATTEMPTS System Parameter). Once this number is exceeded, an administrator inactivates the user account, pending reactivation.

### **11.5.4 Configurable Max Sessions Per User**

OmniMessaging allows the configuration of a maximum number of POP and IMAP sessions per user (MAX\_SESSIONS\_PER\_USER System Parameter). Once this number is reached, any further login requests (POP or IMAP) for the user are rejected.

### **11.5.5 Inactivity Timeout**

OmniMessaging allows the configuration of an inactivity timeout. For IMAP and POP sessions, if no command is issued before the configured inactivity timeout interval elapses, then the session is terminated.

The Inactivity Timeout value is configured via the NSIM-IMAP-INACT-TIMEOUT and NSIM-POP3-INACT-TIMEOUT parameters for the IMAP and POP servers respectively. The value is specified in minutes.

# *OmniMessaging Functional Description*

## 11.5.6 Login Timeout

OmniMessaging allows the configuration of a login timeout. For IMAP and POP sessions, if the user has not logged in successfully before the login timeout expires, then the session is terminated.

The Login Timeout value is configured via the NSIM-IMAP-LOGON-TIMEOUT and NSIM-POP3-LOGON-TIMEOUT parameters for the IMAP and POP servers respectively. The value is specified in seconds.

## 11.5.7 BCC Header Deletion

For full RFC compliance, OmniMessaging has the capability to delete the BCC header from within the Message header. By default this feature is inactive, but can be activated via the use of the REMOVE\_BCC\_HEADER system parameter setting.

## 11.5.8 Quoted User Name in Local Language

OmniMessaging provides Quoted User Name support as defined in RFC 2821. This allows for the use of characters not normally allowed in a user name either encapsulated in quotes or by escaping each character that is not normally allowed by the escape character “\”.

The special characters “\” and the double quote character must always be preceded by the escape character even if they appear in a quoted string, e.g.

john [“@main\helpdesk” smith@domain.com](#)

Would be reformatted for transmission as:-

“john \”@main\\helpdesk\” smith”@domain.com

## 11.5.9 Configurable Non-Delivery Report Messages

The header and text used in NDRs is configurable at system level within OmniMessaging. A separate mail message format can be configured for each of the following types of NDR: -

- Mailbox Full
- Message Too Large
- Recipient Redirection Error
- Invalid Reverse Path Error
- SMTP Error
- Mail Address Not Found
- SMTP Message too large
- Local Language support

## *OmniMessaging Functional Description*

### 11.5.10 Optional IMAP Login Failure

Within OmniMessaging it is possible to configure how a failed login is handled. This is to allow for differences between different client types.

There are two options:-

- Drop the session if the user fails authentication
- Retain the session if the user fails authentication

This is controlled by the system parameter

AUTH\_FAILED\_KEEP\_CONNECTION.

### 11.5.11 Use of local HOST or DNS lookup for IP resolution

OmniMessaging uses a two step sequence to resolve an IP address from a given domain name. Firstly the MTA checks the local HOST file to see if it can resolve the domain name locally. If it cannot be resolved locally, the MTA then invokes the DNS lookup service. The DNS lookup service is usually provided by an ISP and therefore resides on an external platform. In this scenario it can be beneficial to define frequently used domains locally on the HOST file to avoid a potential delay in doing an external lookup.

**Warning:** Adding entries to the local HOST file can result in performance improvements of lookup operations. However, in undertaking this operation, the customer must be aware of their responsibility to maintain the HOST file in the event of domain name/IP address changes.

## 12 APPENDIX - System Parameters

### Parameter Descriptions

The following table lists and describes all system parameters. Flags have values of either MSD\_ACTIVE or MSD\_INACTIVE.

Parameter	Description	Sect · Ref.	Units	Default Value	Special Values
MS_VERSION	Message Store Version			FIXED	FIXED
MAX_MSG_SIZE	Maximum Local Message Size	11.2 .5	Bytes	83,886,080	MSD_NOLIMIT
MAX_MAILBOX_SIZE	Maximum Mailbox Size	11.2 .1	Bytes	MSD_NOLIMIT	MSD_NOLIMIT
MAX_MSG_RETENTION_PERIOD	Maximum Message Retention Period	11.2 .4	Milli- secs	MSD_NOLIMIT	MSD_NOLIMIT
THRESHOLD	Mailbox Size Threshold	11.2 .2	%	100	none
IMAP_RESTRICTED_TO_SUBNETS	IMAP Restricted To Subnets		flag	MSD_INACTIVE	none
POP_RESTRICTED_TO_SUBNETS	POP Restricted To Subnets		flag	MSD_INACTIVE	none
IGNORE_QUOTAS_FOR_REPORTS	Ignore Quotas for Reports		flag	MSD_INACTIVE	none
IGNORE_QUOTAS_FOR_ALERTS	Ignore Quotas for Alerts		flag	MSD_INACTIVE	none
KEEP_UNDELIVERABLE_REPORTS	Keep undeliverable Reports		flag	MSD_INACTIVE	none
NDR_RELAY_OMIT_ORIG_MSG	For NDR Relay - Omit Original Message	11.1 .5	flag	MSD_ACTIVE-	none
DOMAIN_LEVEL_SPAM_CHECKING	Check for Domain Level Spam	11.1 .6	flag	MSD_INACTIVE	none
MAILBOX_LEVEL_SPAM_CHECKING	Check for Mailbox Level Spam	11.1 .6	flag	MSD_INACTIVE	none
MAX_BLIST_DOM_CACHE	Blacklist System Domain Cache size		count	100	none
MAX_BLIST_IP_CACHE	Blacklist System IP Cache size		count	500	none
MAX_BLIST_ADDR_CACHE	Blacklist System Address Cache size		count	500	none
MAX_BLIST_KEEP_PERIOD	Blacklist System Cache keep period		Milli- secs	10,800,000,000	none
MAX_BL_DOM_DOM_CACHE	Blacklist Client Domain Cache size		count	500	none
MAX_BL_DOM_IP_CACHE	Blacklist Client IP Cache size		count	100	none
MAX_BL_DOM_ADDR_CACHE	Blacklist Client Address Cache size		count	100	none
MAX_DOM_CACHE	Domain Cache size		count	100	none
MAX_DOM_KEEP_PERIOD	Domain Cache keep period		Milli- secs	300,000,000	none

