



# ロードマスター

## クイック・スタート・ ガイド

ドキュメントバージョン 1.0  
ファームリリース 7.0-10

発行 : 2014 年 1 月 29 日

World Headquarters:  
KEMP Technologies, Inc.  
12 Old Dock Road  
Yaphank , NY 11980  
U.S.A.  
+1 (631) 345 5292

EMEA Headquarters:  
KEMP Technologies Ltd.  
Mary Rosse Centre  
Holland Road, National Tech.  
Park  
Limerick, Ireland  
+353 (61) 260 101



1	初期設定を行うには.....	4
2	ネットワークの考慮点.....	4
2.1	1アーム (One-Armed) トポロジー.....	4
2.2	2アーム (Two-Armed ) トポロジー.....	5
2.3	リアルサーバのデフォルトゲートウェイ.....	6
2.4	IPアドレスの管理.....	6
3	初期設定のためのロードマスターへの接続.....	8
3.1	シリアルポートよりターミナル・エミュレータを使用する場合.....	8
3.2	VGA モニターと USB 用キーボードを装置に直接接続する場合.....	8
3.3	PC (パソコン) よりブラウザを使用する場合.....	11
3.4	ライセンスの取得.....	12
3.4.1	オンラインでの取得.....	12
3.4.2	オフラインでの取得.....	16
3.5	HA 設定 : HA-2 セットアップ.....	19
3.6	仮ライセンスの永久ライセンスへの更新.....	21
3.6.1	アプライアンスの場合.....	21
3.6.2	VLM の場合.....	22
4	ウェブユーザインターフェース (WUI).....	23
4.1	初めての接続.....	23
4.2	仮想仮想サービスとリアルサーバの概念.....	25
4.2.1	仮想仮想サービス.....	25
4.2.2	リアルサーバ.....	26
4.2.3	ネットワークでのパケットの流れ.....	27
4.3	仮想仮想サービス作成.....	30
4.3.1	仮想仮想サービスの作成.....	30
4.3.2	リアルサーバの設定.....	37
4.3.3	仮想仮想サービスの状態確認.....	38
4.3.4	仮想仮想サービス/リアルサーバへのアクセス.....	38
5	透過、それとも非透過モード.....	39
5.1	ネットワーク構成.....	39
5.2	透過モードの要求.....	40
5.2.1	ネットワーク透過、SNAT、1アームネットワーク.....	41
5.2.2	非透過モード.....	42
6	ネットワーク透過設定.....	43
6.1.1	ネットワーク透過.....	43
6.1.2	非透過モード.....	46

---

## 1 初期設定を行うには

---

初期設定を実施するには下記の3つの方法があります。

- VGA モニターと USB キーボードを直接装置へ接続し、コンソール画面より行う。
- PC (パソコン) を装置のシリアルポートに接続し、VT-100 ターミナルエミュレーターを使用してコンソール画面より行う。
- ブラウザーより装置のデフォルト IP アドレス “192.168.1.101” に HTTPS 接続をして、ウェブユーザインターフェースを介して行う。  
もしくは、SSH クライアントより接続してコンソール画面より行う。  
この場合は、“192.168.1.0/24” のサブネットが必要です。

---

## 2 ネットワークの考慮点

---

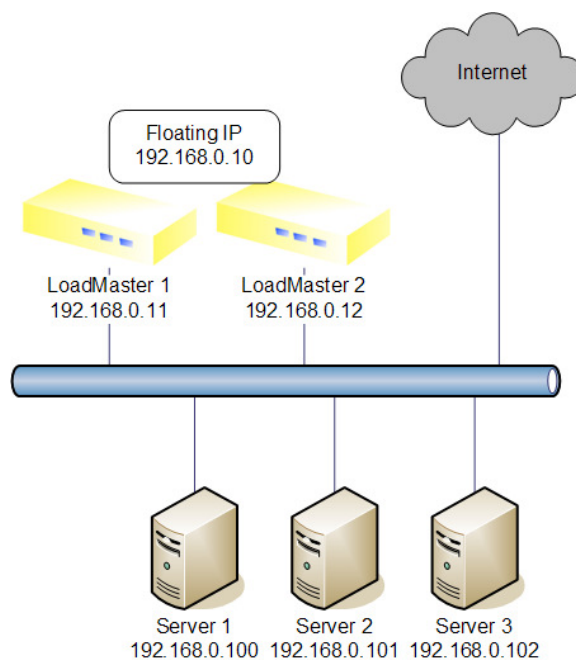
ロードマスターをインストールする前に、どのようにロードマスターをネットワークに接続するのかを考慮する必要があります。一般的に、ロードマスターを既存のネットワークに接続する形態として1アームと2アームの2つの形態があります。

### 2.1 1アーム (One-Armed) トポロジー

このネットワーク形態は、下記の場合に採用されます。

- ほとんどのユーザがロードマスターとアプリ用サーバが接続されているネットワーク外に存在する。
- アプリ用サーバからインターネット接続時に S-NAT の必要がない。
- ダイレクトサーバリターン (DSR) を利用する必要がある。
- 仮想仮想サービスとアプリ用サーバが同じネットワーク内に存在する。

この形態は、ひとつのイーサポートが受信/送信の両方のトラフィックのために使用されます。



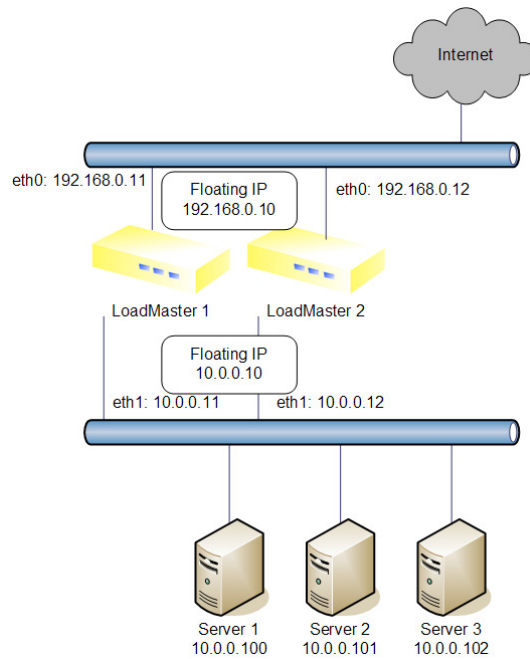
図— 1 : 1 アーム HA 構成図

注意：冗長構成（HA）の場合は、必ず、ロードマスターのイーサポート 1 同士をストレート、もしくはクロスケーブルで接続します。相手の稼動状態を監視するためのバックアップポートとして使用されます。

## 2.2 2アーム (Two-Armed) トポロジー

このネットワーク形態は、下記の場合に採用されます。

- ほとんどのユーザが、ロードマスターとアプリ用サーバが接続されているネットワーク内に存在する。
- アプリ用サーバからインターネット接続時に S-NAT を必要とする。
- この形態は、1つのイーサポートがネットワーク側に接続され、もう1つのイーサポートがアプリサーバ群を接続するために使用されます。



図— 2 : 2 アーム HA 構成図

## 2.3 リアルサーバのデフォルトゲートウェイ

もう1つの大事な考慮点は、ロードマスターをネットワークに接続する場合のリアルサーバ (RS) のデフォルトゲートウェイの設定です。2アーム形態でロードマスターを設置する場合、リアルサーバはロードマスターをデフォルトゲートウェイとして設定します。しかし、1アーム形態の場合、クライアントのIPアドレスをサーバのアクセスログに記録するかどうかで、設定が変わってきます。もし、クライアントのIPアドレスをアクセスログに記録する場合は、仮想仮想サービス (VS) を透過モード (ネットワーク・トランスペアレンシー) にし、リアルサーバのデフォルトゲートウェイをロードマスターに設定する必要があります。

クライアントのIPアドレスをアクセスログへ記録する必要がなければ、非透過モードとし、デフォルトゲートウェイの設定を変更する必要はありません。

詳細は、この“クイック・スタート・ガイド”の第7章を参照してください。

## 2.4 IP アドレスの管理

ロードマスターを単一構成 (非 HA) で設置する場合は、使用する各イーサポートに1つの特定IPアドレスが必要です。

2台のロードマスターを冗長構成 (HA) で設置する場合は、3つ (2アームの場合は6つ) の特定IPアドレスが必要になります。それぞれのロードマスターのイーサポートに割り当てるIPアドレスが2つ、両方のロードマスターで共用するシェアIPアドレスが1つです。これらのIPアドレスは、ロードマスターを管理するためのもので、その他に、仮想仮想サービス用 (クラスター、もしくはVIP) のIPアドレスが必要です。仮想仮想サービス用IPアドレスは、初期設定が終了した後、各仮想仮想サービスを作成するときに指定します。

冗長構成で設置し、リアルサーバのデフォルトゲートウェイとして、ロードマスターを指定しなければならぬ時は、リアルサーバが接続されているイーサポートのシェアIPアドレスを指定し

てください。

次の表 1 と表 2 は、2アーム形態の単一構成、冗長構成でのそれぞれの各イーサポートに割り当てる IP アドレスの例を示しています。

ネットワーク側 (eth0) が "192.168.0.0/24" のサブネットで、ファーム側 (eth1) が "10.0.0.0/8" のサブネットの例です。

ネットワークセグメント	インターフェース	サブネット	IP アドレス
Network side	eth0	192.168.0.0/24	192.168.0.10
Farm side	eth1	10.0.0.0/24	10.0.0.10

表 1: 単一構成の IP アドレス例

ネットワークセグメント	インターフェース	サブネット	IP アドレス
Network side	eth0	192.168.0.0/24	シェア: 192.168.0.10 HA-1: 192.168.0.11 HA-2: 192.168.0.12
Farm side	eth1	10.0.0.0/8	シェア: 10.0.0.10 HA-1: 10.0.0.11 HA-2: 10.0.0.12

表 2: 冗長構成の IP アドレス例

繰り返しますが、シェア IP アドレスはロードマスターの管理専用の IP アドレスです (ネットワーク形態、もしくは透過モードによっては、リアルサーバのデフォルトゲートウェイの IP アドレスとして使用されます)。仮想仮想サービス (クラスター、VIP) 用の IP アドレスは、仮想仮想サービスを作成するときに指定します。

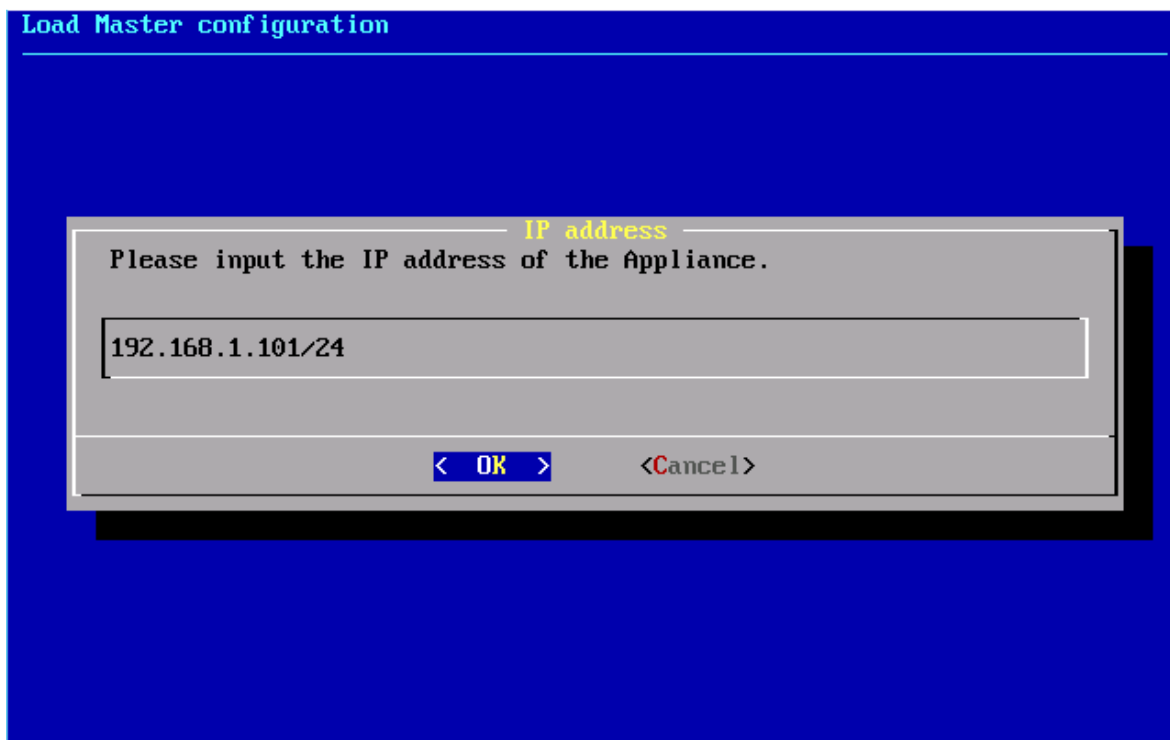
## 3 初期設定のためのロードマスターへの接続

初期設定を行うために、ロードマスターは次の3つの方法を提供しています。

- ・ シリアルポートよりターミナル・エミュレータを使用する場合
- ・ VGA モニターと USB 用キーボードを装置に直接接続する場合
- ・ PC (パソコン) よりブラウザを使用する場合

