© 2002-2011 KEMP Technologies, Inc. All rights reserved. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc.

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster product line including software and documentation. The use of the LoadMaster appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows and Microsoft Lync Server are registered trademarks of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.
Table of Contents

Table of Contents ..................................................................................................................................3

1 About KEMP Technologies..................................................................................................................5
  1.1 Load Balancing Microsoft Lync Server 2010..................................................................................5
  1.2 About This Manual .........................................................................................................................6
  1.3 Prerequisites ..................................................................................................................................6

2 Microsoft Lync Server 2010 Overview ..............................................................................................7
  2.1 Workloads .....................................................................................................................................7
  2.2 Server Roles ..................................................................................................................................8
    2.2.1 Standard Edition Server .........................................................................................................8
    2.2.2 Enterprise Edition - Front End server and Back End Server ..................................................8
    2.2.3 A/V Conferencing Server .......................................................................................................9
    2.2.4 Edge Server ...........................................................................................................................9
    2.2.5 Mediation Server ....................................................................................................................10
    2.2.6 Monitoring Server ..................................................................................................................10
    2.2.7 Archiving Server .....................................................................................................................10
    2.2.8 Director ..................................................................................................................................10
    2.2.9 File Server ..............................................................................................................................10
  2.3 High Availability Concepts ............................................................................................................11
    2.3.1 Standard Edition Server .........................................................................................................11
    2.3.2 Front End server and Back End Server ....................................................................................11
    2.3.3 A/V Conferencing Server .......................................................................................................11
    2.3.4 Edge Server ...........................................................................................................................11
    2.3.5 Mediation Server ....................................................................................................................11
    2.3.6 Monitoring & Archiving Server ...............................................................................................11
    2.3.7 Director ..................................................................................................................................12
  2.4 Overview of High Availability options per Lync Server Role ........................................................12
  2.5 Advantages to using a KEMP LoadMaster ....................................................................................12
  2.6 Optimizing the KEMP LoadMaster for Microsoft Lync 2010 ....................................................12
    2.6.1 Microsoft Terminology vs Kemp Terminology ......................................................................13
    2.6.2 Load Balancer Deployment Options .......................................................................................14
    2.6.3 SSL Acceleration (SSL Offloading) .......................................................................................15
    2.6.4 L7 Transparency .....................................................................................................................16
    2.6.5 Persistence ...............................................................................................................................16
    2.6.6 Idle Connection Timeout .........................................................................................................17
    2.6.7 Port Configuration ....................................................................................................................17
    2.6.8 Connection Scaling ..................................................................................................................17

3 Hardware Load Balancing vs DNS Load Balancing for Lync Server 2010 ......................................17
  3.1 Hardware Load balancing ...............................................................................................................17
  3.2 DNS Load Balancing ......................................................................................................................18
    DNS load balancing is introduced in Microsoft Lync Server 2010 communications software. The objective of DNS load balancing is to provide a native load balancing mechanism option in Lync Server 2010. A Hardware Load Balancer is still required for Load Balancing the Web traffic. ................................................18
  3.3 DNS Load Balancing matrix .........................................................................................................18

4 Network deployment Examples ..........................................................................................................20
  4.1 Typical Deployment Option ..........................................................................................................20
  4.2 Alternative Deployment Option: ...................................................................................................21
4.3 Alternative Deployment Option: .................................................................22
5 General Configuration ..................................................................................23
  5.1 Disable Global SNAT ..............................................................................23
  5.2 Change Drop Connections settings .......................................................23
  5.3 Increase the Connection Timeout .........................................................23
  5.4 Connection Scaling For Large Scale Deployments ............................23
6 Load Balancing Lync Front-End servers .................................................25
  6.1 Required Services for Front-End pools ................................................25
  6.2 Optional Services for Front-End pools ................................................26
  6.3 Configuring a Virtual Service for SIP services on the Lync Front-End servers ..................................................................................26
  6.4 Configuring a Virtual Service for Additional services on the Lync Front-End servers ......................................................................27
  6.5 Configuring a Virtual Service for Internal HTTPS-based services for the Front-End servers .................................................................27
  6.6 Configuring a Virtual Service for External HTTPS-based services for the Front-End servers ..........................................................28
7 Load Balancing Lync Director servers ....................................................29
  7.1 Required Services for Director pools ..................................................29
  7.2 Configuring a Virtual Service for SIP services on the Director servers .................................................................................................30
8 Load balancing internal Lync Edge servers ...........................................32
  8.1 Required Services for Edge pools facing internally ............................32
  8.2 Configuring a Virtual Service for SIP services on the Internal EDGE servers .......................................................................................32
  8.3 Configuring a Virtual Service for Additional services on the Lync Internal Edge servers .................................................................33
  8.4 Configuring a Virtual Service for Audio & Video services on the Internal EDGE servers .................................................................34
9 Load balancing external Lync Edge servers ...........................................35
  9.1 Required Services for Edge pools facing externally ............................35
  9.2 Optional Services for Edge pools facing externally ............................36
  9.3 Configuring a Virtual Service for SIP services on the External EDGE servers .......................................................................................36
  9.4 Configuring a Virtual Service for Remote User services on the External EDGE servers .................................................................37
  9.5 Configuring a Virtual Service for Conferencing services on the External EDGE servers .................................................................37
  9.6 Configuring a Virtual Service for TCP Audio/Video services on the External EDGE servers .................................................................38
  9.7 Configuring a Virtual Service for UDP Audio/Video services on the External EDGE servers .................................................................39
10 Document History ....................................................................................41
1 About KEMP Technologies

Since the year 2000, and with thousands of customers world-wide, KEMP leads the industry in driving the price/performance value proposition for application delivery and server load balancing to levels that businesses of any size can afford. KEMP’s LoadMaster family of purpose-built hardware and Virtual Appliances (VLM) offer advanced L4/7 server load balancing, content switching, SSL Acceleration and a multitude of other advanced Application Delivery and Optimization (ADC) features. The LoadMaster intelligently and efficiently distributes user traffic among application servers so that your users get the best experience possible.

1.1 Load Balancing Microsoft Lync Server 2010

An enterprise high available deployment of Lync Server requires deploying multiple servers in Front End pools, Director pools, and or Edge Server pools, Load balancing is necessary when using multiple servers in a pool and a Load Balancer distributes the traffic among the servers.

Microsoft Lync Server 2010 supports two load balancing solutions: DNS load balancing and hardware load balancing. You can choose different load balancing solutions for each pool in your deployment. Hardware load balancers are also required to provide load balancing for the internal and external web services when DNS load balancing is used.

The KEMP LoadMaster combines versatility with ease-of-use to speed deployment of the complete portfolio of advanced messaging applications and protocols used by Microsoft Lync Server 2010. Layer 7 health checking at the LoadMaster ensures that should one of the servers become inaccessible, the load balancer will take that server off-line, while automatically re-routing and reconnecting users to other functioning servers.

The entire KEMP LoadMaster product family, including the Virtual LoadMaster (VLM) supports Microsoft Lync 2010, and includes a comprehensive first year warranty and technical support agreement.

For more information about KEMP Technologies, visit us online at www.kemptechnologies.com or call +1 (631) 345-5292 (U.S.A.) or +1 353 61 260101 (Europe)
1.2 About This Manual

This manual addresses how to deploy and configure a LoadMaster appliance with Microsoft Lync Server 2010. Specifically, configuration information applies to Front-End pools, Director pools and Edge pools.

Kemps’ LoadMaster family of products is available in various models to support networks of different throughput requirements. Information in this manual applies to all LoadMaster models.

Images used in this manual are samples to help you determine if you are “in the right place” when actually performing the configuration.

Certain procedures contain instructions that refer to a Website. If you are configuring your LoadMaster at the same time you wish/need to access a Website then you should do so in a new and different browser session (i.e. do not use your web browser to access/configure the LoadMaster and then prior to finishing your configuration browse to a different URL and then use the “Back” button or other method to return to the LoadMaster).