## OmniMessaging Functional Description

Parameter	Description	Sect · Ref.	Units	Default Value	Special Values
MAX_SUBNET_CACHE	Subnet Cache size		count	100	none
MAX_SUBNET_KEEP_PERIOD	Subnet Cache keep period		Milli- secs	300,000,000	none
MAX_PARAMS_KEEP_PERIOD	System Parameter Cache keep period		Milli- secs	1,200,000,000	none
MAX_WLIST_DOM_CACHE	Whitelist Domain Cache size		count	100	none
MAX_WLIST_DOM_KEEP_PERIOD	Whitelist Domain Cache keep period		Milli- secs	300,000,000	none
AUTOREPLY_INTERVAL	Minimum interval between a second auto-reply message being sent to the same address	11.1 .4	Milli- secs	604,800,000,000	none
WARN_MAIL_SEND_INTERVAL	Minimum interval between a second warning mail being sent to a local user notifying them that their mailbox is greater than the threshold value or has exceeded its limit	11.2 .111 .2.2 11.2 .3	Milli- secs	17,200,000,000	none
DANGLING_MSG_KEEP_PERIOD	Dangling Message Keep Period (Minutes)		Milli- secs	7,200,000,000	none
MAX_MBOX_PER_USER	Maximum Mailbox Per User	11.2 .7	count	MSD_NOLIMIT	MSD_NOLIMIT
MAX_SUBSCRIPTION_PER_USER	Maximum Subscription Per User	11.2 .8	count	MSD_NOLIMIT	MSD_NOLIMIT
MAX_LOGIN_ATTEMPTS	Maximum Login Attempts	11.5 .3	count	MSD_NOLIMIT	MSD_NOLIMIT
MAX_SESSIONS_PER_USER	Maximum Sessions Per User	11.5 .4	count	MSD_NOLIMIT	MSD_NOLIMIT
REMOVE_BCC_HEADER	Activate Removal of BCC Header		flag	MSD_INACTIVE	none
POP_BEFORE_SMTP	Activate POP Before SMTP	11.5 .1	flag	MSD_ACTIVE	none
POP_BEFORE_SMTP_PERIOD	POP Before SMTP Period (Hours)	11.5 .1	Milli- secs	3,600,000,000	MSD_NOLIMIT
MAX_REMOTE_MSG_SIZE	Maximum message size for sending remote messages	11.2 .6	Bytes	83,886,080	MSD_NOLIMIT
NDR_INCLUDE_ONLY_HEADERS	Include header information only in NDR	11.1 .5	flag	MSD_INACTIVE	none
MAX_NUMBER_OF_MESSAGES	Max Number of Mailbox Messages	11.2 .3	count	MSD_NOLIMIT	MSD_NOLIMIT
AUTH_FAILED_KEEP_CONNECTION	For IMAP sessions – if login authentication	11.2 .3	flag	MSD_ACTIVE	none

## *OmniMessaging Functional Description*

Parameter	Description	Sect · Ref.	Units	Default Value	Special Values
	fails, retain the connection				

## **13 Billing Module**

(To purchase this additional module please contact your HP Sales Representative)

OmniMessaging provides users a Billing module that can be used to generate files in customized CDR formats. The files can be made available to other modules that run on platforms, like HP-Unix, Alphaservers, etc.

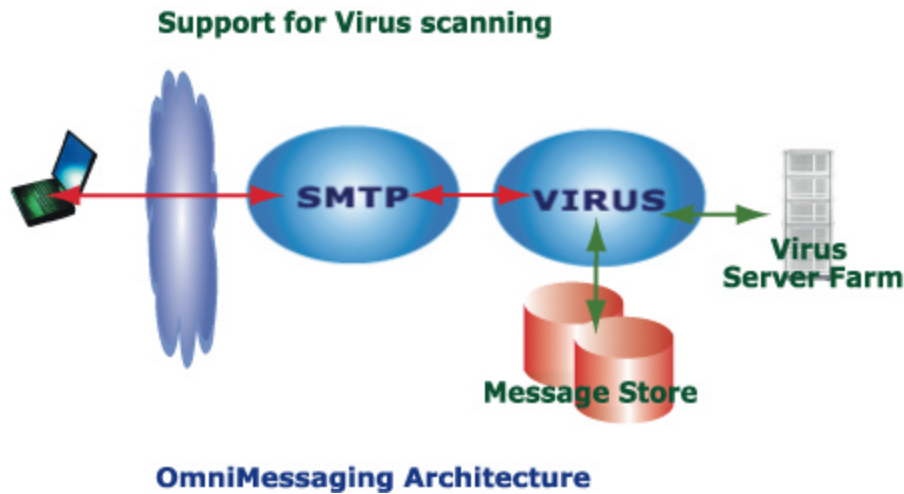
The OmniMessaging modules log every activity of the user and make the necessary information available to the Billing application. Thus the user's log is retained for information like connection-time, message-traffic and usage.

In addition the reports are also available over a Web interface. Thus the administrator can always use the Web screen to get a report on the usage in terms of mailbox-usage, daily/monthly usage, user-growth, message-traffic etc. These reports can be used to configure the system appropriately for better performance.



## 14 Virus Scan Module

(To purchase this additional module please contact your HP Sales Representative)



OmniMessaging performs the following:  
Filter out unwanted message.

1. Scan messages for rules.
2. Scan messages for virus.

Rules:

System / Domain /User level rules are defined in database.  
Rules can be applied to part of message like "Header" "Body" etc.

Virus Scan:

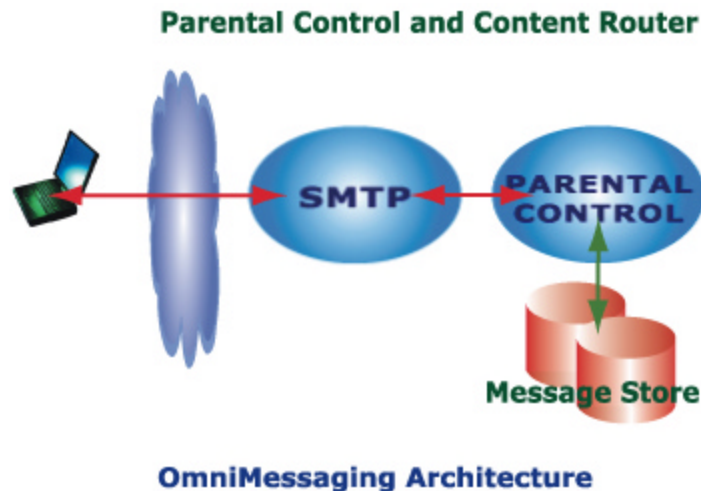
Message attachments will be scanned by PC based virus scan engine  
Protocol for the communication is virus engine based.