### 3.1 シリアルポートよりターミナル・エミュレータを使用する場合

コンピューター (パソコン) とロードマスターのCOMポートを、付属のシリアルケーブル (Null) で接続して、ターミナル・エミュレータから設定を行います。ターミナル・エミュレータは、WindowsのHyperターミナルやFreewareの“Tera Term Pro”などを使用し、通信速度115,200 bps、8ビットデータ長、パリティなし、ストップビット1で設定を行ってください。システムが正しく起動するとログイン画面が表示されますので、ユーザ名 ‘bal’、パスワード ‘1fourall’ と入力します。入力が正しいと、下記のようにEth0ポートのIPアドレスの設定画面が表示されますので、次項の“3.2 VGAモニターとUSB用キーボードを装置に直接接続する場合”を参照して設定を終了させて下さい。



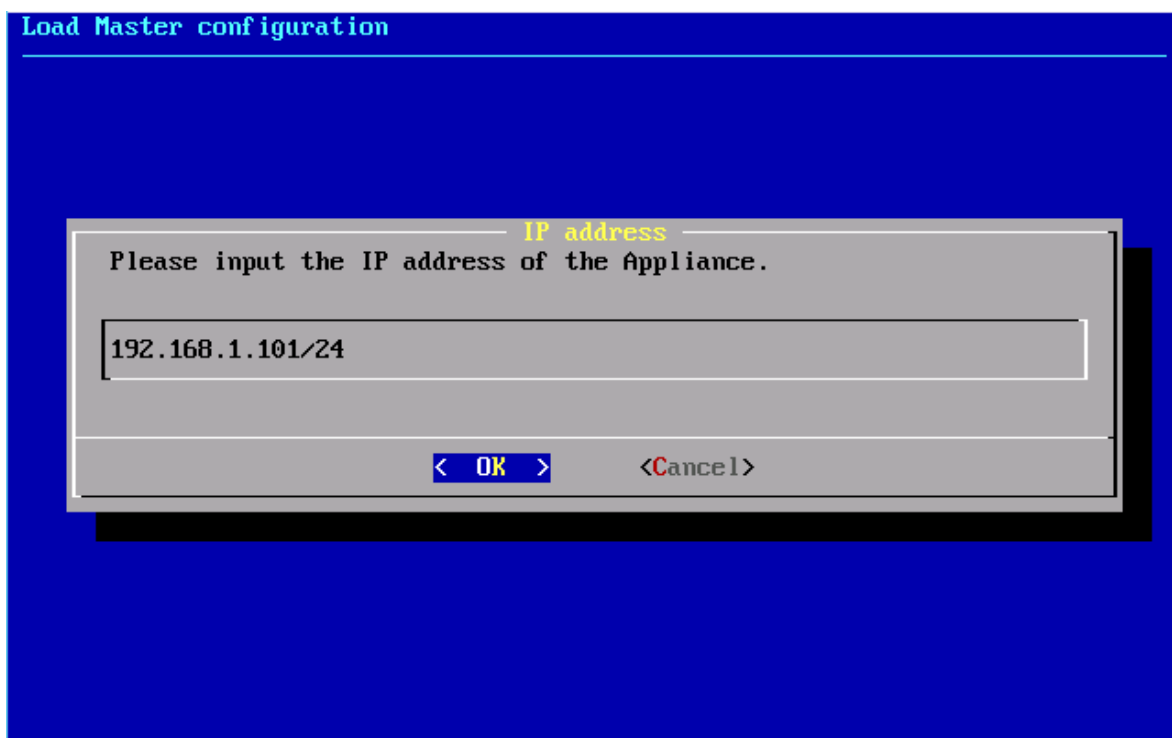
### 3.2 VGA モニターと USB 用キーボードを装置に直接接続する場合

ロードマスターと通信を行うために、VGAモニターとUSBキーボードを用意します。それらを装置の各ポートに接続します。装置が正しく起動すると、ログイン画面が表示されますので、ユーザ名 ‘bal’、パスワード ‘1fourall’ と入力します。

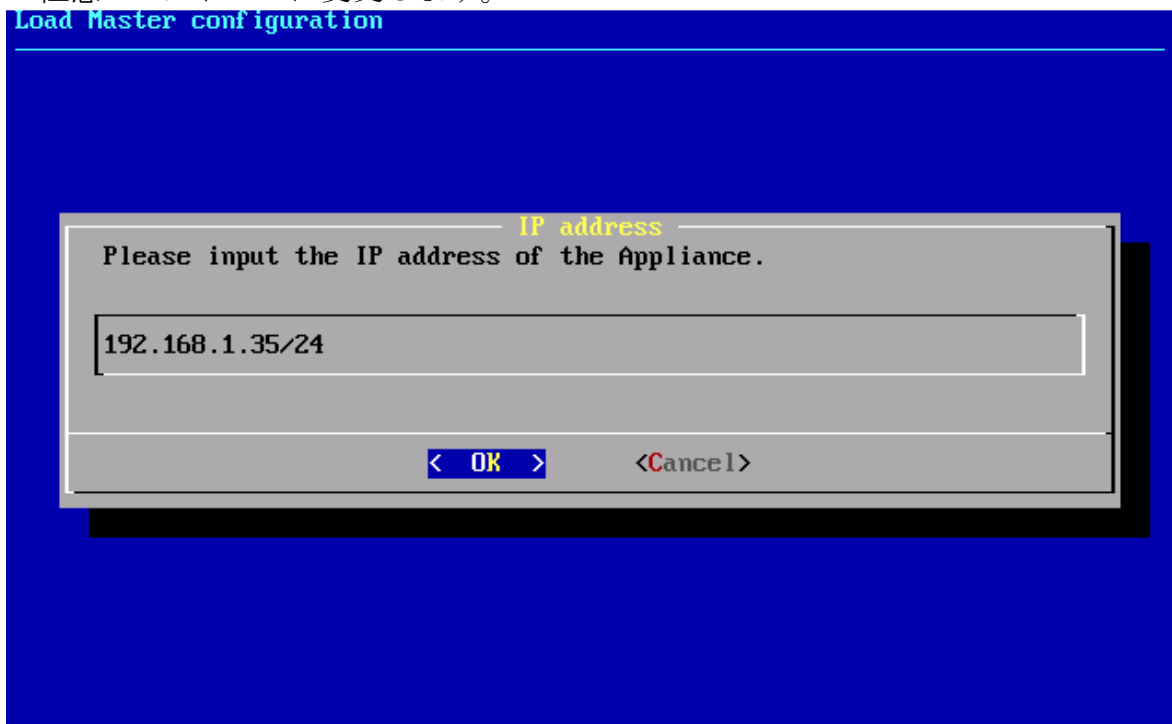
1. 入力が正しいと、下記のようにEth0ポートのIPアドレスの設定画面が表示されます。



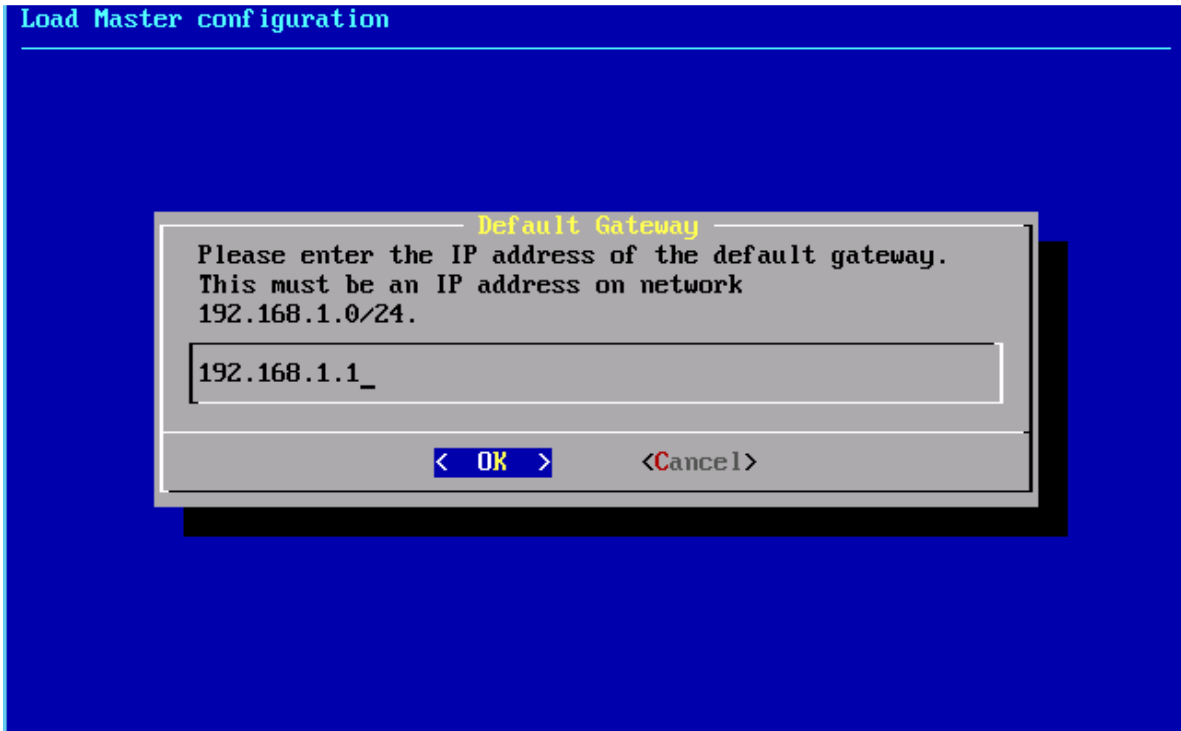
デフォルトの '192.168.1.101' が設定されています。



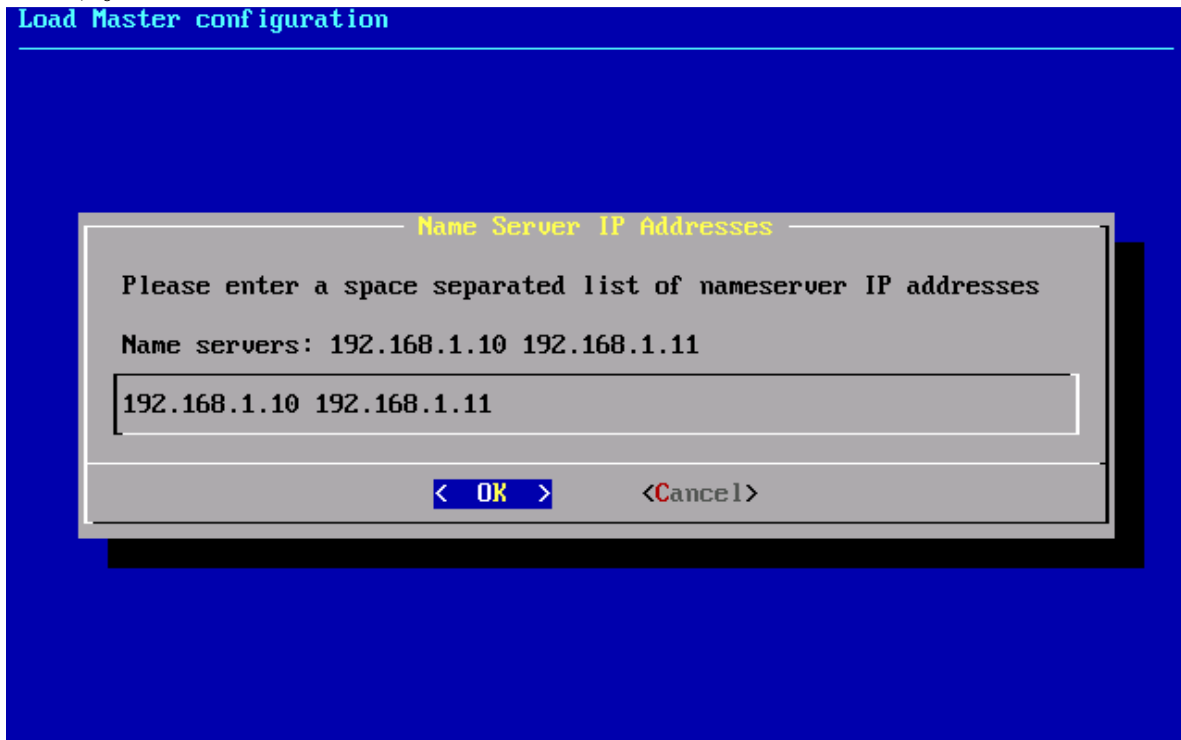
2. 任意のIPアドレスに変更します。



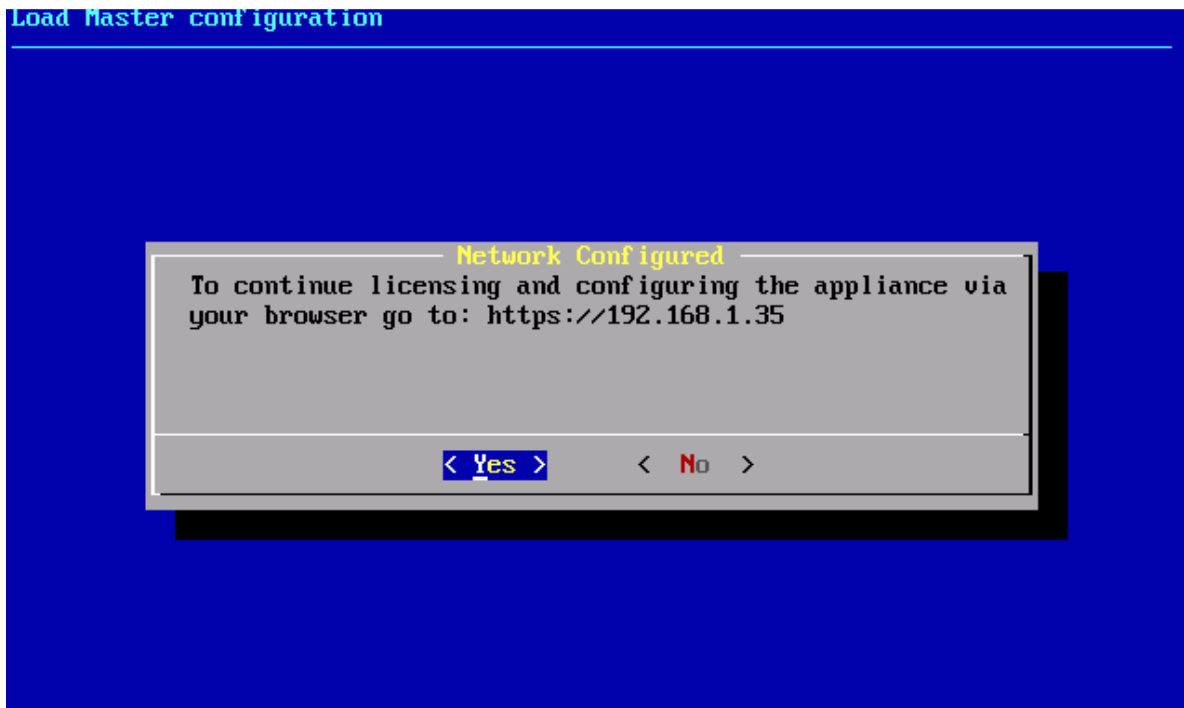
3. 現状のDefault Gateway設定が表示されますので任意のIPアドレスへ変更します。