1.3 Prerequisites

It is assumed that the reader is a network administrator or a person otherwise familiar with networking and general computer terminology. It is further assumed that you have set up your Microsoft Lync Server 2010 environment and have installed your KEMP LoadMaster.

You should have reviewed the LoadMaster Quick Start Installation documentation and the LoadMaster Configuration Guide. Documentation is available at http://www.kemptechnologies.com/documentation.

At a minimum, you should have:

• At least LoadMaster firmware 5.1-74
• Configured and published Microsoft Lync Server architecture with Lync Topology builder.
• Installed your Microsoft Servers, Active Directories and followed other Microsoft requirements.
• Configured Internal and External DNS entries for Front-End, Director and Edge pools.
• Established access to the LoadMaster Web User Interface.
• The Microsoft Lync 2010 Server was tested on Voice, Instant Messaging (IM), Presence, Desktop Collaboration and Audio Visual (AV) conferencing applications. Testing was performed for both internal and external users.
• Testing was performed using Microsoft Lync Server 2010 Enterprise Server with the 64-bit Microsoft SQL Server Enterprise Edition Version 2008 R2.
• All Lync 2010 Server Components were running on Windows 2008 R2 (64-bit) Standard Edition Server Operating System.
• Lync Clients were running Windows 7 Operating System.
• The lab setup was based on One-Arm deployment.
2 Microsoft Lync Server 2010 Overview

Microsoft® Lync™ ushers in a new connected user experience transforming every communication into an interaction that is more collaborative, engaging, and accessible from anywhere. For IT, the benefits are equally powerful, with a highly secure and reliable system that works with existing tools and systems for easier management, lower cost of ownership, smoother deployment and migration, and greater choice and flexibility.

Microsoft Lync Server 2010 communications software and its client software, such as Microsoft Lync 2010, enable the end users to connect in new ways and to stay connected, regardless of their physical location. Lync 2010 and Lync Server 2010 bring together the different ways that people communicate in a single client interface,

2.1 Workloads

The table below illustrates the major feature sets, also called workloads that Lync 2010 provides to the end user.

<table>
<thead>
<tr>
<th>Workload</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and presence</td>
<td>Instant messaging (IM) and presence help your users find and communicate with one another efficiently and effectively. IM provides an instant messaging platform with conversation history, and supports public IM connectivity with users of public IM networks such as MSN/Windows Live, Yahoo!, and AOL. Presence establishes and displays a user’s personal availability and willingness to communicate through the use of common states such as Available or Busy. This rich presence information enables other users to immediately make effective communication choices.</td>
</tr>
<tr>
<td>Conferencing</td>
<td>Lync Server includes support for IM conferencing, audio conferencing, web conferencing, video conferencing, and application sharing, for both scheduled and impromptu meetings. All these meeting types are supported with a single client. Lync Server also supports dial-in conferencing so that users of public switched telephone network (PSTN) phones can participate in the audio portion of conferences. Conferences can seamlessly change and grow in real time. For example, a single conference can start as just instant messages between a few users, and escalate to an audio conference with desktop sharing and a larger audience instantly, easily, and without interrupting the conversation flow.</td>
</tr>
<tr>
<td>Enterprise Voice</td>
<td>Enterprise Voice is the Voice over Internet Protocol (VoIP) offering in Lync Server 2010. It delivers a voice option to enhance or replace traditional private branch exchange (PBX) systems. In addition to the complete telephony capabilities of an IP PBX, Enterprise Voice is integrated with rich presence, IM, collaboration, and meetings. Features such as call answer, hold, resume, transfer, forward and divert are supported directly, while personalized speed dialing keys are replaced by Contacts lists, and automatic intercom is replaced with IM. Enterprise Voice supports high availability through call admission control (CAC), branch office survivability, and extended options for data resiliency.</td>
</tr>
<tr>
<td>Support for remote users</td>
<td>Full Lync Server functionality can be provided for users that are currently outside the organization’s firewalls by deploying servers called Edge Servers to provide a connection for these remote users. These remote users can connect to conferences by using a personal computer with Lync 2010 installed, the phone, or a web interface. Deploying Edge Servers also enables federation with partner or vendor organizations. A federated relationship enables the users to put federated users on their Contacts lists, exchange presence information and instant messages with these users, and invite them to</td>
</tr>
</tbody>
</table>

Copyright © 2002-2011 KEMP Technologies, Inc. All Rights Reserved.
audio calls, video calls, and conferences.

Integration with other products
Lync Server integrates with several other products to provide additional benefits to the users and administrators.

Meeting tools are integrated into Outlook 2010 to enable organizers to schedule a meeting or start an impromptu conference with a single click and make it just as easy for attendees to join.

Presence information is integrated into Outlook 2010 and SharePoint 2010.

Exchange Unified Messaging (UM) provides several integration features. Users can see if they have new voice mail within Lync 2010. They can click a play button in the Outlook message to hear the audio voice mail, or view a transcription of the voice mail in the notification message.

Lync Features and Workloads

2.2 Server Roles
To support the workloads as outlined in the previous paragraph, Lync server 2010 supports distinct server roles:

- Standard Edition Server
- Front End server and Back End Server
- A/V Conferencing Server
- Edge Server
- Mediation Server
- Monitoring Server
- Archiving Server
- Director

For most server roles, for scalability and high availability pools of multiple servers can be deployed. Each server in a pool must run an identical server role or roles. For some types of pools in Lync Server, a load balancer must be deployed to spread traffic between the various servers in the pool. The table below provides a scalability overview for all server roles when installed on physical servers.

2.2.1 Standard Edition Server
The Standard Edition server is designed for small organizations, and for pilot projects of large organizations. It enables many of the features of Lync Server 2010, including the necessary databases, to run on a single server thus combining many of the server roles on one server.

Standard Edition server offers instant messaging (IM), presence, conferencing, and Enterprise Voice, all from one server. One Standard Edition server supports as many as 5,000 users if deployed as a physical server.

2.2.2 Enterprise Edition - Front End server and Back End Server
The Front End server is the core server role, and runs many basic Lync Server functions. The Front End servers, along with the Back End Servers that provide the database, are the only server roles required to be in any Lync Server Enterprise Edition deployment.

Front End server includes the following functionality:

- User authentication and registration
- Presence information and contact card exchange
- Address book services and distribution list expansion
- IM functionality, including multiparty IM conferences
- Web conferencing and application sharing (if deployed)
- Application hosting services, for both applications included with Lync Server (for example, Conferencing Attendant and Response Group application) and third-party applications
- Application services for application hosting and hosts applications (for example, Response Group application, and several others)

Additionally, one Front End pool in the deployment also runs the Central Management Server, which manages and deploys basic configuration data to all servers running Lync Server 2010. The Central Management Server also provides the Lync Server Management Shell and file transfer capabilities.

The Back End Servers are database servers running Microsoft SQL Server that provide the database services for the Front End pool. Back End Servers do not run any Lync Server software. If a SQL Server cluster is already deployed for other applications, this cluster can be used for Lync Server 2010, if performance allows.

Information stored in the Back End Server databases includes presence information, users' Contacts lists, conferencing data including persistent data about the state of all current conferences, and conference scheduling data.

**Front End server Scalability**

A Front End pool, if deployed on physical hardware, should have one Front End server for every 10,000 users homed in the pool, plus an additional Front End server to provide good performance when one server is unavailable. The maximum number of users in one Front End pool is 80,000. If the number of users exceeds 80,000 users at a site, additional Front End pools can be deployed. To provide High Availability at least two Front End servers are required.

The additional Front End server ensures good performance in case one server is unavailable. When an active server is unavailable, its connections are transferred automatically to the other servers in the pool.

**2.2.3 A/V Conferencing Server**

The A/V Conferencing Server provides A/V conferencing functionality to the deployment. It can be collocated with Front End server, or deployed separately as a single server or A/V Conferencing Server pool. If a site has more than 10,000 users, it is recommended to deploy a separate A/V Conferencing pool.

**A/V Conferencing Server Scalability**

If A/V Conferencing Server is deployed separately, one physical A/V Conferencing Server for each 20,000 users at a site is needed.