Thus when the message is received by the MTA, virus-scanning is performed prior to storing it in the database. The MTA server passes it on to the SCAN server, that interacts with the Virus-scan engine. The user can choose which types of attachments needs to be scanned by the Virus-scan Engine. The user will be notified if the mail is found to be infected, so that corrective actions can be performed.

OmniMessaging has been fully integrated and tested with Symantec AntiVirus Scan Engine for Windows® 2000.

## 15 Parental Control and Content Router

(To purchase this additional module please contact your HP Sales Representative)



OmniMessaging performs the following:  
Filter out unwanted message.

3. Scan messages for rules.
4. Scan messages for virus.

Rules:

System / Domain /User level rules are defined in database.  
Rules can be applied to part of message like "Header" "Body" etc.

Virus Scan:

Message attachments will be scanned by PC based virus scan engine  
Protocol for the communication is virus engine based.

If a message is found to violate the rules set by the Content-Parser or Parental Control engine then take one of the following actions.

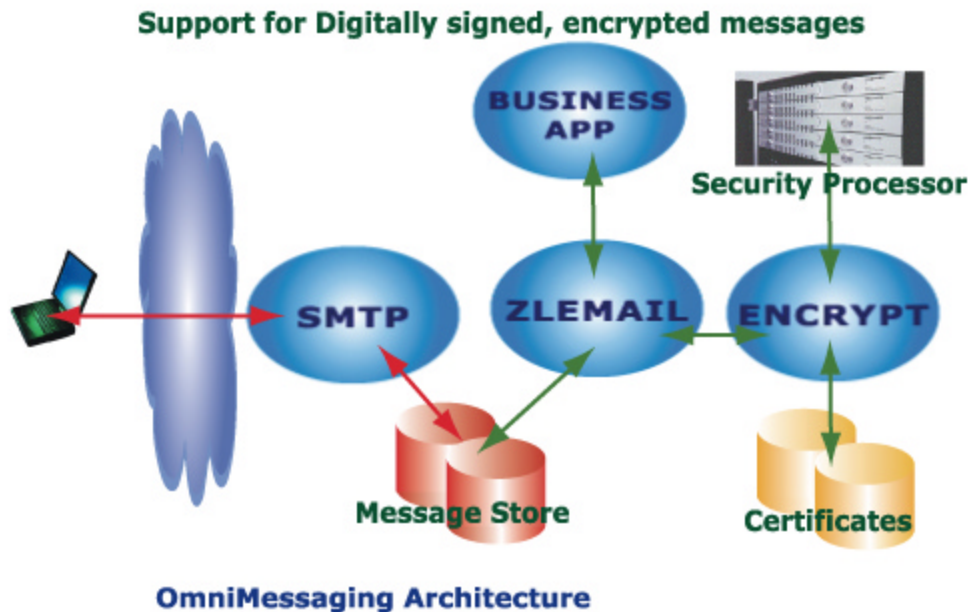
- a. Forward to parent: whole / partial
- b. Move message to spam folder
- c. Delete message
- d. Quarantine such attachment.

Thus specific actions can be taken based on the rule-violation.

Thus when the message is received by the MTA, virus-scanning is performed prior to storing it in the database. The MTA server passes it on to the SCAN server, that applies the rules. The user or administrator can configure the rules based on whether it is user-specific or system-specific.

### 16 ACH / EDI Support with Digital Signatures X.509

(To purchase this additional module please contact your HP Sales Representative)



#### 16.1 Secure email is defined as

- 1) The value-bearing portion, or the entire body, must be encrypted.
- 2) The value-bearing portion, or the entire body, must be authenticated via digital certificate.

#### 16.2 Some requirements for Secure email

- 1) Customers want to be able to send us financial transactions using secure email.
- 2) They want transaction returns via secure email. (Returns are transaction rejects).
- 3) They want to receive reports via secure email.
- 4) There might also be a need to receive confirmations (i.e. "yes, we received such-and-such") via secure email.
- 5) Web application screens allow users to request a report delivery via email.
- 6) Replace large daily fax transmissions with email.
- 8) Must have a programmatic API to email support to legacy applications.
- 9) Must function through proxies for digital certificate handling.
- 10) Must interface with other mail servers for receiving and transmitting email.

#### 16.3 Encrypted and digitally signed emails

OmniMessaging supports Secure Messages with full support for PKI certificates. An end user prepares the message using their standard email client such as Outlook or

## *OmniMessaging Functional Description*

Netscape. A user may optionally choose to encrypt or digitally sign the message or even a combination of encryption and signature. The message is then delivered via the internet to Bank's mail server.

The OmniMessaging POP client retrieves these messages from the remote (Lotus, Exchange, Hotmail etc) Mail server and securely stores these messages in the OmniMessaging Message Store.

The business application requests for new messages via a published interface. The ZLEMail adapter extracts the message and passes it to the Business Application. The message is first decrypted and the digital signature verified for authenticity.

There are times when the business application needs to send a secure message / file to the end user. This can be achieved using the published interface to send emails. The ZLEMail adaptor will digitally sign and encrypt the message using the organizations digital certificate.

The OmniMessaging MTA will relay the message to the Lotus mail server. The message is fully encrypted and secure during transit and can only be decrypted by the user for whom it is intended. The mail server will deliver these messages over the internet to the destination users' mailbox.

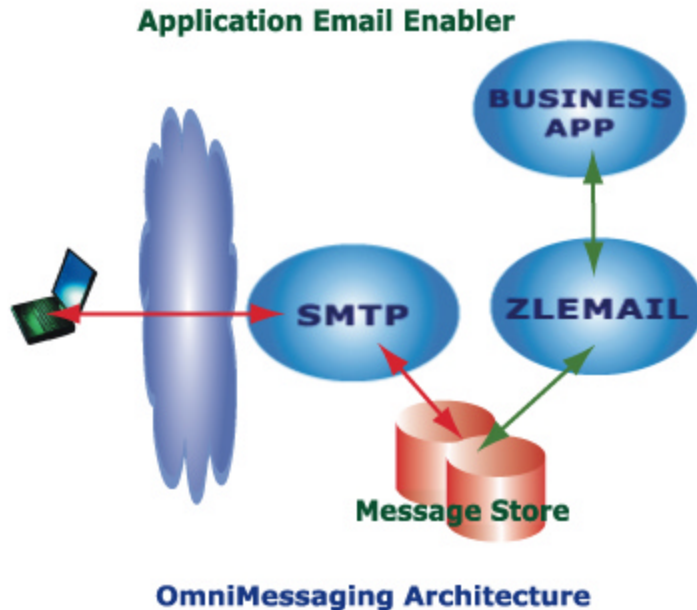
Benefits of this approach

- Secure transport of messages and attachments using simple inexpensive methods
- High Level of security using industry standard Public Key Infrastructure
- Very secure and yet very inexpensive to implement
- Support for large message size and attachments

The user certificates and organization certificates are stored on the NonStop server for security and fast access. The entire encryption / decryption is performed using the industry's most secure hardware devices built by the HP Atalla Division. The HP Atalla devices support 3DES encryption standards, are tamper proof and prevent electro magnetic hacking, vibrations etc to ensure that Bank's private certificate is 100% safe.