4. Name Server IP Addressの画面が表示されますので、任意のDNSサーバーのIPアドレスを入力します。



5. これ以降の設定はWUIから行なうようにいう指示が表示されますので、<Yes>を選択してEnterキーを押します。次項の“3.3 PC (パソコン) よりブラウザーを使用する場合”を参考にして設定を終了させて下さい。

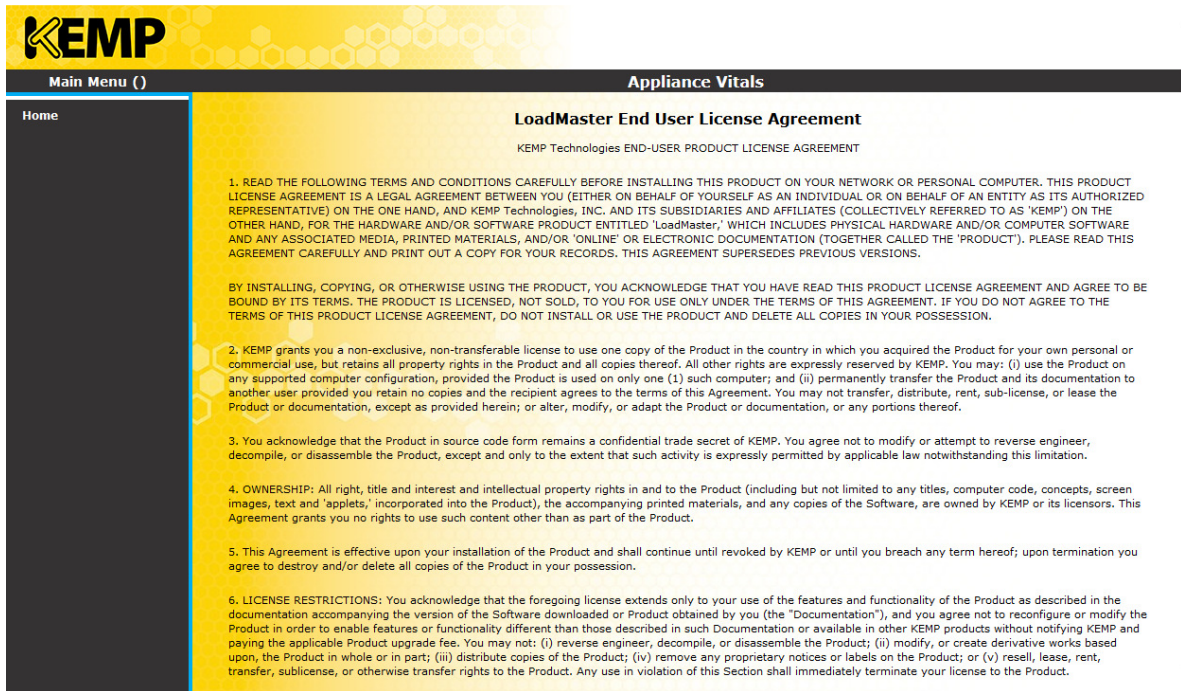


### 3.3 PC (パソコン) よりブラウザーを使用する場合

ロードマスターは、上記の3.2項でアドレスを変更しないで立ち上げるとデフォルトとしてイーサポート0に”192.168.1.101”のIPアドレスがアサインされて起動します。ロードマスターをこのIPアドレスで通信できるネットワークに接続することで、設定の全てをWUIより行えます。このような環境がない場合には、独自のLAN”192.168.1.0/24”を構築して設定を行うことができます。イーサポート0をネットワークに接続して、PCのブラウザーより

‘<https://192.168.1.101>’にアクセスします。上記の3.2項でIPアドレスを変更した場合は‘<https://<変更したIPアドレス>>’にアクセスします。証明書の署名者が見つからないメッセージが表示されますが、承諾することで下記のWUIホームページが表示されます。

下記の“User License Agreement”が表示されますので、内容を読んで承諾できるならば“Agree”ボタンをクリックします。



“Agree”ボタンをクリックしないと正規のWUI画面に進めず、WUIへアクセスしようとする  
 といつもEULAが表示されます。日本語訳は下記URLから入手できます。

EULA日本語訳：[http://www.kemptechnologies.jp/support/Documentation/60/LoadMaster-EULA\\_JPN.pdf](http://www.kemptechnologies.jp/support/Documentation/60/LoadMaster-EULA_JPN.pdf)

## 3. 4ライセンスの取得

### 3.4.1 オンラインでの取得

1. 上記 3.3 項の EULA に ‘Agree’ すると、ライセンスをリクエストする下記の画面が表示されます。オンライン、もしくはオフラインでのリクエストが可能です。システムがまだネットワークに接続されていない場合は、オフラインモードでの E メールによる申請となりますので、下記 3.4.2 項の “オフラインでの取得” にスキップします。

The screenshot shows the 'Appliance Vitals' page. At the top left is the KEMP logo. Below it is a 'Main Menu ()' button. The page title is 'Appliance Vitals' and the version is 'Vers:7.0-8e(Hyper-V)'. A table displays the following information:

IP address	192.168.1.34
Serial Number	
Boot Time	Mon Nov 11 14:47:25 UTC 2013
Appliance Version	7.0-8e

Below the table is a section titled 'License Required To Continue'. It contains a dropdown menu for 'Online Licensing' and a yellow box with the following text:

Please enter your KEMP ID and password below.  
 If you do not have a KEMP ID, please create one by visiting <https://alsi.kemptechnologies.com/register>

Below the yellow box are input fields for 'KEMP ID:', 'Password:', and 'Order ID# (optional):', along with a 'License Now' button.

At the bottom, it says 'Copyright © 2002-2013 KEMP Technologies, Inc.'

ライセンス取得には KEMP ID が必要です。KEMP ID を取得していない場合は、上記の表示画面内にある <https://alsi.kemptechnologies.com/register> をクリックします。表示された下記の登録画面に必要な項目を入力して “I have read the Terms and Conditions” に同意の上 ‘Submit’ をクリックします。システムが問題なくこの登録を受信したならば、直ちに入力した E メールアドレス宛へ KEMP ID が送信されます。詳細につきましては、下記の URL より ‘Feature\_Description-Licensing.pdf’ をダウンロードして参照して下さい。

[http://kemptechnologies.com/files/downloads/documentation/7.0/Feature\\_Description/Feature\\_Description-Licensing.pdf](http://kemptechnologies.com/files/downloads/documentation/7.0/Feature_Description/Feature_Description-Licensing.pdf)

The screenshot shows the 'Register a new KEMP ID to Activate and License a LoadMaster' page. It is divided into two main sections: 'New User Registration Details' and 'Existing Users'.

**New User Registration Details**

All fields are required

Input fields include: Company Name, First Name, Last Name, Country List (dropdown), Phone Number, KEMP ID\* (your email address), Retype KEMP ID, Password (with strength indicator), and Retype Password.

\* IMPORTANT NOTE  
 Your KEMP ID is the email address where we will send validation emails and licenses

[I have read the Terms and Conditions](#)

Buttons: Clear, Submit

**Existing Users**

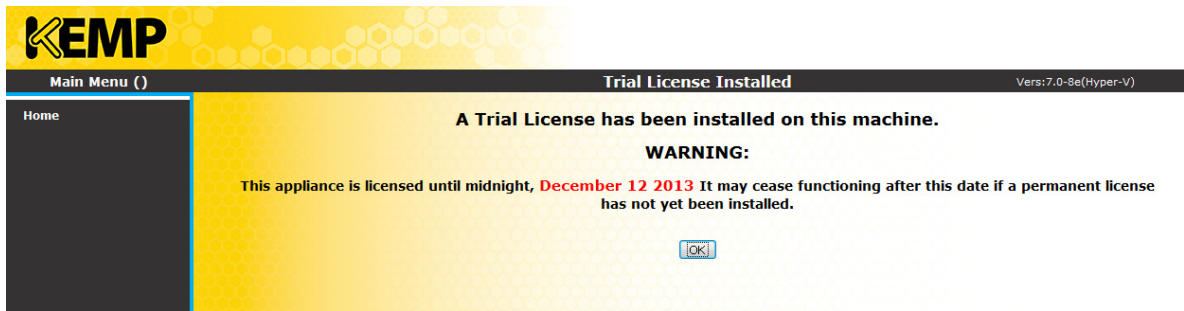
If you are an existing user but have forgotten your password please click here :  
 Password Reset

**Resend Activation Email**

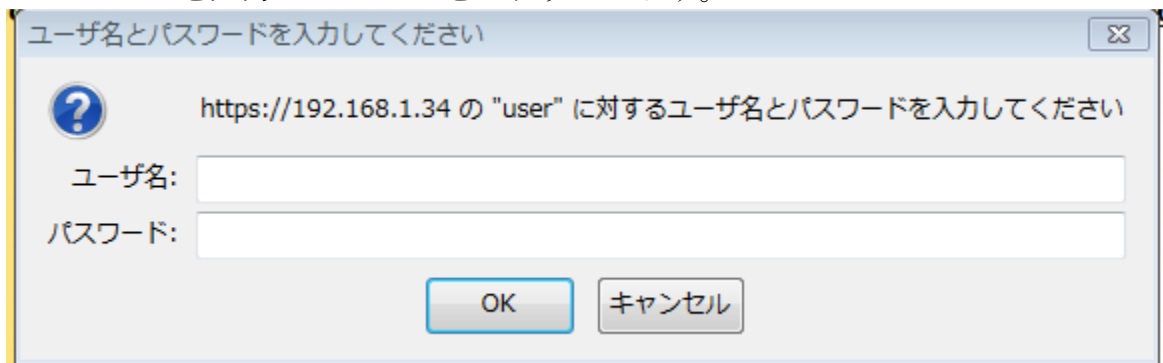
If you have registered before, but have not activated your account or did not receive an activation email, please click here :  
 Send Activation Email

2. Eメールで受信したKEMP IDと登録時に入力したパスワードを入力し、“License Now”をクリックします。下記の“Trial License Installed”メッセージが帰ってきたら“OK”をク

クリックします。



3. 下記の認証画面が表示されますので、デフォルトのユーザー名 ‘bal’ とパスワード ‘1fourall’ を入力して “OK” をクリックします。



4. パスワード更新画面が表示されますので、新しいパスワードを入力して “Set Password” をクリックします。パスワードは、半角文字で8文字から16文字までの範囲で指定できます。使用できる文字は英字（大文字、小文字）、数字、英数字以外の記号文字で、これらの文字を任意に組合わせて指定できます。ロードマスターは指定された文字列の強度を自動的に計算して、パスワードの強度が弱い場合はメッセージを表示します。メッセージが表示されたら文字種類を変更するか桁数を増やしてパスワードの強度を高めて下さい。

#### パスワード指定例

- |                 |        |               |
|-----------------|--------|---------------|
| ・英小文字のみ：        | 9文字以上  | ancdefghi     |
| ・英小文字と数字の混在：    | 8文字以上  | 1abcdefg      |
| ・英大文字と英小文の混在：   | 8文字以上  | Abcdefgh      |
| ・英小文字、記号、数字の混在： | 8文字以上  | ab!12345      |
| ・数字のみ：          | 13文字以上 | 0123456789012 |



**KEMP Appliance**

Main Menu (bal) 08:33:06 PM Appliance Vitals Vers:7.0-8e(Hyper-V)

Home

IP address	192.168.1.34
Serial Number	1000253
Boot Time	Mon Nov 11 14:47:25 UTC 2013
Appliance Version	7.0-8e

**A Password is required to access the Appliance**

Password:

Retype Password:

Copyright © 2002-2013 KEMP Technologies, Inc.