**2.2.4 Edge Server**

The Edge Server enables the users to communicate and collaborate with users outside the organization's firewalls. These external users can include the organization's own users who are currently working offsite, users from federated partner organizations, and outside users who have been invited to join conferences hosted on your Lync Server deployment. Edge Server also enables connectivity to public IM connectivity services, including Windows Live, AOL, and Yahoo!.

**Edge Server Scalability**

For performance, one physical Edge Server should be deployed for every 15,000 users that are expected to access a site remotely.
2.2.5 Mediation Server

A Mediation Server is a necessary component for implementing Enterprise Voice and dial-in conferencing. The Mediation Server translates signaling and, in some configurations, media between the internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk.

Mediation Server Scalability

A co-located Mediation server scales to a maximum of 226 concurrent calls. If the call volume exceeds this maximum number a dedicated Mediation server can be deployed. A dedicated server scales to, depending of the hardware and the ration remote vs. internal users, to a maximum of 1,200 concurrent calls per server.


2.2.6 Monitoring Server

The Monitoring Server collects data about the quality of the network media, in both Enterprise Voice calls and A/V conferences. This information can help to provide the best possible media experience for the users. It also collects call error records (CERs), which can be used to troubleshoot failed calls. Additionally, it collects usage information in the form of call detail records (CDRs) about various Lync Server features. These metrics can be used to calculate return on investment of the Lync deployment, and plan the future growth.

Monitoring Server Scalability

One physical Monitoring Server can support up to 250,000 users if not collocated with Archiving Server. If collocated, it can support up to 100,000 users.

2.2.7 Archiving Server

The Archiving Server enables archiving of IM communications and meeting content for compliance reasons.

Archiving Server Scalability

One physical Archiving Server can support up to 500,000 users if not collocated with Monitoring Server. If collocated, it can support up to 100,000 users.

2.2.8 Director

Directors can be used to authenticate Lync Server user requests, but do not home user accounts, or provide presence or conferencing services. Directors are most useful in deployments that enable external user access, where the Director can authenticate requests before sending them on to internal servers. Directors can also improve performance in organizations with multiple Front End pools.

Director Server Scalability

For performance, one physical Director should be deployed for every 15,000 users who will access a site remotely. At a minimum it is recommend deploying two Directors for high availability.

2.2.9 File Server

Lync Server 2010 requires a file share for several services including the address book service, conferencing data and device update files. The file share is supported on either direct attached storage (DAS) or a storage area network (SAN), including Distributed File System (DFS), and on a redundant array of independent disks (RAID).
Lync Server 2010 supports the use of a shared cluster for the file shares in the Lync deployment. If a shared cluster for the file shares is used in the Lync deployment, the Cluster Administrator should be used to create the file shares.

2.3 High Availability Concepts

With the exception of the Archiving and Monitoring role and the standard edition server, all other Lync server roles can be deployed for high availability. The following sections describe the required additional components.

2.3.1 Standard Edition Server

The Standard Edition server combines many of the server roles on one server. High availability options are not available for the Standard Edition server therefore it is recommended to use Lync Server 2010 Enterprise Edition if a highly available solution is required.

2.3.2 Front End server and Back End Server

To improve availability Front End servers are deployed in a pool. A Front End pool is a set of Front End servers configured identically, that work together to provide services for a common group of users. A pool provides scalability and failover capability to the users. If multiple servers are configured in a Pool configuration, Hardware and or DNS load balancing is required to distribute the load and enable failover.

Increasing the availability of the Back End servers can be achieved by deploying a cluster of two or more servers.

2.3.3 A/V Conferencing Server

Conferencing servers can either be deployed co-located on the Front End servers in a pool or as one or more dedicated servers. When deployed co-located the pool setup assures high availability. In case of dedicated server deployment it is recommended to deploy at least two A/V Conferencing Servers for high availability.

2.3.4 Edge Server


If high availability is required, at least two Edge Servers should be deployed in a pool. A single Edge pool will support up to ten Edge Servers. If multiple servers are configured in a Pool configuration, Hardware and or DNS load balancing is required to distribute the load and enable failover.

2.3.5 Mediation Server

To improve availability multiple Mediation servers can be deployed. The Enterprise Voice routing component will reroute voice traffic in case of server or connection failure.

2.3.6 Monitoring & Archiving Server

Monitoring and or Archiving server outage will not negatively affect overall Lync service availability. Both server roles use Microsoft message queuing for data exchange and are therefore less susceptible to failure. If an Archiving or Monitoring server fails, messages will remain in the queue until the server is available again. The availability of the server role can be improved by upgrading the hardware specifications and clustering the Back End database server. It is possible to configure the Archiving service as critical for the Lync deployment; this will cause the Lync services to pause if the Archiving service is unavailable for a longer period of time and prevent messages
from not being archived. For this mode of operation a standby server could be considered to improve availability.

2.3.7 Director

Similar to the Front End server, Director server availability can be increased by deploying multiple director servers in a pool. A pool of Directors must be load balanced by either a hardware load balancer or by implementing Domain Name System (DNS) load balancing to take care of the SIP traffic.

2.4 Overview of High Availability options per Lync Server Role

<table>
<thead>
<tr>
<th>Role</th>
<th>High Availability</th>
<th>Load Balancer</th>
<th>DNS Load Balancing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Edition Server</td>
<td>Not Available</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Enterprise Edition Front End server</td>
<td>Deploy Multiple Server in a Pool and use Load Balancing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Back End Server</td>
<td>SQL Server uses Windows Clustering for High Availability</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>A/V Conferencing Server</td>
<td>Deploy Multiple Servers in a Pool. Load Balancing not required</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Edge Server</td>
<td>Deploy Multiple Servers in a Pool and use Load Balancing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mediation Server</td>
<td>Deploy Multiple Servers in a Pool and use Load Balancing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Standby Server (MSMQ on the Front-End queues messages in the event of a failure)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Archiving</td>
<td>Standby Server (MSMQ on the Front-End queues messages in the event of a failure)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Director</td>
<td>Deploy Multiple Servers in a Pool and use Load Balancing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>File Server</td>
<td>Use Windows Clustering or Distributed File System</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

2.5 Advantages to using a KEMP LoadMaster

KEMP LoadMaster offers performance, security and functional advantages that combine versatility with ease-of-use to speed deployment of the Microsoft Lync infrastructure. Layer 7 health checking at the LoadMaster ensures that should one of the servers become inaccessible, the LoadMaster will take that server off-line.

2.6 Optimizing the KEMP LoadMaster for Microsoft Lync 2010

Your KEMP LoadMaster has features and capabilities in addition to those described in this manual, however, these features and capabilities in particular can be used to optimize the configuration of LoadMaster to work best with your Lync 2010 server load balancing requirements.
2.6.1 Microsoft Terminology vs Kemp Terminology

2.6.1.1 Microsoft Terminology

Load balancers can be configured to support Network Address Translation (NAT) using one of the following modes:

- **Full-NAT (SNAT) mode** (also known as proxy, secure NAT, source NAT, or SNAT mode). In full-NAT mode, both the source and IP destinations are changed as packets pass through the load balancer.

- **Half-NAT (DNAT) mode** (also known as transparency, destination NAT, DNAT mode or Load Balancers Default Gateway LBDG). In half-NAT mode, the destination IP address is changed as packets pass through the load balancer, but the source IP address remains intact.

⚠️ Load balancing using Direct Server Return configuration is not supported.

The following table describes the supported configurations for full-NAT and half-NAT modes.