## 17 Deliver Invoices, Statements via email

(To purchase this additional module please contact your HP Sales Representative)



The ZLEMail Adapter is provided to email enable applications. Applications can send email messages to internet users via the ZLE Adapter. The Adaptor can be invoked by applications on the platform as well as applications off the platform. The adaptor supports a simple input buffer. Applications on the NonStop™ platform can invoke the ZLE Adapter via a simple server class send. Applications from an NT or UNIX platform can invoke the adaptor using a socket interface.

The applications generating the emails can reside on any Network server.

Value proposition: Corporate Users Value Added Services

## **18 Consolidates users email addresses**

(To purchase this additional module please contact your HP Sales Representative)

The POP Client is an email gathering utility to retrieve mails from a mailbox residing on a remote system using POP3 protocol to a local OmniMessaging mailbox on our system. The POP client is an add-on component to the OmniMessaging Core.

The POP Client interfaces with the users email server using the POP3 protocol and retrieves the mails for the user. These mails are then stored by the POP Client in the users' local OmniMessaging mailbox.

### **18.1 Features**

- Retrieves messages from multiple email addresses
- Passwords are stored in encrypted form in the OmniMessaging Message Store
- Supports delete messages from remote server or leave messages on remote server
- Configurable retrieve messages interval per user

## 19 Voice Mail server

(To purchase this additional module please contact your HP Sales Representative)

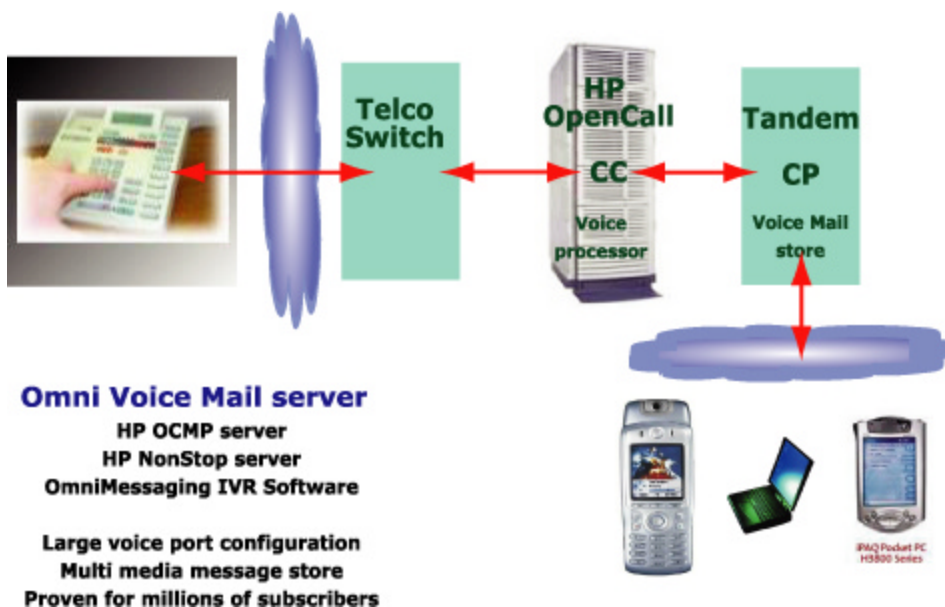
OmniMessaging Voice Mail server is for Carriers and Mobile Operators supporting millions of voice mail boxes. Voice messages can be accessed via standard phones, mobile phones, email and MMS clients. The solution is completely integrated with the carriers Network Protocols to provide Intelligent Messaging Services.

The GUI enables easy customization of prompt menus so it is easy to replace existing aging Voice Mail servers with newer technologies and yet eliminate user retraining.

### 19.1 Recording Voice Messages

Voice messages are recorded in the CC component and these are then safe stored using the OmniIVR Message Store on the NonStop SQL database. The message store is secure, reliable and scalable. There are no practical limits on the message store and it can grow to large sizes. The message store can be upgraded online and new capacity added online. This feature allows us to start with a small configuration and grow as more capacity is needed.

#### OmniMessaging Voice Mail server architecture



### 19.2 Retrieving Voice Messages

Voice messages are retrieved from the OmniIVR Message store in real time and played using the HP IVR. The user has several options to store, delete, fast forward, rewind, increase the volume etc.

### **19.3 Deleting Voice messages**

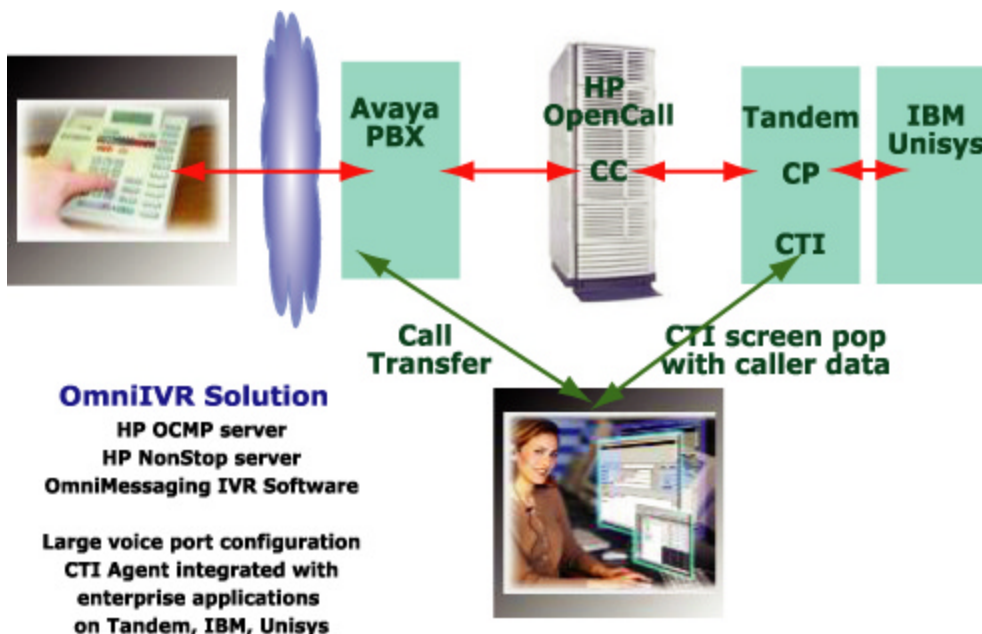
The system deletes the voice messages from the message store in a two phased approach. The messages are first marked for logical deletion and control returned immediately to the user. The task of physical deletion is performed later in deferred online mode.