5. 再度認証画面が表示されますので、更新したパスワードを入力して“OK”をクリックします。

ユーザ名とパスワードを入力してください

https://192.168.1.34 の "user" に対するユーザ名とパスワードを入力してください

ユーザ名:

パスワード:

6. WUIのHomeページが表示されます。

**KEMP LoadMaster**

Main Menu (bal) 08:37:49 PM LoadMaster Vitals Vers:7.0-8e(Hyper-V)

Home

- Virtual Services
- Global Balancing
- Statistics
- Real Servers
- Rules & Checking
- Certificates
- System Configuration

Credentials		System Metrics	
IP address	192.168.1.34	CPU Load	1%
Serial Number	1000253	TPS [conn/s]	Total 0 (SSL 0)
Boot Time	Mon Nov 11 14:47:25 UTC 2013	NetLoad	Mbits/sec
LoadMaster Version	7.0-8e	eth0	0.0
License	UUID: f5861ff0d9407f1ad164d87a9b2e5d42ae3682d5152caac47c41d10db8a1bc3a Activation date: Mon Nov 11 20:26:43 UTC 2013 Licensed until: December 12 2013	eth1	0.0
		CPU Temp.	---

Network Metrics	Virtual Services	Real Servers
hour day month quarter year	Active Services 0 [0]	Active Servers 0 [0]
Packets Bits Bytes	hour day month quarter year	hour day month quarter year
network traffic eth0	Connections Bits Bytes	Connections Bits Bytes
network traffic all VS	network traffic all RS	

bit/sec

19:40 20:00 20:20

max avg min

in	8.35 kbps	3.14 kbps	1.24 kbps
out	0.01 kbps	0.00 kbps	0.00 kbps

### 3.4.2 オフラインでの取得

1. システムがインターネットへアクセス出来る状態にない場合は、‘Offline License’を選択します。オフラインを選択すると、下記の画面が表示されます。

The screenshot shows the KEMP Appliance Vitals web interface. At the top, there is a navigation menu with 'Main Menu ()' and 'Home'. The main content area is titled 'Appliance Vitals' and 'Vers: 7.0-8e(Hyper-V)'. Below this, there is a table displaying appliance details:

IP address	192.168.1.231
Serial Number	
Boot Time	Thu Nov 14 15:56:00 UTC 2013
Appliance Version	7.0-8e

Below the table, the text 'License Required To Continue' is displayed. A dropdown menu is set to 'Offline Licensing'. A yellow box contains the following text:


Click [here](#) to obtain your license or visit <https://alsi.kemptechnologies.com/register/offlineLicensing.php?656y4-gwwpw-a2uwg-q5uwg&xparam=08&xvln=HYPERV&xvers=7.0-8e>

Access Code: 656y4-gwwpw-a2uwg-q5uwg

Below this, there is a 'License:' input field and an 'Apply License' button. At the bottom, the copyright notice 'Copyright © 2002-2013 KEMP Technologies, Inc.' is visible.

2. “here” をクリックするか “or visit” に続く URL をコピーしてブラウザにペーストします。
3. “here” をクリックした場合、“or visit” 後の URL にアクセスした場合の両方とも下記のようにアクセスコードと KEMP ID + パスワードが自動的に入力された申請画面が表示されます。KEMP ID を取得していない場合は、右横の “Create KEMP ID” をクリックして登録手続き後 KEMP ID を入力します。そして、LoadMaster Type と Firmware Version を選択後に ‘Submit’ をクリックします。




Offline Licensing

### Offline Licensing

All fields marked \* are mandatory

Access Code \*

Order ID (optional)

KEMP ID \*

Password \*

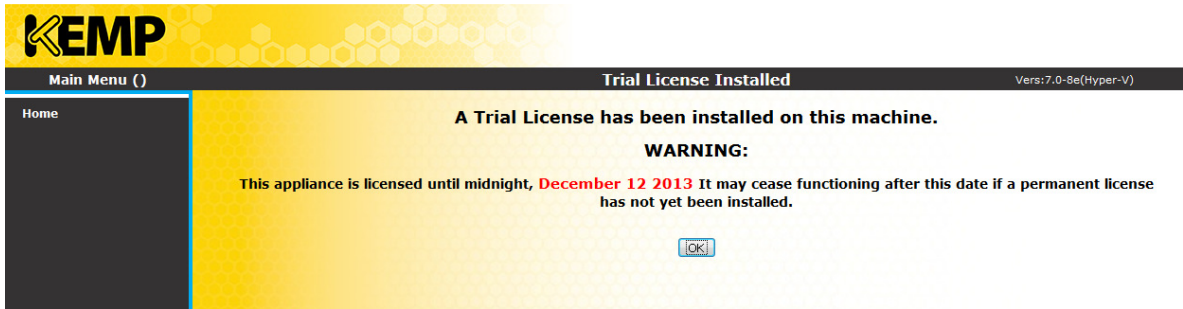
4. オフラインでのライセンスリクエストは E メールにて送信されて、KEMP 社よりライセンスを添付で含んだ返信が直に返ってきます。添付のライセンスは、下記のようなフォームで書かれていますので、Begin からの end までをコピーして上記 9 項の“License”欄にペーストして‘Apply License’をクリックします。

License Block (copy and paste from begin to end):

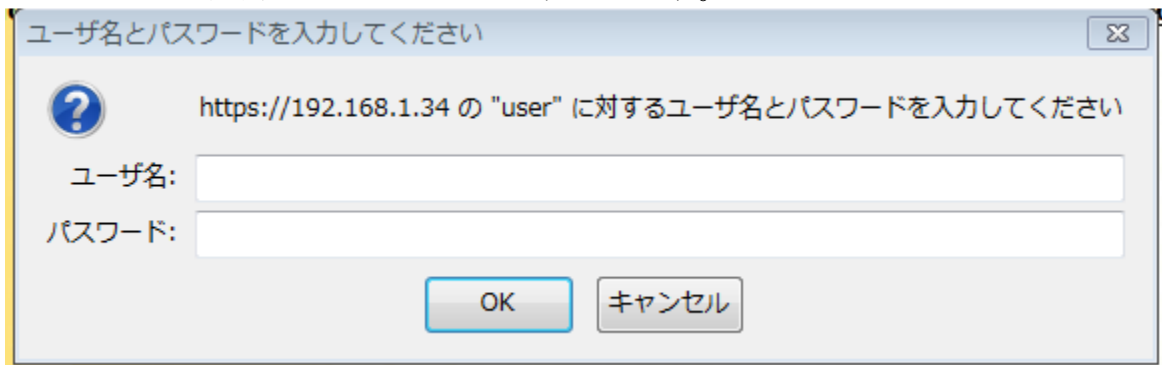
```
begin
666 /dev/null
MD0&Y%N96KP`W9C8S9F9E9&,R-S$Q9#4P,F9C-C)C-C,P8V)A93EE8S4S9#4T
M.&$Q8S0S.3EF.3=A-C1B,SEF8C5F8C-D9#)D`
M`
M`!D!`~~~~~`KU:1`;D6Y@`W_)ate%NO]5(Q.)UL;!(X`&U%&?NVH94.B3J":
M395^LNI+_T*AR;=LK5IHE[H5UX[I_V^[04W$0LUV:(7%2;=H+Y%^(!)IQ_)*)
M8N,_WK1J"H;M$0?@<B4ZDI7¥;¥*K(D*NGSI17#815F7XUZNWD9Q`"#V&ZE@9
MC[MJH!4MX@`#%R<JDFU`K7VR97IB<Y4#UVA_$3S!^1CN3-PC=G!U__J`X2.A
M;3ILD>(8S@O'VUSHH@W2*M+SNDA;^)>[*KJF8ZKHB'650CGR!GN[]`#:9AHZ
M>U(!"L$)!YC;Z_1#[,P(S%2$B;DIBMT'Y00(80>"LO[¥[NEB$LV?N9INS
```

```
<CA+W&"HF3T1_'RL"N7¥5I$0$1GRQ09MJ5SW.<@``
、
end
```

5. 下記の“Trial License Installed”メッセージが帰ってきたら“OK”をクリックします。



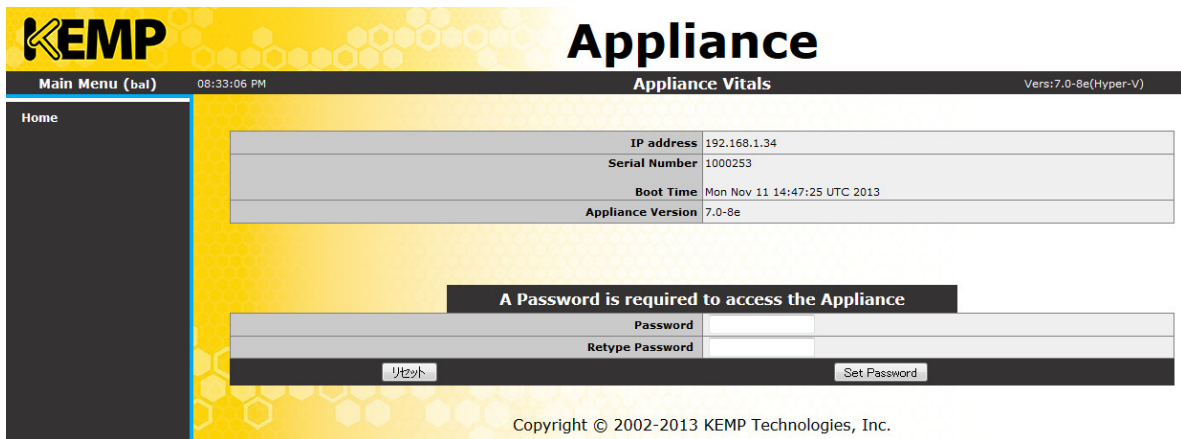
6. 下記の認証画面が表示されますので、デフォルトのユーザー名‘bal’とパスワード‘1fourall’を入力して“OK”をクリックします。



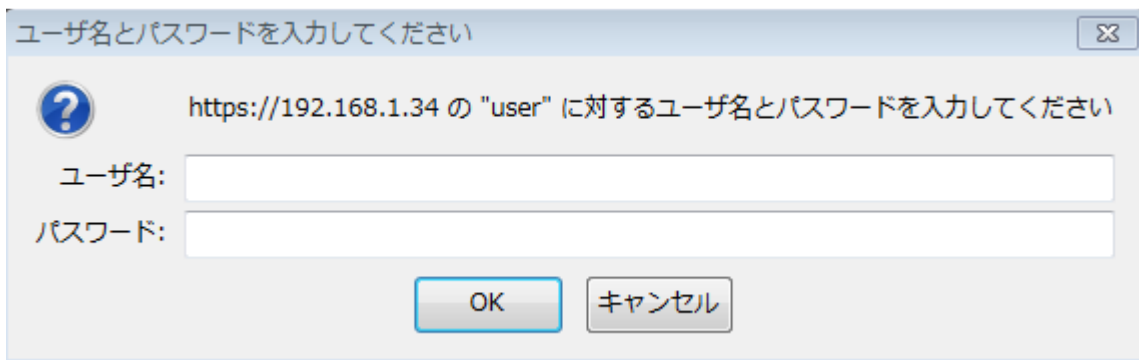
7. パスワード更新画面が表示されますので、新しいパスワードを入力して“Set Password”をクリックします。パスワードは、半角文字で8文字から16文字までの範囲で指定できます。使用できる文字は英字（大文字、小文字）、数字、英数字以外の記号文字で、これらの文字を任意に組合わせて指定できます。ロードマスターは指定された文字列の強度を自動的に計算して、パスワードの強度が弱い場合はメッセージを表示します。メッセージが表示されたら文字種類を変更するか桁数を増やしてパスワードの強度を高めて下さい。

パスワード指定例

- ・ 英小文字のみ： 9文字以上    abcdefghi
- ・ 英小文字と数字の混在： 8文字以上    1abcdefg
- ・ 英大文字と英小文の混在： 8文字以上    Abcdefgh
- ・ 英小文字、記号、数字の混在： 8文字以上    ab!12345
- ・ 数字のみ： 13文字以上    0123456789012