<table>
<thead>
<tr>
<th>Load-Balanced Pools</th>
<th>Supported NAT Modes</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise pools and</td>
<td>Full-NAT (SNAT)</td>
<td>Half-NAT is not supported for load balancing of internal pools because inter-server communications within an internal pool fail when servers in the pool try to connect to their own VIP.</td>
</tr>
<tr>
<td>Communicator Web Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edge pools</td>
<td>Full-NAT (SNAT)</td>
<td>The VIP for the external interface of Edge Servers should be set to half-NAT or full-NAT only for traffic to the edge (for each VIP that is used for Edge Servers and HTTP). Also, NAT is not supported for the IP address of the external interface of the A/V Edge Server of an Edge Server, so the IP address of the external interface of the A/V Edge service on each Edge Server must be publicly routable (no NAT).</td>
</tr>
<tr>
<td></td>
<td>and Half-NAT (DNAT)</td>
<td></td>
</tr>
</tbody>
</table>
2.6.1.2 Kemp Terminology

- **Full-NAT (SNAT)** mode is the equivalent of KEMP Non-transparency mode.
- **Half-NAT (DNAT or LBDG)** mode is the equivalent of KEMP Transparency mode.

How to configuring NAT options:

<table>
<thead>
<tr>
<th>Microsoft NAT</th>
<th>KEMP NAT</th>
<th>Layer</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full-NAT (SNAT)</td>
<td>Non-transparency</td>
<td>7</td>
<td>When creating a Virtual Service Layer 7 is check by default and you need to uncheck L7 transparency.</td>
</tr>
<tr>
<td>Half-NAT (DNAT) LBDG</td>
<td>Transparency</td>
<td>4</td>
<td>All layer 4 traffic is transparent, no configuration necessary. Default gateway needs to be changed on Real Server to point to IP Address of the Load balancer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>To configure transparency for Layer 7 (Force Layer 7) you just need to make sure that L7 Transparency check box is checked and you must change the default gateway on the Real Servers to point to the IP Address of the Load balancer.</td>
</tr>
</tbody>
</table>

2.6.2 Load Balancer Deployment Options

The supported deployments of the Lync Server and the Kemp Load Balancer are described in the following sections. Multiple Load Balancers can be deployed for Internal Pools, Internal Edge Server and External Edge Server. Single Load Balancers can be used to support both internal and external servers.

2.6.2.1 Lync Internal Server Deployment Options

Non-Transparent (Microsoft SNAT)

- **one-armed** topology
  
  This is the typical deployment method allowing the Load Balancer to be in the same network segment as the Real Servers.

- **two-armed** topology
  
  This topology requires a separate network for the Load Balancer and a separate network for the Real Servers. This requires more configurations networking wise and is considered not a typical deployment.

Transparent (Microsoft DNAT)

- **one-armed** topology & **two-armed** topology
  
  If you require that the Client IP Addresses then you have to use transparent mode.
  
  This topology is not supported as per Microsoft.
2.6.2.2 Lync External Edge Server Deployment Options

- **one-armed** topology & **two-armed** topology

  Transparency must be used when working with Load Balancers (at least for the Audio and Video EDGE Server).

More information about one-armed and two-armed topologies can be found in the LoadMaster Manual.

http://www.kemptechnologies.com/emea/loadmaster-documentation.html

2.6.3 SSL Acceleration (SSL Offloading)

The KEMP LoadMaster offers SSL acceleration (also referred to as “SSL offloading”) for Virtual Services. With SSL acceleration, the SSL session is terminated at the LoadMaster. Some of the benefits to using SSL acceleration are that the LoadMaster migrates the SSL workload from the Real Servers (which can be hardware accelerated by LoadMaster), can perform Layer 7 processing (such as persistence or content switching), SSL security hardening, and a central point of management of SSL certificates.

With SSL Acceleration, the SSL session is terminated at the LoadMaster and sent to the Real Servers un-encrypted. In some security situations, it may be necessary to encrypt the connection between the LoadMaster and Real Servers. This can be achieved with reverse SSL. Review the LoadMaster manual to configure a reverse SSL deployment.

With reverse SSL, the SSL session is first terminated at the LoadMaster. Persistence and other Layer 7 functionality can then be performed. After that, the traffic is re-encrypted in a new SSL session between the LoadMaster and the Real Server.

Without terminating the SSL session at the LoadMaster, the headers and content cannot be read, so persistence cannot be done. The only consistently reliable persistence method available when the SSL session is not terminated at the LoadMaster is Source IP.

Hardware SSL and Software SSL are the two types of SSL termination capabilities available in your LoadMaster. Functionally, hardware and software SSL are the same. The difference is in what part of the LoadMaster handles the actual cryptographic functions associated with SSL operations.

With software SSL, the LoadMaster’s general processor handles encryption/decryption tasks. These tasks are shared with other tasks that the LoadMaster performs, such as server load balancing, health checking, and other administrative tasks. Because SSL operations are CPU-intensive, software SSL is sufficient for low levels of SSL traffic but insufficient for higher levels of SSL traffic. Higher connection rates of SSL on a software SSL LoadMaster may degrade overall performance of the LoadMaster.

With hardware SSL, the LoadMaster has a separate specialized processor, which handles all SSL functions. No matter the level of SSL connections, the LoadMaster’s general processor is not burdened. This specialized hardware is purpose-built for SSL, and can handle extremely high connection rates (TPS) of SSL traffic.

An SSL certificate is required for all SSL transactions, and as such is required for all SSL-enabled Virtual Services. With the LoadMaster, there are two types of SSL certificates: self-signed certificates generated by the LoadMaster or the administrator and certificates that are signed by a trusted CA (Certificate Authority) such as Digicert, Verisign or Thawte. In addition, with LoadMaster you are managing only one certificate instead of multiple certificates on each Real Server.
When an SSL-enabled Virtual Service is configured on the LoadMaster, a self-signed certificate is installed automatically. Both self-signed and CA signed certificates provide encryption for data in motion. A CA-signed certificate also provides authentication -- a level of assurance that the site is what it reports to be, and not an impostor.

The primary operational difference between a self-signed certificate and a CA certificate is that with a self-signed, certificate cannot be used in conjunction with Lync Server 2010. As such, the Lync 2010 configuration instructions indicate that you would first need to export an appropriately signed certificate from Lync Server 2010 in order that you may import it into the LoadMaster.

SSL termination is required for load balanced connections to external Lync Web Services, SSL offloading (relieving a web server of all SSL processing) is not supported because Front End servers do not accept unencrypted HTTP requests for Lync Web Services.

By definition, Super HTTP persistence requires SSL termination on the load balancer, otherwise the load balancer would be unable to inspect HTTP traffic to look at the SSL and header Information. Both client_ssl and server_ssl profiles are required for this to work correctly. The client_ssl profile is used to decrypt the request, and as such, the certificate assigned to the client_ssl profile must contain the external web service FQDNs for the Lync Pool. The server_ssl profile is used to re-encrypt the request before routing it on to the Lync Pool.

The following are the requirements and recommendations regarding encryption:

- You must use TLS/MTLS for all communications between Lync Web App and servers that are running Microsoft Lync Server 2010.
- You should always use HTTPS unless SSL offloading is used for performance reasons and other effective security safeguards are in place.
- You may use HTTP for communications between a hardware load balancer or other device and the Lync Web App if SSL offloading is used for performance reasons. In this case, the physical link should be secured.
- Do not use HTTP between the client and the Lync Web App.

2.6.4 L7 Transparency

Newly created Virtual Services on a LoadMaster are set Transparent on a LoadMaster by default. In Transparent mode, the LoadMaster will forward traffic towards the Lync External EDGE Server while retaining the source IP address with which it arrived at the LoadMaster.

For L7 transparency for Lync External EDGE Servers to work properly:

a) The Real Server settings must ensure that all server replies to client requests are routed through the LoadMaster. Typically, this is achieved by making the LoadMaster the Real Server's default gateway.

b) No clients may be located in the same IP subnet with the Real Servers. If necessary, you can use additional ports on the LoadMaster to ensure that Real Servers and Clients are located on distinct IP subnets.

2.6.5 Persistence

Session persistence (a.k.a. Session Affinity or Stickiness) is the ability of the LoadMaster to make sure a given Client always gets to the same Real Server, even across multiple connections.
Persistence can make sure that all requests from a client are sent to the same server in a Server Load Balancer (SLB) array or server farm.

Source IP Address persistence is used for all Lync Services except the External Web Services which need to use Super HTTP Persistence.

### 2.6.6 Idle Connection Timeout

If there is no traffic for the period of time specified the connection is timed out and disconnected. The global default is 1800 seconds (30 minutes). This value should be adjusted per service type.