## 20 OmniIVR Solution Overview

(To purchase this additional module please contact your HP Sales Representative)

The OmniIVR packaged solution consists of the Omni Software and the HP Open Call Platform. The OmniIVR solution is superior because of its large scalability and tight enterprise integration with the United States House of Representatives, "The Telco", business applications.



## 21 Solution details

### 21.1 Packaged IVR

Opsol has selected the HP Open Call IVR platform for its superior capabilities in handling large number of simultaneous connections. The solution is proven and deployed at several large Telcos. Based on the model types and interfaces the HP Open Call IVRs can handle from 192 (T1 interface) up to 1500 (OC3 interface) simultaneous connections from a single device.

### 21.2 Pre recorded prompts

The solution comes with standard pre recorded prompts and custom messages can be created and updated in real time using a simple interface.

Multiple prompts can be played based on a configured sequence to establish a call flow.

# *OmniMessaging Functional Description*

The prompts are delivered to the central Tandem system and then propagated to all the HP Open Call servers in real time. The update is almost instantaneous and with this method the operator does not need to worry about inconsistency between the servers. Custom messages can be recorded using standard phones.

## **21.3 Adding dynamic content to the prompt**

The prompts can be sequenced to create the flow of static as well as dynamic data. The dynamic prompts are also pre recorded but played based on business rules.

## **21.4 Retry busy numbers for outgoing calls**

The OmniIVR solution can be used to broadcast customized messages to a large list of users. The content in each message can be dynamically created for each message based on business rules and results from the business application.

The OmniIVR solution will re queue busy numbers for later processing. Multiple queues are configured for parallel processing.

If multiple touch points are configured for a person then the call will roll over to the next preferred method to reach the user. These preferences are provisioned by the administrator or the end user in advance. Web interfaces are provided for provisioning.

E.g. user may select the rollover as  
Cell phone  
Land Line  
Alternate Land Line  
Email

Calls are retried based on a decay logic where time interval between every successive retry is increased till the maximum number of retries are exhausted. Retry attempts and the retry interval are configurable.

Internal communication errors, fail over etc are retried immediately.

## **21.5 Confirmed Delivery**

The Opsol solution supports guaranteed delivery and the customer may optionally enable this feature. This feature should be enabled for applications such as delivering a statement, balance etc and should be disabled for emergency broadcasts. At the time of an emergency broadcast it is recommend that this feature is disabled because it increases the call setup time as well as the processing on all infrastructure components. It is also important to reach the user in as many ways as possible to increase success rates.

## **21.6 Call reporting / Auditing facility**

# *OmniMessaging Functional Description*

A logging facility is provided by the OmniIVR application. It identifies the status of each call, duration, success / failure etc. Detailed CDRs are logged so that they can be used for billing and audit purposes.

## **21.7      Scaling for volumes**

OmniIVR has been designed for the enterprise so that all components can be replicated to handle large volumes. This allows configuring multiple Call Control and multiple Call Processing instances. If the number of simultaneous calls increases then multiple HP Open Call servers can be configured. In this method the solution can grow to very large volumes. The configuration is flexible and any component can communicate with the other to result in optimum resource utilization.

## **21.8      Load Balancing**

The PBX routes messages to the OmniIVR based on routing configuration and automatic call distribution supported by the Avaya PBX. The OmniIVR components will automatically get distributed across the multiple process instances on the Tandem. The least busy resource on the Tandem gets assigned to this call. From this point on a dedicated path is established and will be used through completion.

Similar algorithms are used for outbound calls thus ensuring equal distribution across the multiple HP Open Call servers. The HP Open Call servers are configured as devices and additional devices can be added online.

The IVRs are on a private LAN and can be accessed in El Paso or in Brentwood.

## **21.9      Fault Tolerance**

Multiple IVR devices are configured so processing can continue even if a server fails. The entire solution can be built with an N + 1 configuration and is able to easily handle the failure of a single component.

The PBX will stop routing inbound calls to a failed device and will instead route the call to the other devices in the configuration. Thus inbound call processing continues with no impact caused by the failed device.

The fail over algorithms isolate the failed component and stop routing outbound calls to that device. The outbound calls continue to be routed to active devices, thus ensuring that the call service continues.

In this solution the fail over is instantaneous and results in no impact to established calls.

# **22 Hardware and Software Components**

The OmniIVR Solution consists of the following components

OmniIVR HP Open Call Control Module

# *OmniMessaging Functional Description*

## OmniIVR Tandem Call Processing Module

### **22.1 OmniIVR Call Processing module**

This module is deployed on the Tandem server and provides the guts of the call processing. It communicates with the OmniIVR Call Control module to get the data from the caller. The data is transformed and passed to the Stand-In processes.

#### Features

- Load balancing outgoing calls across multiple HP Open Call IVR servers
- Load balancing incoming calls to available components on the Tandem
- Flexible business rules
- Tight integration with Tandem and S390 applications
- Socket interface to the OmniIVR Call Control module

### **22.2 OmniIVR Call Control module**

This module is deployed on the HP Open Call server and interfaces with the IVR hardware. The call control module can handle basic call flow and subsequently passes the data to the Call Processing module for business processing.