8. 再度認証画面が表示されますので、更新したパスワードを入力して“OK”をクリックします。



9. WUIのHomeページが表示されます。

### 3.5 HA 設定 : HA-2 セットアップ

もし、単一構成でロードマスターを設置する場合は、このセクションをスキップして、次の“WUI 設定”に進んでください。

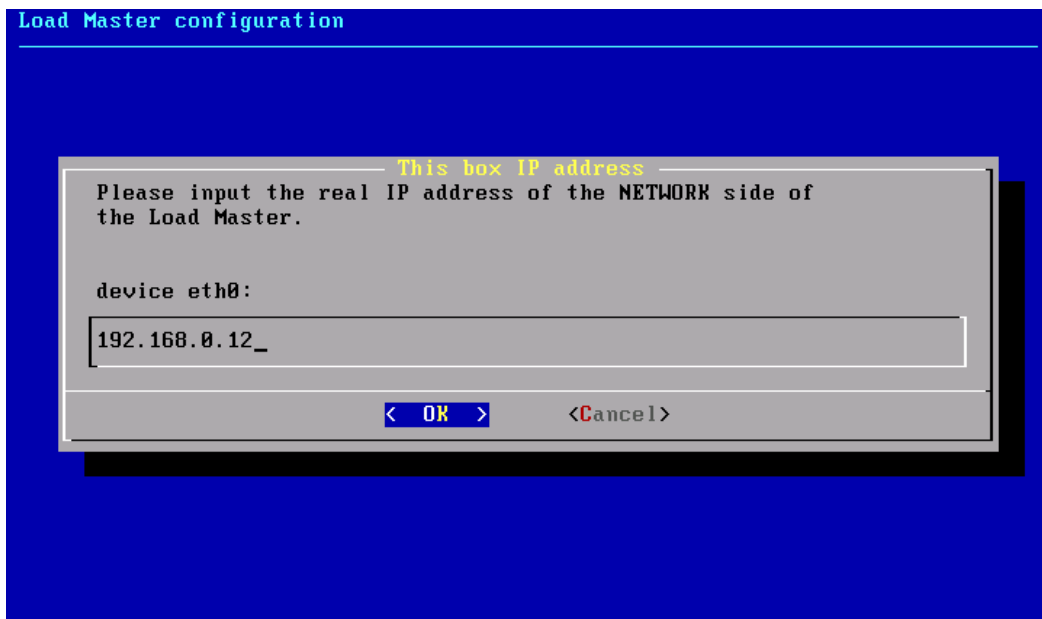
HA 2 ユニットの電源を投入する前に、イーサポート 0 をスイッチに接続しておいてください。既に設定してある共通の情報を HA 1 ユニットから取り込むために必要です。このケーブルの接続に問題があると、HA1 からの設定情報の取り込みが失敗して HA2 のセットアップが成功しませんので注意してください。又、2アームでのネットワーク構成の場合は、イーサポート 1 もファーム側のスイッチへ接続しなければなりません。

1アームでのネットワーク構成の場合は、HA 構成の 2 台のユニットのイーサポート 1 同士をストレート、もしくはクロスケーブルで接続する必要があります。これは、設定情報の同期と相手の状態を監視するために必要です。又、設定が終了して、ロードマスターを再起動した後に、ウェブユーザインターフェース (WUI) から“System Configuration”サブメニュー下の“Interfaces” 1 “を開き、“Use for HA checks”にチェックマークがあることを確認してください。もし、チェックマークがない場合は、チェックマークを付けてください。その他のイーサ

ポート 1 への設定は一切不要です。

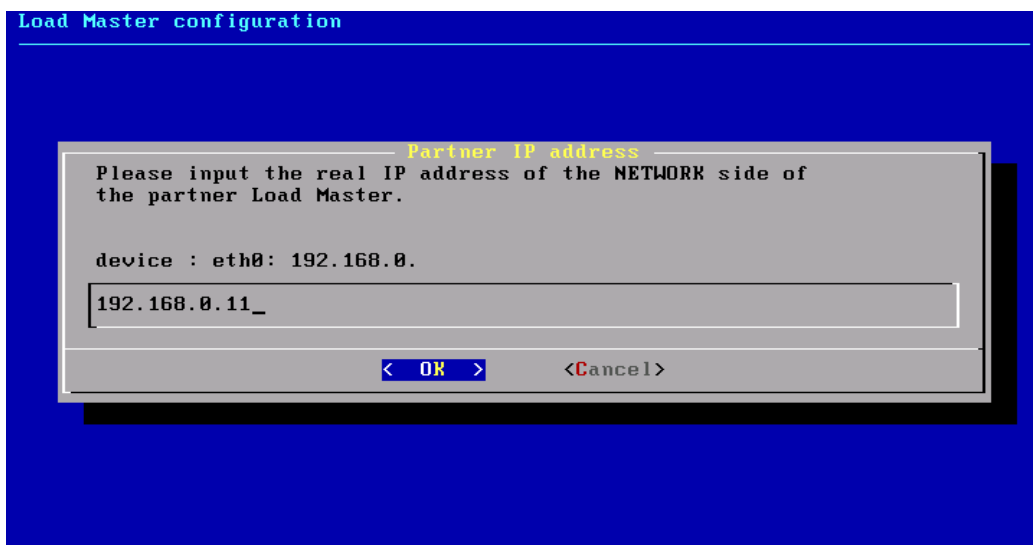
2 アームでは、2 台のユニットのイーサポート 1 同士をケーブルで接続する必要はありませんが、ネットワークを介して HA 同士が同期を取りますので、同じくイーサポート 1 の “Use for HA checks” にチェックマークがあるのを確認してください。

1. ケーブルの接続が終了したら、HA2 ユニットの電源を投入し HA1 で行ったように HA2 用ライセンスキーを入力します。正しいキーが入力されたら、下記のようにイーサネットポート 0 用 IP アドレスの入力画面が表示されます。HA2 用 IP アドレスを入力します。

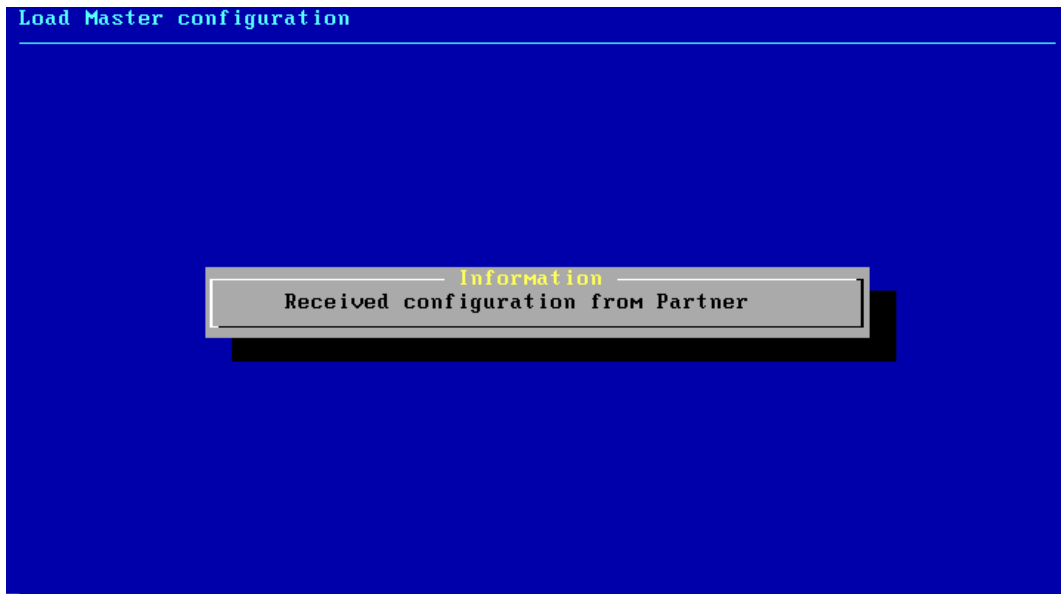


2. HA1 で入力したのと同じネットマスクを入力します。

3. 下図のように、パートナーの IP アドレスの入力が求められますので、HA 1 のイーサポート 0 の IP アドレスを入力します。



4. HA2 は、HA1 より共通の設定情報を取り込みます。この処理は1分以下で終了し、下記の取り込みの成功メッセージが表示されます。



これで両方のユニットの初期設定が正常に完了しました。ここから先は、ウェブユーザーインターフェース (WUI) を使って仮想仮想サービスなどの設定を行います。WUI の使用方法を説明している章を参照して下さい。

### 3.6 仮ライセンスの永久ライセンスへの更新

#### 3.6.1 アプライアンスの場合

アプライアンスのライセンス取得では、例外を除いて当初より永久ライセンスがインストールされます。インストールされているライセンスの種類は、WUI の Home 画面の “Credentials” 内の “License” フィールド欄の “Licensed until” に下記のように表示されています。

- Unlimited: 永久ライセンス
- Up to xxxxxxxxxx: 仮ライセンス

仮ライセンスの場合は、購入された弊社販売店までお問い合わせ下さい。

<b>License</b>	UUID: f28311d7552c07940456d569835a391a7e5f65 7064931d00839fd13fa1e395d0
	Activation date: Sun Dec 1 03:13:14 UTC 2013 Licensed until: unlimited

### 3.6.2 VLM の場合

VLM（仮想アプライアンス）の場合は、ハイパーバイザーへの展開を行って上記の“3.4 項 ライセンスの取得”に沿ってライセンスを取得すると、必ず仮ライセンスがインストールされます。既に購入済みの場合でも同じように仮ライセンスがインストールされますので、下記に沿って永久ライセンスへの更新を行う必要があります。

1. WUI の Home 画面を開き、“Credentials”内の“Serial Number”を取得します。

Credentials	
IP address	192.168.3.200 (VLM201:192.168.3.201:HB)
Serial Number	468305

2. VLM を購入した弊社販売店のほうへ“Serial Number”を添えて永久ライセンスのリクエストを行います。
3. 販売店のほうより永久ライセンスへの更新準備が整った旨の回答が来ます。
4. 上記 3.4 項に沿って、再度ライセンスの取得を行います。
5. WUI の Home ページ上の“Credentials”内の License 欄の“Licensed until :”が‘unlimited’に変更されたのを確認します。もし、変更されない場合は、販売店のほうへ連絡して下さい。

## 4 ウェブユーザインターフェース (WUI)

WUI ユーティリティは、SSL とアクセス管理リストを使ったブラウザーベースの安全なリアルタイム・インターフェースです。この安全なインターフェースは、ロードマスターが搭載している OpenSSL とアパッチ Web サーバによって提供されます。WUI は、下記の理由により、ロードマスターの設定、及び変更を行うための推奨される方法です。

- より直感的で簡単に使用できるので習得の時間が短い。
- 入力項目が直ぐにチェックされ、間違いがレポートされるので、設定エラーを最小限にできる。
- 設定ファイルの再読み込みや、プロセスの再スタートなしで、入力したほとんどの設定や変更が直ぐに適用される。又、それらの設定、変更は設定ファイルへ永続的に保存される。
- 使い慣れたブラウザーからのアクセスなので、SSH クライアントを使ってコンソールへアクセスするより容易である。

### 4.1 初めての接続

ロードマスターのソフトウェアには、安全な SSL 接続を介して WUI ユーティリティより設定を行うための、アパッチ Web サーバのライセンスが含まれています。WUI ユーティリティでは、仮想仮想サービス、リアルサーバ、コンテンツルール、及びシステムパラメータなど、ほとんど全ての設定が行えます。又、WUI ユーティリティは、ネットワークトラフィックの監視、接続状況、システムリソース、及び稼働時のエラーなどをセーブしているメッセージログの表示も行えます。

WUI ユーティリティは、ネットスケープのナビゲーターVersion4.7 以降、もしくはマイクロソフトのインターネットエクスプローラーVersion5 以降を使用する必要があります。

#### ■ WUI ユーティリティへのアクセス手順：

1. ロードマスターにアサインされている IP アドレスに、ブラウザーより HTTPS プロトコルでアクセスします。

<https://<IP address of your LoadMaster>>

**Note:** IP アドレスには、通常ネットワーク側（イーサポート 0）にアサインされた IP アドレスを指定します。

HA 構成の場合は、ネットワーク側のシェア IP アドレスを指定します。個別の IP アドレスでも接続できますが、設定/変更できる項目が制限されます。

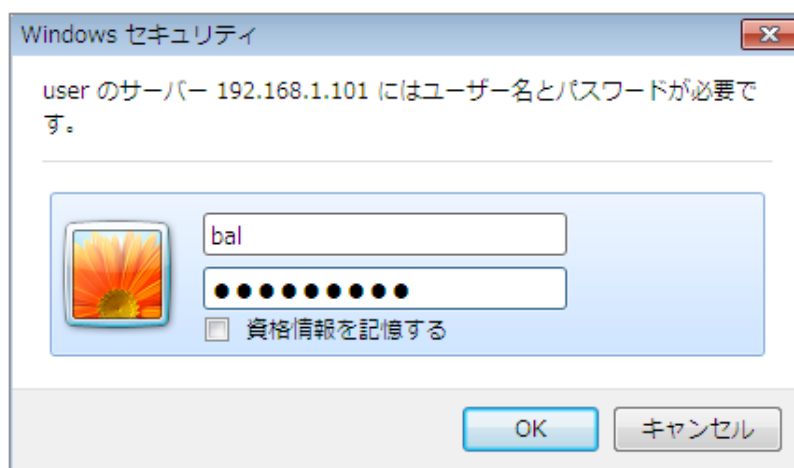
2. ブラウザーより初めてこの WUI ユーティリティにアクセスした際、ブラウザーは下記のような、SSL 証明書が認定を受けた証明機関より発行されたものでない警告を表示します。ロード