For each Virtual Service you can set idle connection timeout values for the TCP/IP connections. In order to make optimal use of your KEMP LoadMaster you should not set these timeout values too low as this could result in clients needing to reestablish a TCP/IP connection, which typically results in the end user will be informed to re-authenticate. It is recommended you test which timeout values works best in your specific scenario before the solution goes into production.

⚠️ The value in the field may show as a zero, which means the global default is the value used by the LoadMaster. The global value is set in the System Configuration; Miscellaneous Options; L7 Configuration; L7 Connection Timeout.

### 2.6.7 Port Configuration

There are many different types of possible data paths. It is recommended that your port configuration stay within the realm of default protocol RFC. However, your KEMP LoadMaster may be configured to use whichever port happens to be most appropriate for your particular network. For more information regarding port definitions, refer to Microsoft documentation at http://technet.microsoft.com/en-us/library/gg398833.aspx

### 2.6.8 Connection Scaling

LoadMaster is a scalable load balancer, allowing for more than 64,000 client connections to a single Virtual Service at one time. If this is required, you should execute the Connection Scaling for Large Scale Deployments procedure located in the Appendix of this manual.

### 3 Hardware Load Balancing vs DNS Load Balancing for Lync Server 2010

Microsoft Lync Server 2010 supports two load balancing solutions: DNS load balancing and hardware load balancing. You can choose different load balancing solutions for each pool in your deployment.

#### 3.1 Hardware Load balancing

Hardware load balancing was the only supported way to deploy a high available Office Communications Server solution. The same functionality is available in Lync Server 2010. A hardware load balancer is used in an Enterprise pool that has more than one Enterprise Edition server. The load balancer performs the critical role of delivering scalability and high availability across multiple servers that are connected to a centralized database on the Lync Server Back-End Database.
3.2 DNS Load Balancing

DNS load balancing is introduced in Microsoft Lync Server 2010 communications software. The objective of DNS load balancing is to provide a native load balancing mechanism option in Lync Server 2010. A Hardware Load Balancer is still required for Load Balancing the Web traffic.

Domain Name System (DNS) load balancing uses DNS as a way to load-balance across multiple servers. DNS load balancing is implemented at the application level in both servers and clients. They both participate in the load-balancing logic.

Hardware Load Balancer is still required for Web traffic. Both HTTP and HTTPS are session-state–oriented protocols. With DNS load balancing, there is no sticky-session state that can be set up. As a result, there is no way to ensure that a session is going to be continued on the correct server. HLB specifically addresses this session problem by caching the client-server state information. For Web-based traffic DNS load balancing is not a solution.

DNS Load Balancing is not supported in all scenarios.

DNS load balancing supports automatic failover only for servers running Lync Server 2010 and Lync Server 2010 clients. Earlier versions of clients and Office Communications Server can still connect to pools running DNS load balancing, but if they cannot make a connection to the first server that DNS load balancing refers them to, they are unable to fail over to another server in the pool.

Additionally, if Exchange UM is used, only Exchange 2010 SP1 has built-in support for Lync Server 2010 DNS load balancing. If an earlier version of Exchange is used, failover capabilities for the following Exchange UM scenarios will not be available:

- Playing their Enterprise Voice mail on their phone
- Transferring calls from an Exchange UM Auto-Attendant

All other Exchange UM scenarios will work properly.

3.3 DNS Load Balancing matrix

<table>
<thead>
<tr>
<th>Situation</th>
<th>DNS load balancing supported?</th>
<th>DNS load balancing recommended?</th>
<th>Hardware load balancer (only) recommended?</th>
</tr>
</thead>
<tbody>
<tr>
<td>All or most users homed in the pool run Lync Server 2010 clients.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Many users homed in the pool still running older clients.</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Interoperates only with other servers running Lync Server 2010.</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Interoperates with many servers running earlier versions of Office Communications Server.</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Running Exchange UM with Exchange 2010 SP1 (or not running Exchange UM)</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>
DNS Load Balancing and Hardware Load Balancer setup for web traffic only is not included in this guide.
4 Network deployment Examples

4.1 Typical Deployment Option
4.2 Alternative Deployment Option:
One (pair of) Loadmaster(s) for load balancing all of the Internal Lync Servers (including the internal facing Lync Edge Server Interface) and one (pair of) Loadmaster(s) for load balancing all of the External facing interfaces for Lync Edge Servers.
4.3 Alternative Deployment Option:
One (pair of) Loadmaster(s) for load balancing all of the Internal Lync Servers and External Lync Edge Servers.

⚠️ This means that Internal and External traffic traverses the same Loadmaster unit, a denial of service could impact both the internal and external Lync Server deployment

![Diagram showing LoadMaster deployment for MS Lync 2010]
5  General Configuration

5.1  Disable Global SNAT

By default Global SNAT is enabled and must be disabled for one armed configurations. The only exception to this rule is for the External Audio & Video EDGE Server.

1. To use disable Global SNAT Control scaling, click **System Configuration**.
2. Click Miscellaneous Options.
3. Click SNAT Control
4. Uncheck “Enable SNAT”

5.2  Change Drop Connections settings

You must configure the Loadmaster to drop connections on Real Server Failure in order to have fast failover for clients to another Real Server.

1. To configure dropping connections, click **System Configuration**.
2. Click Miscellaneous Options.
3. Click L7 Configuration.
4. Configure **Drop Connections on RS failure** to **Yes**.

5.3  Increase the Connection Timeout

You must configure the Loadmaster Connection Timeout to one day. The reason why this value can be set this value so high is that the Loadmaster monitors client connection to real servers and if a server fails then the Loadmaster can drop the associated client connections to that real server. Clients are disconnected from the Loadmaster and then reconnect to the Loadmaster to connect to another Real Server.

One day is the maximum value for this setting and it must be used in conjunction with Drop Connections on Real Server failures.

1. To configure the Connection Timeout, click **System Configuration**.
2. Click Miscellaneous Options.
3. Click L7 Configuration.
4. Configure **L7 Connection Timeout (secs)** value to **86400** (1 day) and click **Set Time**.

5.4  Connection Scaling For Large Scale Deployments

Execution of this procedure is optional and should be used only in cases where you expect your network traffic to be greater than 64,000 server connections at any one particular time.

You must disable L7 Transparency in order to use connection scaling.
1. To use connection scaling, click **System Configuration**.
2. Click Miscellaneous Options.
3. Click L7 Configuration.
4. Use the Allow connection scaling over 64K Connections drop down list and select Yes.

| Allow connection scaling over 64K Connections | Yes | " |

5. Click Virtual Services.
6. Click View/Modify Services.
7. Click the **Modify** button of the appropriate (presumably just created) Virtual IP Address.
8. In the **Advanced Properties** panel, input a list of **Alternate Source Addresses**. Multiple IPV4 addresses must be separated with a space, each must be unallocated and allow 64K connections.
9. Click the Set Alternate Addresses button.
6 Load Balancing Lync Front-End servers

This section provides step by step instructions on how you configure the KEMP LoadMaster to load balance the various services of a Microsoft Lync 2010 Front-End pool.