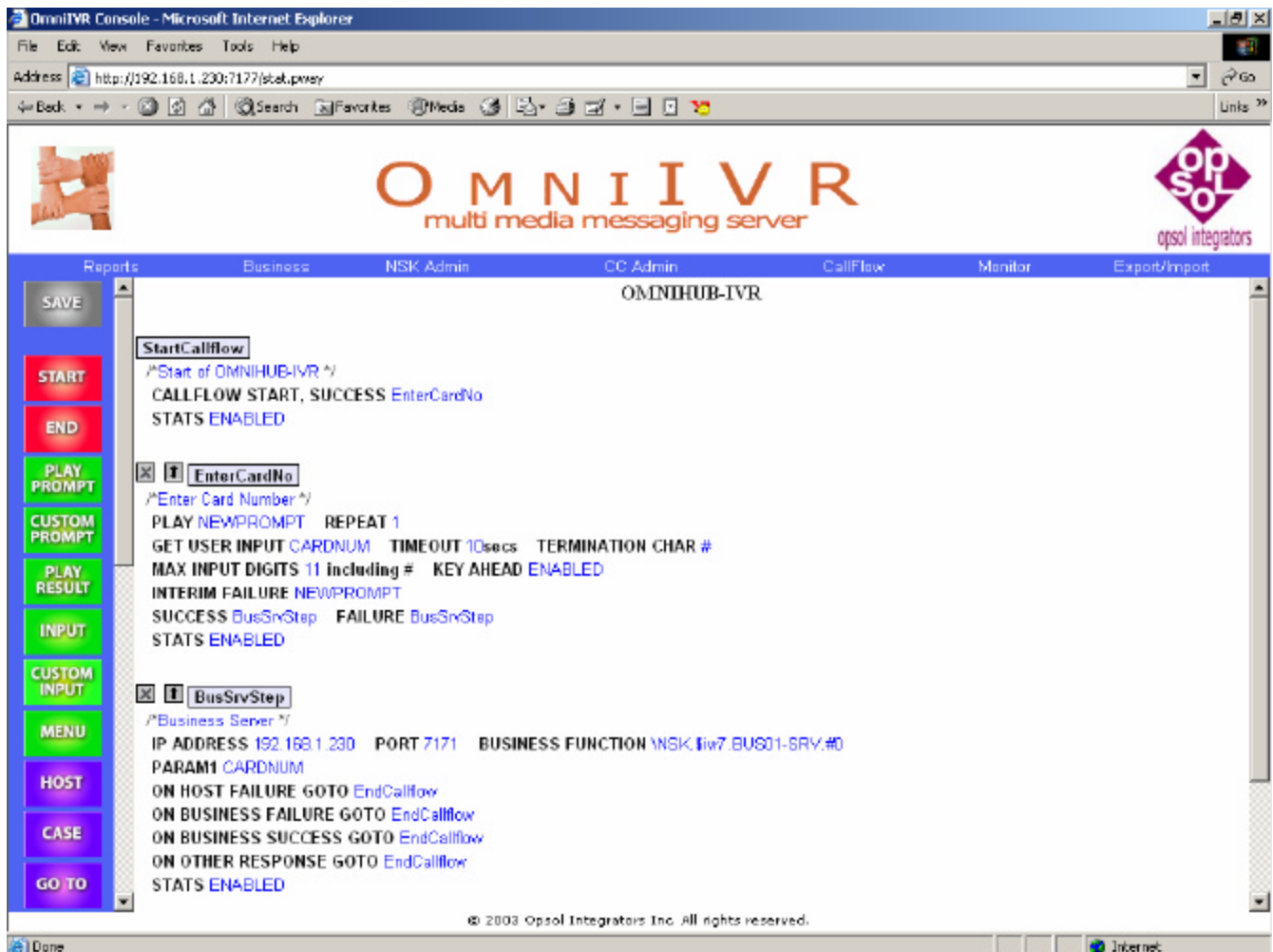
#### Features

- Call control logic on the HP Open Call IVR servers
- Plays voice prompts and menu options
- Receives input data and forwards to the Tandem
- Socket interface to the OmniIVR Call Processing module

# OmniMessaging Functional Description

## 22.3 Call Flow programming

Call Flow programming is performed with an easy to use Web based Service Creation Tool.



## 22.4 Reports and Statistics for IVR servers

The Console is a Web based interface to administer, configure and manage the OmniIVR solution. Customer will have modification rights to change the look and feel of the front end html screens.

### Reports on Time Intervals and Server Types

Reports can be generated for CP, CC and CTI with monthly, daily, hourly or with 10 minutes interval options. Monitoring reports can also be generated to monitor the server activity and gather recent statistics.

## *OmniMessaging Functional Description*

### **Stats table structure**

Reports are generated from stats table, which stores the statistics for CP, CTI and CC. Structure of stats table is show below.

Column Names	Description
Trans_Hash_Key	Hash Key to distribute the records evenly across all the partitions
Transaction_id	Unique ID generated for each transaction
Server_Type	Type of the server for which the stats are being collected
Start_Time	Start time of the transaction in Julian Timestamp
End_Time	End Time of the transaction in Julian Timestamp
Counter1-Counter125	General purpose counters for reporting purposes
Column1-Column10	General purpose columns for reporting purposes

# OmniMessaging Functional Description

## Options for Reports

Report generation is partially automated with the help of generation logic provided in Report Generation screen. In case of reports, which are timely based, the type of report generated is based on the difference between end time and start time.

The table shows the difference in the start time and time and the type of report generated.

Time Difference	Type of report Generated	Applicable to the servers
< 4 hours	10 minutes report	CC, CP, CTI
> 4 hours < 1 Day	Hourly report	CC, CP, CTI
> 1 Day < 1 Month	Daily Report	CC, CP, CTI
> 1 Month	Monthly report	CC, CP, CTI
Last 10 minutes	Monitoring Report	CC, CP, CTI

**Start date**

**End Date**

**Server**

**Start Time**

**End Date**

**Email Generator**

**CALL PROCESSING REPORT**

Start Date: 04/12/04 Time: 10:05:34  
Stop Date: 04/28/04 Time: 10:05:34

DATE TIME	TOTAL CALLS	CALL RATE	SOCK RECV TIMEOUT	SOCK SEND TIMEOUT	DIST READ ERROR	SOCKET ACCEPT ERROR	SOCKET SEND ERROR	SOCKET RECEIVE ERROR	IPC ERROR	SOCKET REPLY ERROR	MAX DURATION	MIN DURATION
2004-04-12	2	0	0	0	0	0	0	0	0	0	1745	444
2004-04-13	1	0	0	0	0	0	0	0	0	0	889	889
2004-04-14	1	0	0	0	0	0	0	0	0	0	593	593

[Download Report](#)

GENERATE RESET EMAIL

© 2003 Opsol Integrators Inc. All rights reserved.