マスターは、セットアップ時、独自の SSL 用証明書を発行しますので、問題のない一般的な警告です。

“続行しますか？”の問いに対して“はい”を選択します。

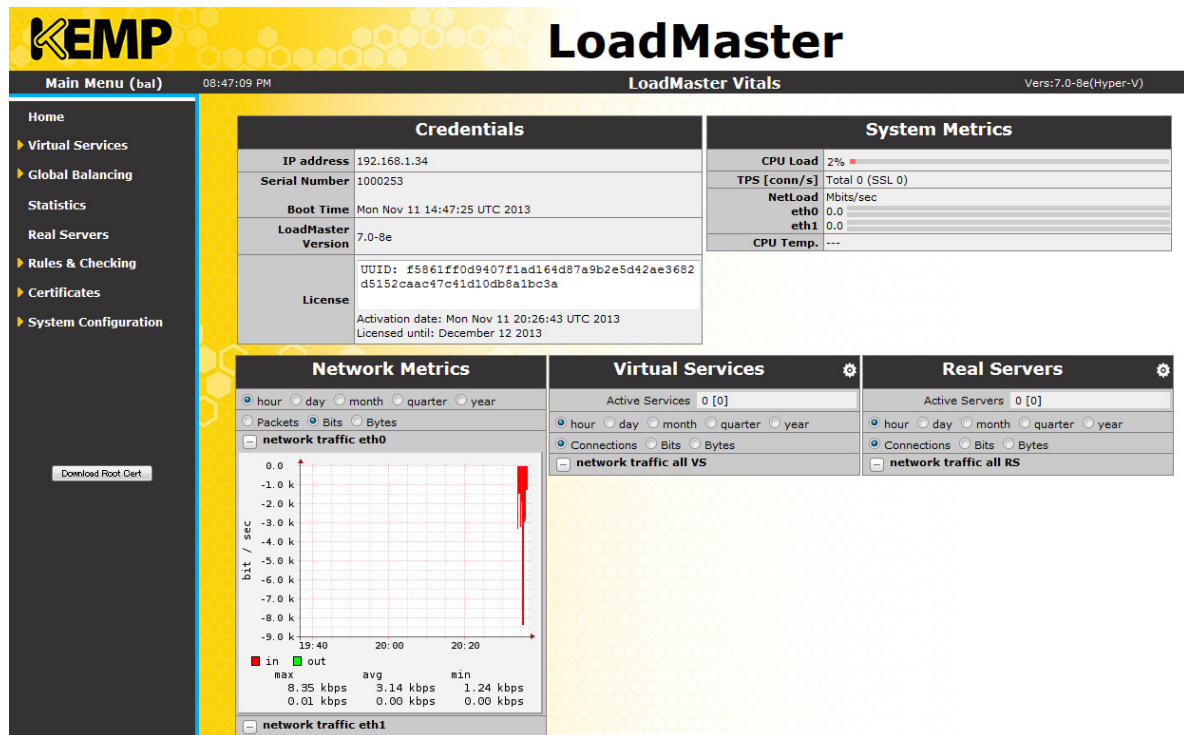


- 次に、ユーザ名とパスワードの入力画面が表示されます。ユーザ名として‘bal’、そして初期設定で変更したパスワードを入力します。正しく入力されると、WUI ユーティリティのページが表示されます。



- 下記のように、WUI ユーティリティのメインページが表示され、ロードマスターの設定とモニター機能を使用できます。現在の全ての設定内容や仮想仮想サービス毎の各リアルサーバの状況、及びシステムの統計情報を確認できます。





## 4.2 仮想仮想サービスとリアルサーバの概念

### 4.2.1 仮想仮想サービス

仮想仮想サービスは、ロードマスターの主要メカニズムでトラフィックの管理と追跡を行います。ロードマスターが管理する各サイトに対して、それに付随する仮想仮想サービスを最低1つ定義します。1つの仮想仮想サービスは、1つの仮想仮想IPアドレスと1つ、もしくはこの仮想仮想ポートのコンビネーションで構成されます。仮想仮想IPアドレスは、クライアントに公開されるIPアドレスで、サイトのドメインとホスト名としてDNSに登録されるものです。仮想仮想ポートは、クライアントプログラムで指定されるTCP、もしくはUDPポート番号です。例えば、KEMPテクノロジー社の [www.kemptechnologies.com](http://www.kemptechnologies.com) は、DNSサーバにてIPアドレス **216.239.138.211** に変換されます。そして、ポート80（通常のHTTP用ポート）を介してアクセスされます。よって、KEMPテクノロジー社のウェブサイトの仮想仮想サービスは、**216.239.138.211:80** ということになります。

仮想仮想サービスは、各サイトへのトラフィックの流れを管理するための多くの機能を持ちます。全ての仮想仮想サービスは、単一のIPアドレスとポートのコンビネーションで表わされ、通常いくつかのリアルサーバを持っています。どの機能を選択したとしても、仮想仮想サービスを介したTCPもしくはUDPの全てのトラフィックは追跡されます。デフォルトとして、ロードマスターは下記の機能を仮想仮想サービスとして提供します。

- 仮想仮想サービスに属する全てのリアルサーバの可用性の確認（ヘルスチェック）
- リアルサーバへのトラフィック負荷分散

- 仮想仮想サービスの IP アドレスから、リアルサーバの IP アドレスへの変換
- 仮想仮想サービスの TCP/UDP ポートから、リアルサーバのポートへの変換

仮想仮想サービス作成時、IP アドレスとポート変換はデフォルトで動作します。更に、仮想仮想サービスは追加的な下記のようなトラフィック管理が働くように設定が可能です。

- コンテンツによるトラフィックの分配—コンテンツスイッチ
- ソースパスに沿ったレスポンスのリターン

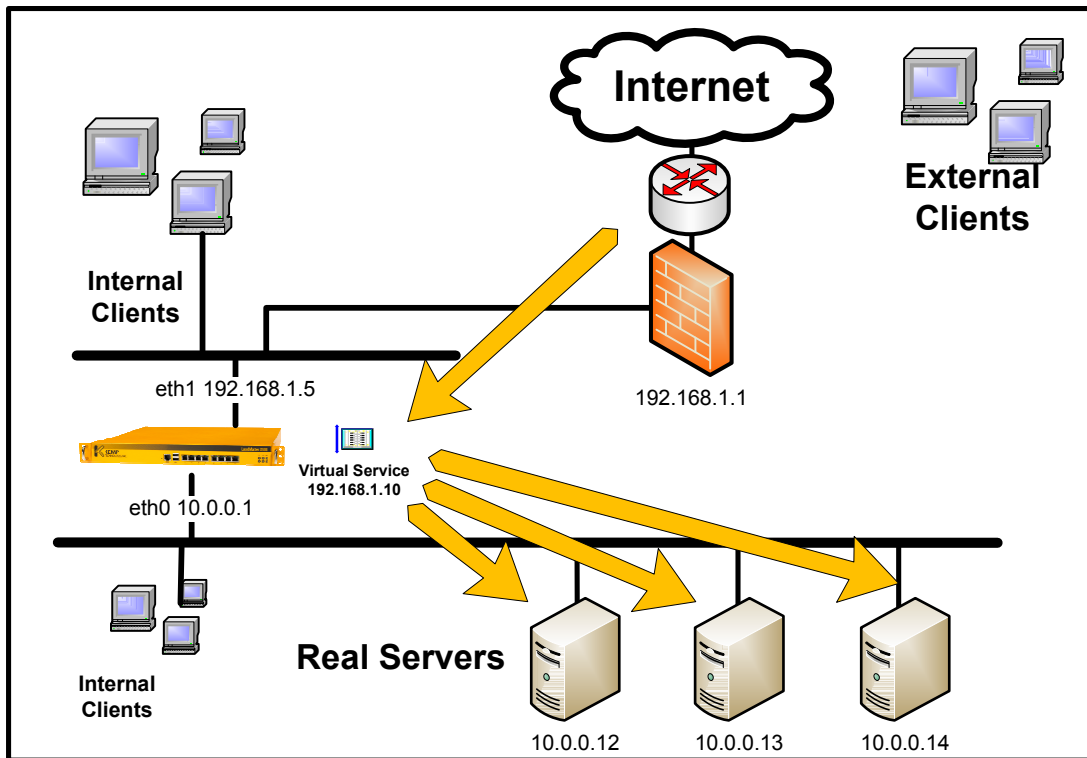
仮想仮想サービスは、サイトに接続するための IP アドレス、ポートのペアと、実際のサービスを提供するホストの IP アドレス、ポートのペアとの関連を定義します。基本的には、1つの仮想仮想 IP アドレスとポートには、最低でも1つ、又は、そのサイトの様々なコンテンツを提供するための複数のリアルサーバが関連付けられます。仮想仮想サービスは、設定によりいずれのポートへの接続も許可できる反面、特定ポートへの接続の制限も行えます。システムは、仮想仮想 IP アドレスとポート番号を基に、入ってくるトラフィックがリアルサーバへの分配を許されているかどうかの判定を行います。

## 4.2.2 リアルサーバ

1つのリアルサーバは、システムとして認知できる物理的なサーバとして、1つの IP アドレスとポート番号のコンビネーションをもつホストです。単一の物理的サーバは、いくつものリアルサーバとしてサービスを提供可能です。複数の仮想仮想サービスが、同じリアルサーバをそのメンバーとして重複して指定することができます。この場合、ある特定のリアルサーバの属性を設定、もしくは変更すると、このリアルサーバをメンバーとしてもつ仮想仮想サービスは、この設定、もしくは変更の影響を受けます。

通常、リアルサーバは仮想仮想サービスよりも安全な所に位置します。これは、多くの場合、リアルサーバにルーティング不可能な IP アドレス (RFC1918) を指定することで可能にしています。

下記のネットワーク図の例として、仮想仮想サービスに 192.168.1.10:80 の IP アドレスとポート番号のコンビネーションを指定したとします。この仮想仮想サービス配下に、1つ、もしくはそれ以上のリアルサーバを設定します。この例では 10.0.0.12:80, 10.0.0.13:80 及び 10.0.0.14:8080 の3つのサーバが設定されており、仮想仮想サービスは、192.168.1.10:80 で受けたパケットをこれらの3つのうちの1つのサーバにフォワードするために、そのサーバの IP アドレスとポート番号へ変換します。



### 4.2.3 ネットワークでのパケットの流れ

上記の仮想仮想サービスとリアルサーバの図を基に、ロードマスターを介したパケットの流れの詳細を説明します。パケットの流れは、エンドユーザにとってトランスペアレントである必要があります。全てのパケットは、内部のリアルサーバに向かうようにロードマスターによりルート変更されます。ロードマスターで使用する機能により例外もありますが、下記はロードマスターを介した場合の共通した一般的なトラフィックの流れです。

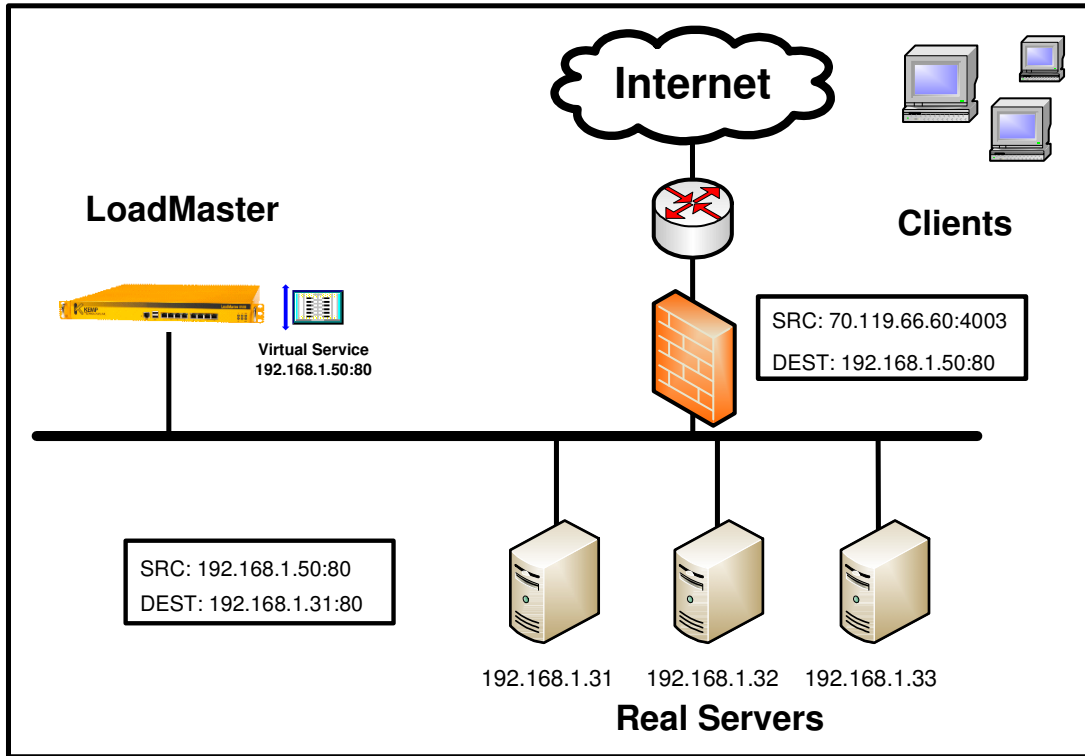
クライアントよりパケットが最初に送信される時、その行き先はロードマスターに設定されている仮想仮想サービスの IP アドレスで、ソース IP アドレスはクライアントの IP アドレスです。ロードマスターは、このパケットを受け取り、行き先 IP アドレスを負荷分散のアルゴリズムにより選択されたリアルサーバの IP アドレスへ変換します。行き先 IP アドレス、及びソース IP アドレスは、リアルサーバがレスポンスを返した時、元のクライアント IP アドレスへ再変換するためにリザーブされます。