Typical deployment type: One-armed Topology and Non-transparent (Microsoft SNAT)

6.1 Required Services for Front-End pools

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Protocol</th>
<th>Port</th>
<th>Virtual IP Address</th>
<th>Real Servers</th>
<th>Persistence</th>
<th>Scheduling</th>
<th>Non-Transparant (MS SNAT)</th>
<th>Layer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE DCOM</td>
<td>TCP</td>
<td>135</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>RPC / DCOM based operations</td>
</tr>
<tr>
<td>FE SIP</td>
<td>TCP</td>
<td>5061</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>SIP / TLS</td>
</tr>
<tr>
<td>FE App Share</td>
<td>TCP</td>
<td>5065</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Application Sharing</td>
</tr>
<tr>
<td>FE QoE</td>
<td>TCP</td>
<td>5069</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>QoE Agent</td>
</tr>
<tr>
<td>FE Conf</td>
<td>TCP</td>
<td>444</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Conferencing</td>
</tr>
<tr>
<td>FE Web Int</td>
<td>TCP</td>
<td>443</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>HTTPS Internal Web Services</td>
</tr>
<tr>
<td>FE Web Ext</td>
<td>TCP</td>
<td>4443</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Super HTTP (*)</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>HTTPS External Web Services</td>
</tr>
</tbody>
</table>

(*) Requires the installation of a valid, none self-signed and trusted certificate on the LoadMaster. Preferably issued by the same Certificate Authority as used by the Lync Servers.
6.2 Optional Services for Front-End pools

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Protocol</th>
<th>Port</th>
<th>Virtual Address IP</th>
<th>Real Servers IP</th>
<th>Persistence</th>
<th>Scheduling</th>
<th>SNAT Layer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE Web 80 TCP</td>
<td>80</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>HTTP Root Certificate Retrieval for Lync Phones</td>
</tr>
<tr>
<td>FE CAC TCP</td>
<td>448</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Call Admission Control</td>
</tr>
<tr>
<td>FE SIPU TCP</td>
<td>5060</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>SIP unsecured</td>
</tr>
<tr>
<td>FE MED TCP</td>
<td>5067</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Mediation Server SIP/TLS</td>
</tr>
<tr>
<td>FE MED TCP</td>
<td>5068</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Mediation Server SIP/TCP</td>
</tr>
<tr>
<td>FE MED TCP</td>
<td>6070</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Mediation Server FE</td>
</tr>
<tr>
<td>FE RSG TCP</td>
<td>6071</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Response Groups</td>
</tr>
<tr>
<td>FE CAA TCP</td>
<td>6072</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Conferencing Attendant</td>
</tr>
<tr>
<td>FE CA TCP</td>
<td>6073</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Conferencing Announcement</td>
</tr>
<tr>
<td>FE OV TCP</td>
<td>6074</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>Outside Voice Control</td>
</tr>
<tr>
<td>FE TCP</td>
<td>6075</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td></td>
</tr>
<tr>
<td>FE TCP</td>
<td>6076</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td></td>
</tr>
<tr>
<td>FE TCP</td>
<td>6080</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td></td>
</tr>
<tr>
<td>FE Web 8080 TCP</td>
<td>8080</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>HTTP Root Certificate Retrieval for Lync Phones</td>
</tr>
</tbody>
</table>

6.3 Configuring a Virtual Service for SIP services on the Lync Front-End servers.

1. Connect and log in to your LoadMaster.
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address of the Lync Server Front-End Pool using the format ###.###.###.### (10.84.10.33).
4. Enter 5061 as the Port.
5. Select tcp as the Protocol.
   
   The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.
6. Click Add this Virtual Service.
7. Select the Force L7 check box.
8. Unselect the L7 Transparency check box.

9. Select TCP Connect Only in Real Server Check Parameters, type 5061 in Check Port. Click Set Checked Port.

10. Enter a Service Nickname. This is for display purposes only. For example, “FE SIP”. Click Set Name.

11. For Persistence Options, select Source IP as the Mode. Use the Timeout drop down list to select 20 minutes and the Netmask drop down list to select/32.

12. Select Least Connection as the Scheduling Method.

13. For Idle Timeout enter 1800 (30 minutes). Click Set Idle Timeout.

14. Add Real Servers. Click Add New…

15. For each Front-End server, input its IP address (10.84.10.14 & 10.84.10.13) as the Real Server Address on Port 5061. Click Add This Real Server.

16. Click OK in response to the confirmation that the Real Server was added.

6.4 Configuring a Virtual Services for Additional services on the Lync Front-End servers.

Additional Services need to be configured for at least the following ports 135 (RPC), 444 (Conferencing), 5065 (Application Sharing) and 5069 (QoE Agent)

⚠️ Potentially other ports are required; review all the ports in the following table: Optional Services for Front-End pools and add an Additional Service as required.

Configure the Additional Services for the Front-End Servers according to Section 5.3 (Configuring a Virtual Service for SIP services on the Lync Front-End servers).

You only have to replace the values in Step 4 (Port configuration), Step 9 (Checked Port configuration), Step 10 (Service Nickname) and Step 15 (Port on Real Server) according to the following table:

<table>
<thead>
<tr>
<th>Service</th>
<th>Step 4 (Port)</th>
<th>Step 9 (Checked Port)</th>
<th>Step 10 (Service Name)</th>
<th>Step 15 (Port)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE RPC</td>
<td>135</td>
<td>5061</td>
<td>FE RPC</td>
<td>135</td>
<td>Port checking on port 135 does not work as this is a Windows RPC Port and always returns alive also when Lync is not running so checking on a Lync port is required 5061 in this case.</td>
</tr>
<tr>
<td>FE Conf</td>
<td>444</td>
<td>444</td>
<td>FE Conf</td>
<td>444</td>
<td></td>
</tr>
<tr>
<td>FE App Share</td>
<td>5065</td>
<td>5065</td>
<td>FE App Share</td>
<td>5065</td>
<td></td>
</tr>
<tr>
<td>FE QoE</td>
<td>5069</td>
<td>5069</td>
<td>FE QoE</td>
<td>5069</td>
<td></td>
</tr>
</tbody>
</table>

6.5 Configuring a Virtual Service for Internal HTTPS-based services for the Front-End servers.

1. Connect and log in to your LoadMaster.

2. Create a Virtual Service. Click Virtual Services and then click Add New.

3. Enter the Virtual Address of the Lync Server Internal Base Webservices URL using the format ###.#####.#### (10.84.10.33).
4. Enter 443 as the Port.
5. Select tcp as the Protocol.

⚠️ The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.

6. Click Add this Virtual Service.
7. Select the Force L7 check box.
8. Unselect the L7 Transparency check box.
9. Select HTTPS Protocol in Real Server Check Parameters, type 443 in Checked Port. Click Set Checked Port. Enter /abs/handler in URL and click Set URL.
10. Enter a Service Nickname. This is for display purposes only. For example, “FE WEB INT”. Click Set Nickname.
11. For Persistence Options, select Source IP as the Mode. Use the Timeout drop down list to select 20 minutes and the Netmask drop down list to select/32.
12. Select Least Connection as the Scheduling Method.
13. For Idle Timeout enter 1800 (30 minutes). Click Set Idle Timeout.
14. Add Real Servers. Click Add New...
15. For each Front-End server, input its IP address (10.84.10.14 & 10.84.10.13) as the Real Server Address on Port 443. Click Add This Real Server.
16. Click OK in response to the confirmation that the Real Server was added.

6.6 Configuring a Virtual Service for External HTTPS-based services for the Front-End servers.
1. Connect and log in to your LoadMaster.
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address of the Lync Server External Base Webservices URL using the format ###.###.###.### (10.84.10.33).
4. Enter 4443 as the Port.
5. Select tcp as the Protocol.

⚠️ The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.

6. Click Add this Virtual Service.
7. Select the Force L7 check box.
8. Unselect the L7 Transparency check box.
9. Select HTTPS Protocol in Real Server Check Parameters, type 4443 in Checked Port. Click Set Checked Port. Enter /abs/handler in URL and click Set URL.
10. Enter a Service Nickname. This is for display purposes only. For example, “FE WEB EXT”. Click Set Nickname.
11. For Persistence Options, select Super HTTP as the Mode. Use the Timeout drop down list to select 20 minutes and the Netmask drop down list to select/32.
12. Select **Least Connection** as the Scheduling Method.
13. For **Idle Timeout** enter 1800 (30 minutes). Click **Set Idle Timeout**.
14. Click **Enable** for **SSL Acceleration**.
15. Select the **Reencrypt** option and Click **OK** to close the certificate warning about the self-signed certificate popup.