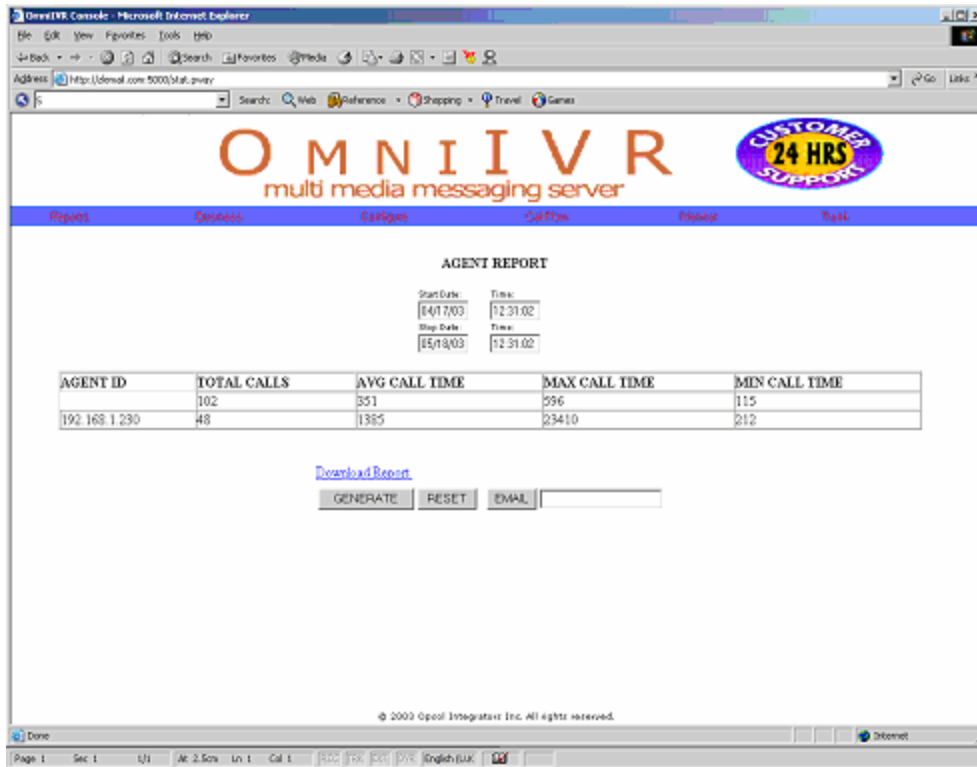
# OmniMessaging Functional Description

## Agent Statistics and Reports

Agent statistics for all the agents can be generated.

Input	Output	Constraints
Start_date, End_date, Start_time, End_time	Agent Statistics Report	

Output Attributes
Agent Id
Total Calls
Average Call Time
Maximum call Time
Minimum Call Time





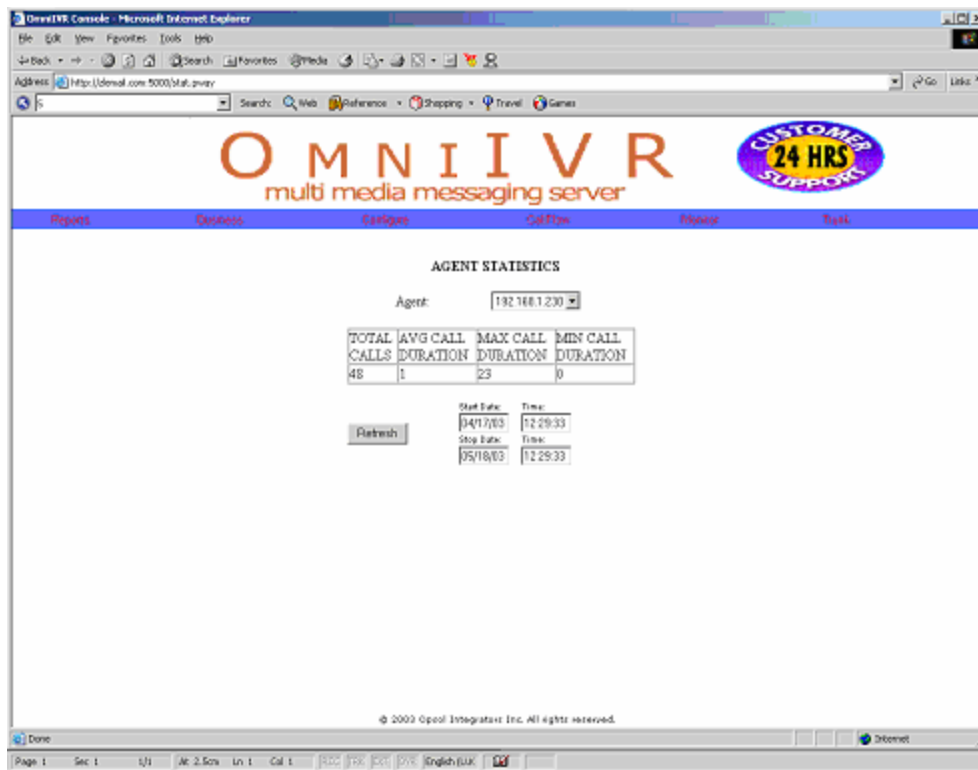
# OmniMessaging Functional Description

## Agent Statistics for particular Agent

Agent Statistics for a particular Agent can be generated.

Input	Output	Constraints
Start_date, End_date, Start_time, End_time, Agent_Id	Agent Statistics Report	

Output Attributes
Total Calls
Average Call Time
Maximum call Time
Minimum Call Time



# OmniMessaging Functional Description

## Emailing and downloading options for reports

Reports can be downloaded in the form of CSV files or can be emailed to the users.