ソース IP アドレスに関しては、ロードマスターが仮想仮想サービスを設定する時に選択できる2つのオプションがあります。

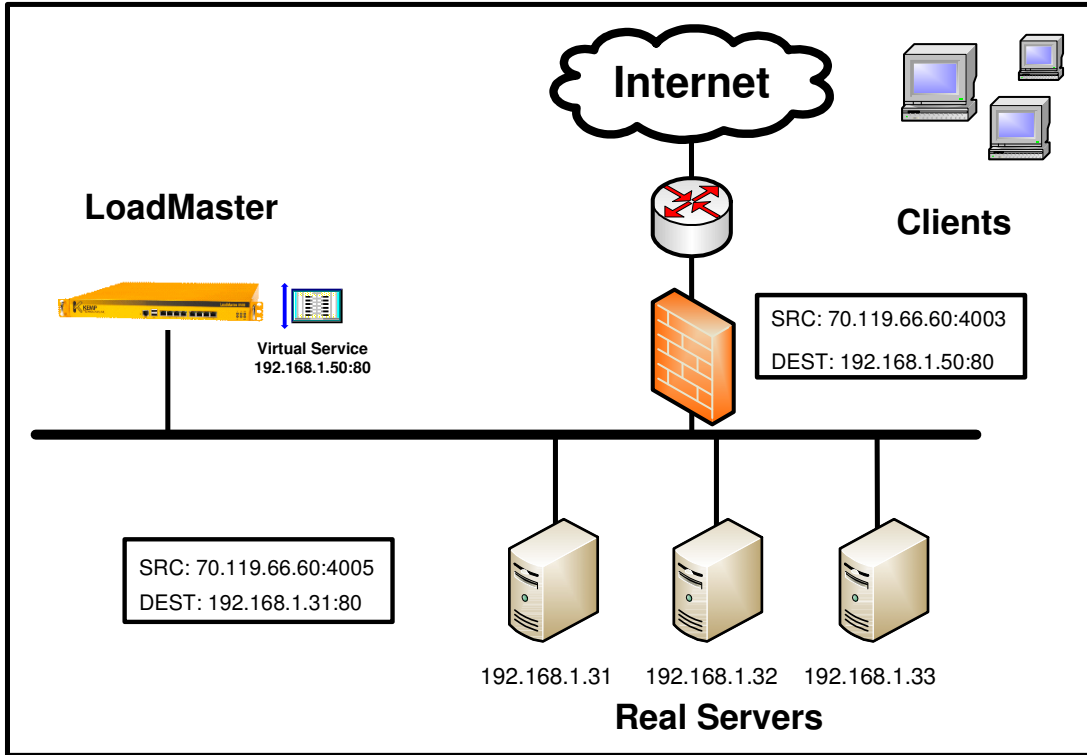
デフォルトのオプションは、ソース IP アドレスを仮想仮想サービスの IP アドレスに変換する非透過モードです。他のオプションは、クライアント IP アドレスをそのままソース IP アドレスに使用して、リアルサーバに通過させる透過モードです。

これらのパケットの流れを下記の図に示します。

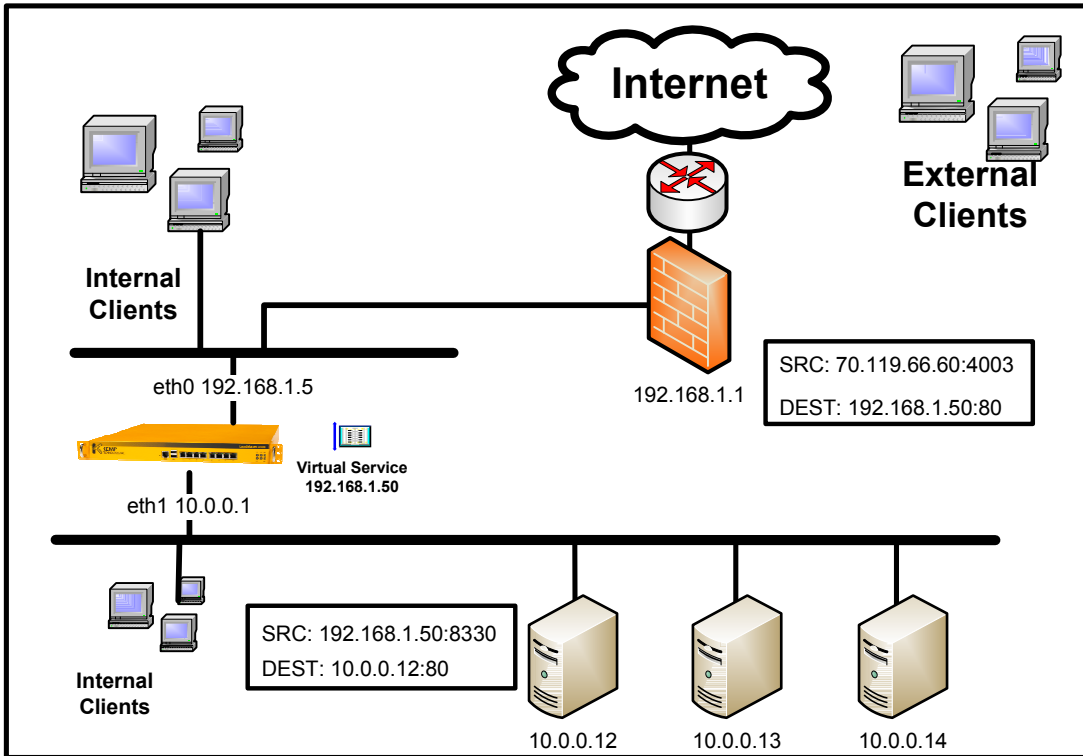
- 1-アームネットワーク形態 - 非透過モード



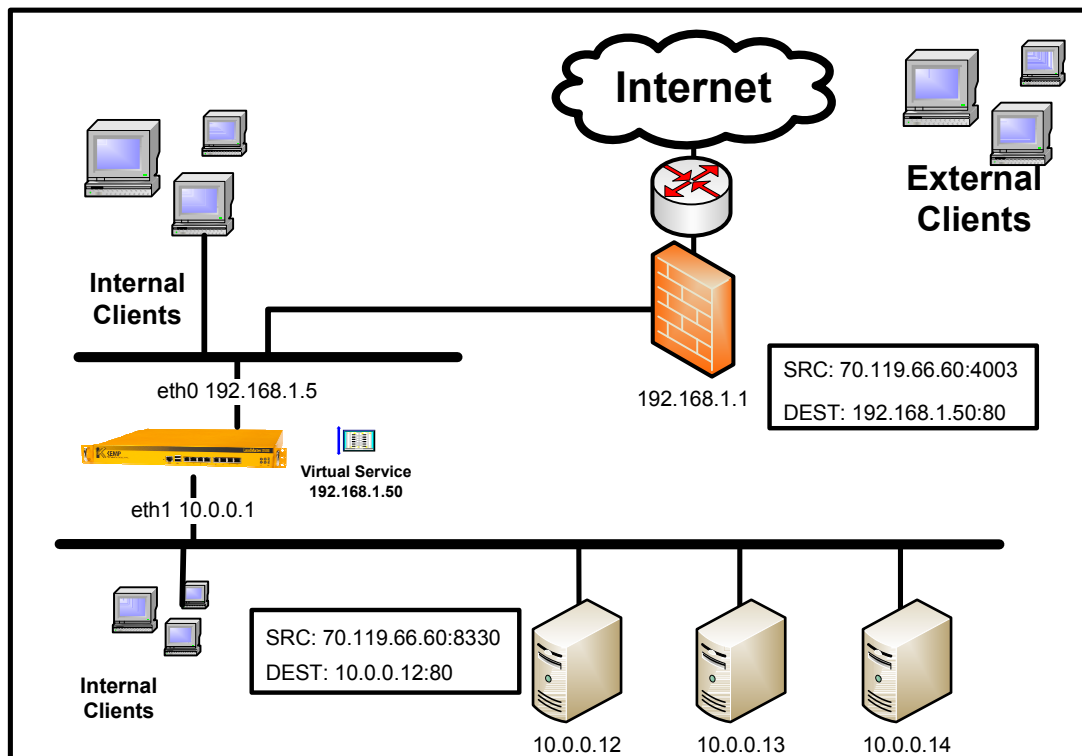
- 1-アームネットワーク形態 - 透過モード



- 2-アームネットワーク形態 - 非透過モード



- 2-アームネットワーク形態 - 透過モード



## 4.3 仮想仮想サービス作成

### 4.3.1 仮想仮想サービスの作成

仮想仮想サービス・サブメニュー下の“Add New”をクリックし、特定の IP アドレスとポート番号、及びプロトコルを入力します。ポート番号は、サービスリストとして一般的な番号を使用します。特定の IP アドレスとは、クライアントが使うサービスを DNS が変換したものです。例えば、弊社のウェブサイト“www.kemptechnologies.com”が DNS サーバにより変換された IP アドレスです。

1. メインメニューの“Virtual Service”を選択し、[> Add New] をクリックします。
2. “Please Specify the Parameters for the Virtual Service”画面で、仮想仮想 IP アドレス、ポート番号を入力し、特定のプロトコルを選択します。各フィールドの説明を以下に示します。

パラメータ	解説	デフォルト
Virtual Address	DNS が解決するサービスの IP アドレス	空白
Port	Virtual Address が使用するポート番号.	80
Protocol	Virtual Address が使用するプロトコル	tcp

- [Add this Virtual Service]ボタンをクリックします。
- 入力が正しいと下図の“Virtual Service Properties”画面が表示されます。

- この“Virtual Service Properties”画面で、下記の特性を指定します。

#### ■ Basic Properties (基本特性)

パラメータ	解説	デフォルト
Active or Deactivate Service	この仮想仮想サービスを有効、もしくはは無効にする。	有効
Service Type	アプリケーションのタイプを選択します。	ポート番号により可変
Service Name	この仮想仮想サービスの識別用ニックネームを作成します。	なし
Alternate		

Address		
---------	--	--

## ■ Standard Options

Force L7	この仮想仮想サービスをレイヤー7で稼動するように強制します。このパラメータは、レイヤー4で仮想仮想サービスを設定した時のみ表示されます。	
Extra Ports	VS がサービスを受け付けるポート番号が複数で尚且つ非連続番号であるならば、このパラメータに追加のポート番号を入力します。	
L7 Transparency	レイヤー7での透過モードの設定を行います。“Force 7”や、パーシステンスをクッキー等のL7用に設定した時のみ表示されます。（注：レイヤー4では表示されません。）	チェックマーク有り
Allow Server Initiating Protocols	MTA (SMTP), SSH など、RS から TCP 接続後にアプリケーションレイヤ (L7) でロードマスターにセッションを張るプロトコルでは、このパラメータをオンにする必要があります。（注：L4モードでは現れません。又、必要ではありません。）	チェックマーク無し
Real Server Check Protocol	リアルサーバの正常性をチェックするためのプロトコルを選択します。TCPを選択した場合は、単に接続性をチェックします。	ポートにより可変 (ポート 80 なら HTTP)
Persistence Options	パーシステンス方法を選択します。選択したら、必要に応じてタイムアウトの値を変更します。選択できるオプションを下記の <b>Note-1</b> に示します。	なし (無効)
Scheduling Method	リアルサーバへの負荷分散方法を選択します。選択できるオプションを下記の <b>Note-2</b> に示します。	Round robin
Idle Connection Timeout	L7 用 VS 毎のセッションのアイドルタイムアウト設定用です。‘0’に設定されている場合は、システムの設定値に従います。	0
Use Address for SNAT	2 アーム構成時に RS より外部へのアクセスを可能にする SNAT がオンになっている場合、このパラメータをオンにすることで、VIP アドレスがソース IP ア	無効



	ドレスとして使用されます。	
--	---------------	--

**Note-1:**

パーシステンスを有効にするとクライアントと特定のリアルサーバ間の接続を持続させます。言い換えれば、同じクライアントからの接続は、特定のリアルサーバへのみ接続されます。タイムアウト値は、接続情報をどれだけの期間保持するかを指定するものです。パーシステンスのタイプは、プルダウンリストから選択できます。オプションには、下記のものがあります。

**SRC IP Address (ソース IP アドレス)**

サービスリクエストを行うクライアントの IP アドレスをパーシステンスのキーとして使用します。

ネットマスクは、ロードマスターがその IP アドレスをどれだけの IP アドレス範囲で接続を持続させるかの判断に使用します。

<例>:

ネットマスクを **255.255.255.255** (デフォルト値) に設定した場合、全ての IP アドレスがパーシステンスの対象となります。例えば、**200.190.125.67** の IP アドレスを持ったクライアントがリアルサーバに接続した場合、この特定 IP アドレスをパーシステンスの対象 IP アドレスとします。このクライアントが、接続を終了したとします。ある一定時間を過ぎて (タイムアウト時間内)、このクライアントが前と違う IP アドレス **200.190.125.44** で接続を再開しても、同じリアルサーバへの接続を行う必要性はないと判断します。

しかしながら、もしネットマスクを **255.255.255.0** に設定したとすると、**200.190.125.X** の IP アドレスを持ったクライアントグループの接続は、タイムアウト時間内は全て同じリアルサーバへ接続されます。

**Server Cookie (サーバクッキー)**

ロードマスターは、HTTP ヘッダー内に含まれるクッキーの特定の値をチェックします。同じクッキーと判断されると、前回と同じリアルサーバへ接続されます。このクッキーは、リアルサーバで生成されなければなりません。

**Super HTTP (スーパーHTTP)**

スーパーHTTP オプションは、HTTP リクエストの中の “User-Agent” フィールドをハッシュ化した値を使用します。HTTP リクエスト内に同じ値が含まれているならば、前回接続したリアルサーバへと接続します。もし、HTTP リクエストの中に ‘MSRPC’ という MS Exchange サーバで使用する文字列が含まれていた場合は、“Authorization” フィールドも含めてハッシュ化します。このオプションは、MS Exchange サーバの CAS サービス用仮想仮想サービスを作成する時に推奨します。