⚠️ *Reencryption is required. SSL Offloading is not supported for Lync Web Services.*

16. Click **Add New** to import the exported certificate with private key (can be the same certificate as installed on the Front-End Server)
17. Click **Browse** for the IIS Certificate and select the exported certificate in .PFX format that includes the private key. Enter the **Pass Phrase** which is the password you configured in the .PFX file when exporting the certificate.
18. Add Real Servers. Click **Add New**...
19. For each Front-End server, input its IP address (10.84.10.14 & 10.84.10.13) as the **Real Server Address** on **Port** 4443. Click **Add This Real Server**.
20. Click **OK** in response to the confirmation that the Real Server was added.
21. You have now completed your configuration of LoadMaster for Lync 2010 Internal Web Services. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

7 **Load Balancing Lync Director servers**

This section provides step by step instructions on how you configure the KEMP LoadMaster to load balance the various services of a Microsoft Lync 2010 Director pool.

Typical Deployment Type: One-armed Topology and None transparent (Microsoft SNAT)

### 7.1 Required Services for Director pools

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Protocol</th>
<th>Port</th>
<th>Virtual Address</th>
<th>IP</th>
<th>Real Servers</th>
<th>Persistence</th>
<th>Scheduling</th>
<th>SNAT</th>
<th>Layer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIR SIP</td>
<td>TCP</td>
<td>5061</td>
<td>Pool IP</td>
<td>IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>SIP/TLS</td>
</tr>
<tr>
<td>DIR SIPU</td>
<td>TCP</td>
<td>5060</td>
<td>Pool IP</td>
<td>IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>SIP Unsecured</td>
</tr>
</tbody>
</table>

---
7.2 Configuring a Virtual Service for SIP services on the Director servers.

1. Connect and log in to your LoadMaster.
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address of the Lync Server Director Pool using the format ###.###.###.### (10.84.10.34).
4. Enter 5061 as the Port.
5. Select tcp as the Protocol.

   The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.

6. Click Add this Virtual Service.
7. Enter 5060 in the Extra Ports configuration and click Set Extra Ports
8. Select the Force L7 check box.
9. Unselect the L7 Transparency check box.
10. Select TCP Connect Only in Real Server Check Parameters, type 5061 in Checked Port.
    Click Set Checked Port.
11. Enter a Service Nickname. This is for display purposes only. For example, “DIR SIP”. Click Set Nickname.
12. For Persistence Options, select Source IP Address as the Mode. Use the Timeout drop down list to select 20 minutes and the Netmask drop down list to select/32.
13. Select Least Connection as the Scheduling Method.
14. For Idle Timeout enter 1800 (30 minutes). Click Set Idle Timeout.
15. Add Real Servers. Click Add New...
16. For each Front-End server, input its IP address (10.84.10.17 & 10.84.10.16) as the Real Server Address on Port 5061. Click Add This Real Server.

17. Click OK in response to the confirmation that the Real Server was added.

18. You have now completed your configuration of LoadMaster for Lync 2010 Front-End server. If you wish to view, modify, or delete any Real Servers that have been added, click View/Modify Services.
8 Load balancing internal Lync Edge servers

This section provides step by step instructions on how you configure the KEMP LoadMaster to load balance the various services of a Microsoft Lync 2010 Edge pool.

Typical Deployment Type:

- One-armed Topology and None transparent (Microsoft SNAT)
- (Optional) One or Two-armed Transparency using a Layer 4 Service

8.1 Required Services for Edge pools facing internally

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Protocol</th>
<th>Port</th>
<th>Virtual Address</th>
<th>IP</th>
<th>Real Servers</th>
<th>Persistence</th>
<th>Scheduling</th>
<th>SNAT</th>
<th>Layer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDI SIP</td>
<td>TCP</td>
<td>5061</td>
<td>Pool IP</td>
<td></td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>SIP/TLS</td>
</tr>
<tr>
<td>EDI Auth</td>
<td>TCP</td>
<td>5062</td>
<td>Pool IP</td>
<td></td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>A/V Authentication</td>
</tr>
<tr>
<td>EDI http</td>
<td>TCP</td>
<td>443</td>
<td>Pool IP</td>
<td></td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L7</td>
<td>TCP Audio, Video, Sharing &amp; Files</td>
</tr>
<tr>
<td>EDI Conf</td>
<td>UDP</td>
<td>3478</td>
<td>Pool IP</td>
<td></td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>Yes</td>
<td>L4</td>
<td>Audio/Video</td>
</tr>
</tbody>
</table>

Lync EDGE Pool internal FQDN in DNS points to 10.84.10.97 (KEMP LoadMaster)

Edge Server 1
IP Address: 10.84.10.11
Subnet: 255.255.0.0
Default Gateway: 10.84.10.1

Edge Server 2
IP Address: 10.84.10.12
Subnet: 255.255.0.0
Default Gateway: 10.84.10.1
8.2 Configuring a Virtual Service for SIP services on the Internal EDGE servers.

1. Connect and log in to your LoadMaster.
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address of the Internal Lync Server EDGE Pool using the format ###.###.###.### (10.84.10.97).
4. Enter 5061 as the Port.
5. Select tcp as the Protocol.

![The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.]
6. Click Add this Virtual Service.
7. Select the Force L7 check box.
8. Unselect the L7 Transparency check box.
9. Select TCP Connect Only in Real Server Check Parameters, type 5061 in Checked Port. Click Set Checked Port.
10. Enter a Service Nickname. This is for display purposes only. For example, “EDI SIP”. Click Set Nickname.
11. For Persistence Options, select Source IP Address as the Mode. Use the Timeout drop down list to select 20 minutes and the Netmask drop down list to select/32.
12. Select Least Connection as the Scheduling Method.
13. For Idle Timeout enter 1800 (30 minutes). Click Set Idle Timeout.
14. Add Real Servers. Click Add New...
15. For each Front-End server, input its IP address (10.84.10.11 & 10.84.10.12) as the Real Server Address on Port 5061. Click Add This Real Server.
16. Click OK in response to the confirmation that the Real Server was added.

8.3 Configuring a Virtual Services for Additional services on the Lync Internal Edge servers.

Additional Services need to be configured for at least the following ports 443 (TCP Media) and 5062 (Authentication).

Configure the Additional Services for the Internal Edge Servers according to Section 7.2 (Configuring a Virtual Service for SIP services on the Internal EDGE servers.).

You only have to replace the values in Step 4 (Port configuration), Step 9 (Checked Port configuration), Step 10 (Service Nickname) and Step 15 (Port on Real Server) according to the following table:
8.4 Configuring a Virtual Service for Audio & Video services on the Internal EDGE servers.

1. Connect and log in to your LoadMaster.
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address of the Internal Lync Server EDGE Pool using the format ###.###.###.### (10.84.10.97).
4. Enter 3478 as the Port.
5. Select udp as the Protocol.
   *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click Add this Virtual Service.
7. Enter a Service Nickname. This is for display purposes only. For example, “EDI AV”. Click Set Nickname.
8. For Persistence Options, select Source IP Address as the Mode. Use the Timeout drop down list to select 30 minutes and the Netmask drop down list to select /32.
9. Select Least Connection as the Scheduling Method.
10. Add Real Servers. Click Add New...
11. For each Front-End server, input its IP address (10.84.10.11 & 10.84.10.12) as the Real Server Address on Port 3478. Click Add This Real Server.
12. Click OK in response to the confirmation that the Real Server was added.
13. You have now completed your configuration of LoadMaster for Lync 2010 Internal EDGE server. If you wish to view, modify, or delete any Real Servers that have been added, click View/Modify Services.
9 Load balancing external Lync Edge servers

This section provides step by step instructions on how you configure the KEMP LoadMaster to load balance the various services of a Microsoft Lync 2010 Edge pool.