**OmniVR**  
multi media messaging server

**24 HRS CUSTOMER SUPPORT**

**CALL PROCESSING REPORT**

Start Date: 05/12/03 Time: 14:15:11  
Stop Date: 05/12/03 Time: 22:15:11

[Download Report](#)

DATE	TOTAL CALLS	CALL RATE	SOCKET REC'D TIMEOUT	SOCKET SEND TIMEOUT	DIST READ ERROR	SOCKET ACCEPT ERROR	SOCKET SEND ERROR	SOCKET RECEIVE ERROR	IPC ERROR	SOCKET REPLY ERROR	MAX DURATION	MIN DURATION
2003-05-12-17:3	723	292	0	0	0	0	0	0	0	0	899	294
2003-05-12-17:5	844	281	0	0	0	0	0	0	0	0	1402	276
2003-05-12-18:1	861	289	0	0	0	0	0	0	0	0	1027	321

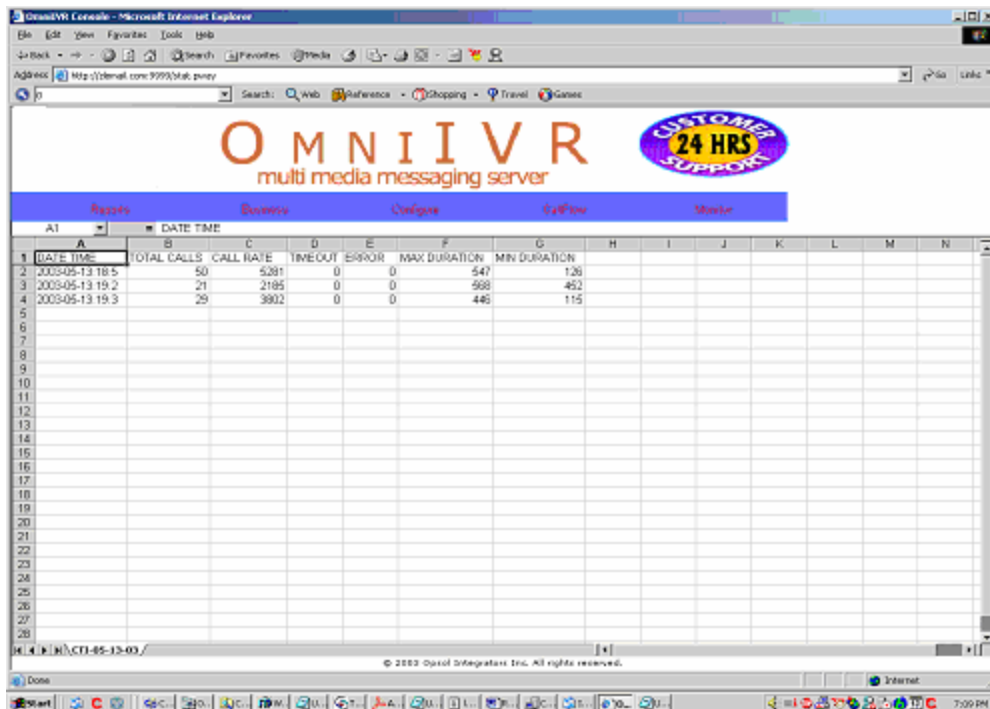
GENERATE RESET EMAIL

© 2003 Opsol Integrators Inc. All rights reserved.

Email

# OmniMessaging Functional Description

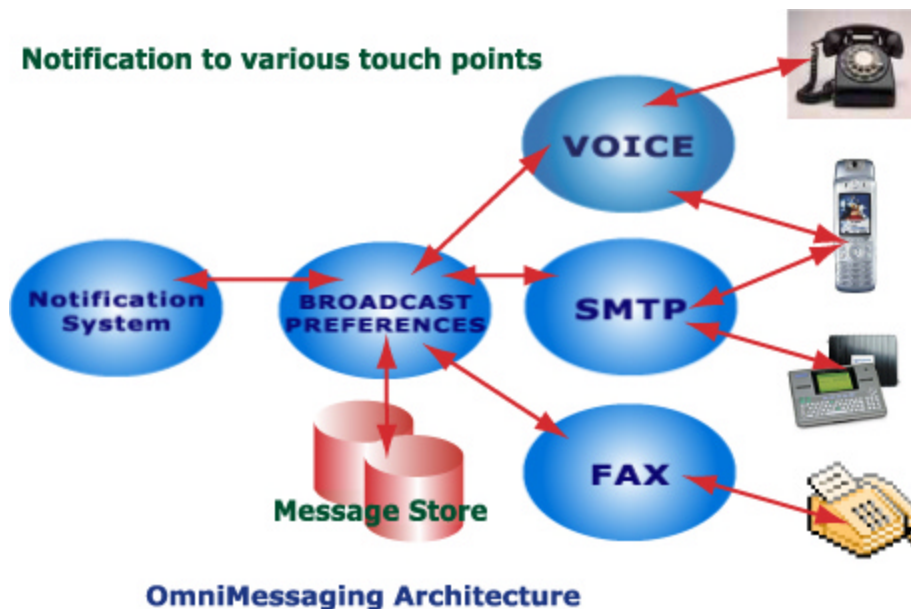
Reports downloaded in Excel format



The screenshot shows a web browser window displaying the OmniVR multi media messaging server interface. The interface includes a header with the OmniVR logo and a 'CUSTOMER SUPPORT 24 HRS' badge. Below the header is a navigation bar with links: Reports, Overview, Configure, Self-Test, and Monitor. The 'Reports' link is selected, and a report is displayed in a table format. The table has columns for DATE TIME, TOTAL CALLS, CALL RATE, TIMEOUT, ERROR, MAX DURATION, and MIN DURATION. The data is organized into rows, with the first row showing data for 2003-05-13 18:5.

DATE TIME	TOTAL CALLS	CALL RATE	TIMEOUT	ERROR	MAX DURATION	MIN DURATION
2003-05-13 18:5	50	5.281	0	0	547	1.26
2003-05-13 19:2	21	2.185	0	0	568	452
2003-05-13 19:3	29	3.802	0	0	446	1.15

## 23 Additional features to increase revenue



### 23.1 Delivering confirmations, notifications via voice messages, email, fax

## *OmniMessaging Functional Description*

The OmniMessaging components support message delivery to numerous touch points. With the OmniMessaging solution we can deliver statements, invoices, notifications to multiple touch points. Voice messages can be delivered to the card holder's cell phone or the card issuing company's phone. These messages can be application generated to notify of outstanding balances, payment receipt etc and may also include emails.

### **23.2 Supported touch points**

- Message to e-mail addresses
- SMS to cellular phone
- pre-recorded voice message to land line and cellular phone
- fax
- pager
- Qualcomm computer in the truck cab

### **23.3 Sending Outbound Faxes**

The OmniMessaging solution has a fax adapter that allows messages to be delivered from "The Telco" business applications to customers fax machines. Each fax is tracked for completion and can be retried until success.

The applications generating the faxes can reside on any Networked server.