Typical Deployment Type: One or Two-armed Transparent using a Layer 4 Service

9.1 Required Services for Edge pools facing externally

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Protocol</th>
<th>Port</th>
<th>Virtual IP Address</th>
<th>Real Server IPs</th>
<th>Persistence</th>
<th>Scheduling</th>
<th>SNAT</th>
<th>Layer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDE Access SIP</td>
<td>TCP</td>
<td>5061</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>No</td>
<td>L7</td>
<td>SIP/TLS</td>
</tr>
<tr>
<td>EDE Access Remote</td>
<td>TCP</td>
<td>443</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>No</td>
<td>L7</td>
<td>Remote Users</td>
</tr>
<tr>
<td>EDE Conf</td>
<td>TCP</td>
<td>443</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>No</td>
<td>L7</td>
<td>Conferencing</td>
</tr>
<tr>
<td>EDE AV TCP</td>
<td>TCP</td>
<td>443</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>No</td>
<td>L7</td>
<td>Fallback port TCP Audio, Video, Sharing &amp; Files</td>
</tr>
<tr>
<td>EDI AV UDP</td>
<td>UDP</td>
<td>3478</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>No</td>
<td>L4</td>
<td>Audio/Video</td>
</tr>
</tbody>
</table>

9.2 Optional Services for Edge pools facing externally

Pool IP = Enterprise Front-End Pool FQDN IP Address
Server IPs = IP Addresses of Front-End Servers

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Protocol</th>
<th>Port</th>
<th>Virtual IP Address</th>
<th>Real Server IPs</th>
<th>Persistence</th>
<th>Scheduling</th>
<th>SNAT</th>
<th>Layer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDE AV TCP High</td>
<td>TCP</td>
<td>50.000 – 59.999</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>No</td>
<td>L7</td>
<td>Fallback port Audio/Video High port Range. Desktop Sharing / CWA</td>
</tr>
<tr>
<td>EDI AV UDP High</td>
<td>UDP</td>
<td>50.000 – 59.999</td>
<td>Pool IP</td>
<td>Server IPs</td>
<td>Source IP</td>
<td>Least Connection</td>
<td>No</td>
<td>L4</td>
<td>Audio/Video High port Range. Federation/Remot e Users</td>
</tr>
</tbody>
</table>
9.3 Configuring a Virtual Service for SIP services on the External EDGE servers.

1. Connect and log in to your LoadMaster.
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address of the External Lync Server Access EDGE Pool using the format ###.###.###.### (172.16.84.97).
4. Enter 5061 as the Port.
5. Select tcp as the Protocol.

   The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.

6. Click Add this Virtual Service.
7. Select the Force L7 check box.
8. Unselect the L7 Transparency check box.
9. Select TCP Connect Only in Real Server Check Parameters, type 5061 in Checked Port. Click Set Checked Port.
10. Enter a Service Nickname. This is for display purposes only. For example, “EDE SIP”. Click Set Nickname.
11. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **20 minutes** and the **Netmask** drop down list to select/32.

12. Select **Least Connection** as the **Scheduling Method**.

13. For **Idle Timeout** enter **1800** (30 minutes). Click **Set Idle Timeout**.

14. Add Real Servers. Click **Add New**...

15. For each Front-End server, input its IP address (172.16.84.11& 172.16.84.12) as the **Real Server Address** on **Port** 5061. Click **Add This Real Server**.

16. Click **OK** in response to the confirmation that the Real Server was added.

---

### 9.4 Configuring a Virtual Service for Remote User services on the External EDGE servers.

1. Connect and log in to your LoadMaster.

2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.

3. Enter the **Virtual Address** of the External Lync Server Access EDGE Pool using the format ###.###.###.### (172.16.84.97).

4. Enter **443** as the **Port**.

5. Select **tcp** as the **Protocol**.

   - *Tip: The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*

6. Click **Add this Virtual Service**.

7. Select the **Force L7** check box.

8. Unselect the **L7 Transparency** check box.

9. Select **TCP Connect Only** in Real Server Check Parameters, type **443** in Checked Port. Click **Set Checked Port**.

10. Enter a **Service Nickname**. This is for display purposes only. For example, “EDE Remote”. Click **Set Nickname**.

11. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **20 minutes** and the **Netmask** drop down list to select/32.

12. Select **Least Connection** as the **Scheduling Method**.

13. For **Idle Timeout** enter **1800** (30 minutes). Click **Set Idle Timeout**.

14. Add Real Servers. Click **Add New**...

15. For each Front-End server, input its IP address (172.16.84.11& 172.16.84.12) as the **Real Server Address** on **Port** 443. Click **Add This Real Server**.

16. Click **OK** in response to the confirmation that the Real Server was added.
9.5 Configuring a Virtual Service for Conferencing services on the External EDGE servers.

1. Connect and log in to your LoadMaster.
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address of the External Lync Server Conferencing EDGE Pool using the format ###.###.###.### (172.16.84.98).
4. Enter 443 as the Port.
5. Select tcp as the Protocol.
   
   The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.
6. Click Add this Virtual Service.
7. Select the Force L7 check box.
8. Unselect the L7 Transparency check box.
9. Select TCP Connect Only in Real Server Check Parameters, type 443 in Checked Port. Click Set Checked Port.
10. Enter a Service Nickname. This is for display purposes only. For example, “EDE Conf”. Click Set Nickname.
11. For Persistence Options, select Source IP Address as the Mode. Use the Timeout drop down list to select 20 minutes and the Netmask drop down list to select /32.
12. Select Least Connection as the Scheduling Method.
13. For Idle Timeout enter 1800 (30 minutes). Click Set Idle Timeout.
14. Add Real Servers. Click Add New...
15. For each Front-End server, input its IP address (172.16.84.21 & 172.16.84.22) as the Real Server Address on Port 443. Click Add This Real Server.
16. Click OK in response to the confirmation that the Real Server was added.

9.6 Configuring a Virtual Service for TCP Audio/Video services on the External EDGE servers.

1. Connect and log in to your LoadMaster.
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address of the External Lync Server Conferencing EDGE Pool using the format ###.###.###.### (172.16.84.99).
4. Enter 443 as the Port.
5. Select tcp as the Protocol.
   
   The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.
6. Click Add this Virtual Service.
7. Select the Force L7 check box.
8. Leave the L7 Transparency check box enabled.
9. Select **TCP Connect Only** in Real Server Check Parameters, type **443** in Checked Port. Click **Set Checked Port**.

10. Enter a **Service Nickname**. This is for display purposes only. For example, “EDE TCP AV”. Click **Set Nickname**.

11. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **20 minutes** and the **Netmask** drop down list to select **/32**.

12. Select **Least Connection** as the **Scheduling Method**.

13. For **Idle Timeout** enter **1800** (30 minutes). Click **Set Idle Timeout**.

14. Select the **Use Address for SNAT** checkbox.

This is a requirement for the External Audio/Video EDGE server only

15. Add Real Servers. Click **Add New**…

16. For each Front-End server, input its IP address (172.16.84.31& 172.16.84.32) as the **Real Server Address** on **Port 443**. Click **Add This Real Server**.

17. Click **OK** in response to the confirmation that the Real Server was added.

9.7 **Configuring a Virtual Service for UDP Audio/Video services on the External EDGE servers.**

1. Connect and log in to your LoadMaster.

2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.

3. Enter the **Virtual Address** of the External Lync Server Conferencing EDGE Pool using the format ###.###.###.### (172.16.84.99).

4. Enter **3478** as the **Port**.

5. Select **udp** as the **Protocol**.

This is a requirement for the External Audio/Video EDGE server only

6. Click **Add this Virtual Service**.

7. Enter a **Service Nickname**. This is for display purposes only. For example, “EDE UDP AV”. Click **Set Nickname**.

8. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **20 minutes** and the **Netmask** drop down list to select **/32**.

9. Select **Least Connection** as the **Scheduling Method**.

10. Select the **Use Address for SNAT** checkbox.

This is a requirement for the External Audio/Video EDGE server only

11. Add Real Servers. Click **Add New**…

12. For each Front-End server, input its IP address (172.16.84.31& 172.16.84.32) as the **Real Server Address** on **Port 3478**. Click **Add This Real Server**.

13. Click **OK** in response to the confirmation that the Real Server was added.
14. You have now completed your configuration of LoadMaster for Lync 2010 External EDGE server. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.
# 10 Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov-11</td>
<td>First draft</td>
<td></td>
<td>JD</td>
</tr>
<tr>
<td>Jan-12</td>
<td>Persist handling edits</td>
<td>consistency</td>
<td>JB</td>
</tr>
</tbody>
</table>