**Server Cookie or Source IP (サーバクッキー、またはソース IP アドレス)**

最初にサーバクッキーでのパーシステンスを試みますが、何らかの理由で失敗した場合は、クライアントの IP アドレスを使ってパーシステンスを試みま

す。

#### **Active Cookie (アクティブクッキー)**

パーシステンスを可能にするためにロードマスターが自動的に特殊なクッキーをセットします。

#### **Active Cookie or Source IP (アクティブクッキー、またはソース IP アドレス)**

最初にアクティブクッキーでのパーシステンスを試みますが、何らかの理由で失敗した場合、クライアントの IP アドレスを使ってパーシステンスを試みます。

#### **Hash all Cookie (ハッシュクッキー)**

クッキーをハッシュ値で判断しパーシステンスを行います。同じクッキーセットを持つリクエストは、同じリアルサーバへ接続されます。

#### **Hash all Cookies or Source IP (ハッシュクッキー、または IP アドレス)**

最初にクッキーセットのハッシュ値でパーシステンスを試みます。もし何らかの理由で失敗した場合は、クライアントの IP アドレスを使ってパーシステンスを試みます。

#### **URL Hash (URL ハッシュ)**

URL をハッシュ値に変換してパーシステンスを行います。同じ URL のリクエストは、同じリアルサーバへ接続されます。

#### **HTTP Host Header (HTTP ホストヘッダー)**

URL 内のホスト値でパーシステンスを行います。同じホストへのリクエストは、同じリアルサーバへ接続されます。

#### **Hash of HTTP Query Item (HTTP クエリーハッシュ)**

URL 内のクエリーキー値をハッシュ値に変換してパーシステンスを行います。同じクエリーキー値のリクエストは、同じリアルサーバへ接続されます。

#### **SSL Session ID (Deprecated) (SSL セッション ID)**

SSL 接続時に、SSL セッション ID でパーシステンスを行います。このオプションは、SSL アクセラレーションを有効させた場合は無効となります。

### **Note-2: 負荷分散方法**

#### **Round Robin (ラウンドロビン)**

ラウンドロビンは、セッションをリアルサーバへ順番に分配します。例えば、最初のセッションは、リアルサーバ 1 へ、そして次のセッションはリアルサーバ 2 へ分配します。全てのリアルサーバに対して同じ負荷配分が行われます。

#### **Weighted Round Robin (重み付けラウンドロビン)**

この方法では、どのリアルサーバへセッションをアサインするかを、各サーバに与えられた重量により判断します。設定された重量が重いほど、分配されるセッション数が多くなります。

#### **Least Connection** (最小接続)

この方法では、接続数が少ないリアルサーバへセッションが分配されます。

#### **Weighted Least Connection** (重み付け最小接続)

各リアルサーバに設定された重量を基に最小接続数が算出されます。算出された値によりリアルサーバへセッションが分配されます。

#### **Fixed Weighting** (固定重み)

一番重量の大きい稼働中のリアルサーバへ、常にセッションが分配されます。各リアルサーバの重量値は異なっていなければなりません。

#### **Resource base(ptive)** (アダプティブ)

この方法では、リアルサーバへエージェントをインストールし、そのエージェントの測定値によりセッションの分配を行います。この方法では、負荷分配をリアルタイムに均等に行うことが可能です。

#### **Weighted response time**

レスポンスの早いRSの重みを大きくして、その重みに従った負荷配分を行います。

#### **Source IP Hash**

同じIPアドレスを持つクライアントからの全てのアクセスを同じRSへとフォワードします。同じホストから一つ以上のアクセスが同時になっても同じRSへフォワードできます。負荷が偏るケースがあるかも知れません。

### ■ **SSL Properties** (SSL 特性)

Parameters	Description	Default
SSL Acceleration	ロードマスターが、SSL プロトコルの最終地点となります。リアルサーバの暗号化、復号化をロードマスターが代行することによりSSL通信の速度向上が可能となります。	無効
Reencrypt	このオプションは、SSL Acceleration で一旦複合化したパケットを再度暗号化してRSへ送付します。リアルサーバにはSSL証明書のインストールが必要です。	
Certificate	“Add New” : 新しいSSL証明書をインストールする時にクリックします。 “Add 3 <sup>rd</sup> Party Cert” : 新しいインターミディエート証明書(ルート証明書)をインストールする時にクリックします。	なし

	注：このパラメータは、“SSL Acceleration”をオンにした時のみ表示されます。	
Rewrite Rules	RS からのリダイレクトを行う URL ロケーションが異なるプロトコル (HTTP/HTTPS) を一つに統一要求する必要がある場合は、このプルダウンリストで選択します。	None
Client Certificates	ユーザ用 SSL 証明書を使用する時に設定を変更します。	No Client Certificate

### ■ Advanced Properties (アドバンスド特性)

Parameters	Description	Default
Content Switching	コンテンツスイッチを使用できるようにします。	無効
HTTP Header Modifications	HTTP ヘッダールールを変更できます。	無効
Enable Caching	RS のコンテンツのキャッシングを可能にします。	無効
Enable Compression	クライアントとの通信パケット圧縮を可能にします。	無効
Detect Malicious Requests	RS への悪意のあるリクエストをブロックします。	無効
Add Header to Request	任意の HTTP ヘッダーを RS へのリクエスト内に挿入します。	無効
Not Available Server (使用可能サーバなし)	リアルサーバが全て使用不可能な場合のバックアップサーバの設定を行います。IP アドレスだけが指定可能です。	なし
Not Available Redirection Handling (N/A リダイレクト処理)	コンテンツが無効な場合のリダイレクト処理を設定します。HTTP から HTTPS への強制は、エラーコード 302 を選択し、'https://<host+domain>%s'をリダイレクト URL に指定します。	なし
Default Gateway	システムに設定してあるデフォルトゲートウェイ以外のデフォルトゲートウェイを指定できます。	なし
Service Specific Access Control	VS 毎のアクセスコントロールを設定出来ます。	なし

### ■ ESP Options

このオプションについては、  
<http://kemptechnologies.com/files/downloads/documentation/7.0/Fea>

[ture Description/Feature Description-ESP.pdf](#) を参照下さい。

### 4.3.2 リアルサーバの設定

1. 仮想仮想サービス特性画面で、下の方に位置する **Real Servers** をクリックします。新しく開かれる **Real Servers** 下の[Add New ...] ボタンをクリックします。

2. リアルサーバの IP アドレスを入力します。また、必要ならば、ポート番号を変更します。

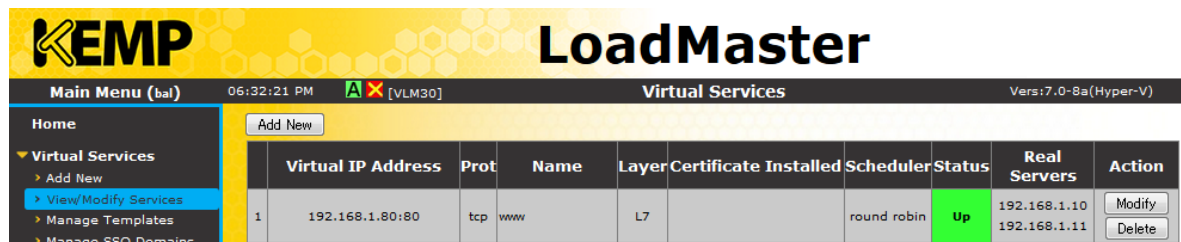
3. もし、ネットワーク形態が1アームで、ダイレクト・サーバ・リターン (DSR) を使用するならば、“**Forwarding method**”を ‘**Directreturn**’ にします。それ以外は ‘**nat**’ のままにしてください。
4. もし、負荷分散方式を重み付けとする場合は、“**Weight**” の値をデフォルト値の “1000” を他の値へ変更してください。関連する重み付け負荷分散方式には “**Weighted Round Robin**”, “**Weighted Least Connection**”、もしくは “**Fixed Weight**” のオプションがあります。
5. リアルサーバの入力を有効にするために [**Add This Real Server**] ボタンをクリックします。

上記 1 – 5 の手順に従い、全てのリアルサーバを設定してください。

注：ローカルのサブネット上に存在しないリモートサーバをリアルサーバ（RS）として登録する場合は、“System Configuration” → “Miscellaneous Options” → “Network Options” 下にある “Enable Non-Local Real Servers” を ‘Yes’ にした後、このリアルサーバ追加画面に新たに表示される “Allow Remote Addresses” をオンにします。仮想仮想サービス（VS）は、非透過モードでなければこのパラメータは表示されません。

### 4.3.3 仮想仮想サービスの状態確認

仮想仮想サービスにリアルサーバの登録を終えたら、“Virtual Service” メニューの “View/Modify Services” より状態を確認します。下図のように Status が Up になっていれば、仮想仮想サービス経由でリアルサーバへのアクセスが可能です。

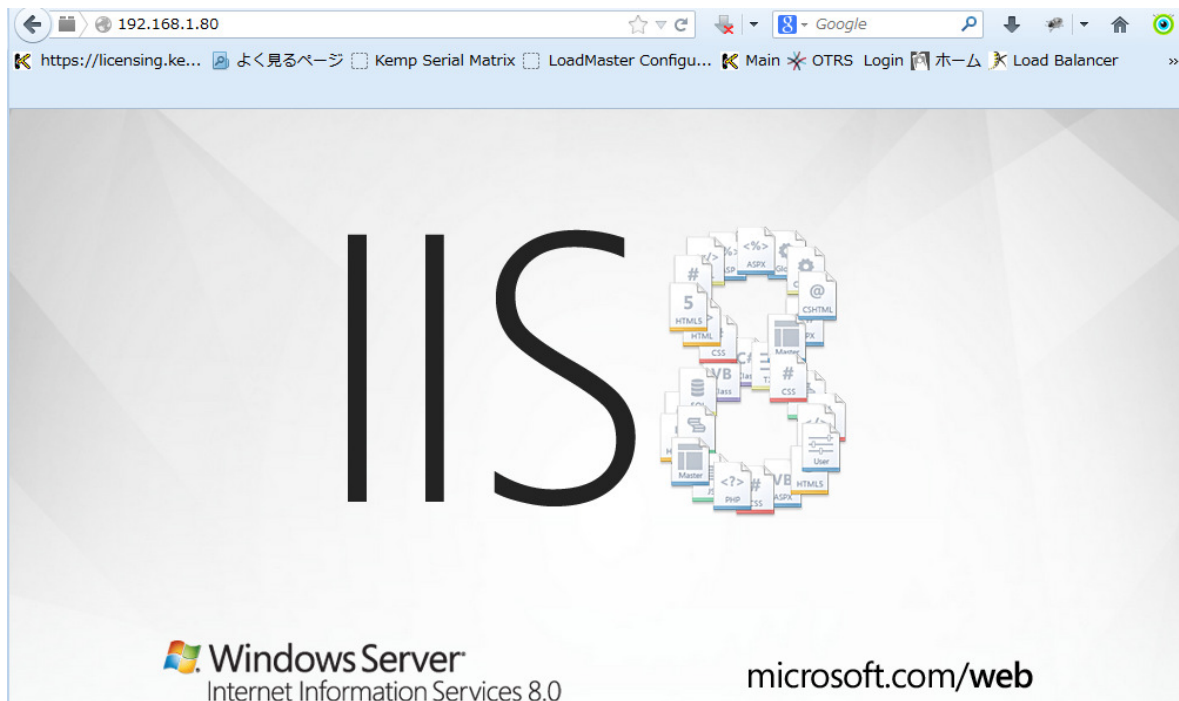


	Virtual IP Address	Prot	Name	Layer	Certificate	Installed	Scheduler	Status	Real Servers	Action
1	192.168.1.80:80	tcp	www	L7			round robin	Up	192.168.1.10 192.168.1.11	Modify Delete

### 4.3.4 仮想仮想サービス／リアルサーバへのアクセス

ブラウザを開いて、作成した仮想仮想サービスへアクセスを試みます。

例えば下図のように、リアルサーバから応答があれば設定は完了です。



## 5 透過、それとも非透過モード

### 5.1 ネットワーク構成

ロードバランサーを実際のプロダクション環境に展開する場合、多種多様なネットワーク構成に絡んだ問題が発生する場合があります。その中でも、一番厄介なのはリアルサーバそのものに影響するものです。このセクションでは、最も共通した問題を解決する手がかりとなる事項とロードマスターの設置方法の手助けとなるオプションについて説明します。

これらの問題の中で、共通した、且つ、把握することが難しいのがレイヤー7の透過に絡んだ問題です。このセクションでは、ネットワークの透過に焦点を当てて、どのように設定を行うかを説明すると共に関係するコンセプトについて説明します。

#### ■ ネットワーク透過の実装

ネットワーク透過の全ての問題は、単一の質問に集約できると言っても過言ではありません。それは；

サーバのアクセスログに、クライアントのIPアドレスが必要ですか？

もしその答えが“はい”ならば、ネットワーク透過の設定が必要で、ネットワークの構成をそれに合ったものにしなければなりません。

もしその答えが“いいえ”なら、ネットワークの設定がより柔軟に行えます。

以下は、ネットワーク透過、非透過モードの長所、短所を述べたものです。

	透過モード	非透過モード
長所	<ul style="list-style-type: none"> <li>クライアント・ソース IP アドレスをそのまま保てる</li> <li>レイヤー4と7の両方で使用できる</li> </ul>	<ul style="list-style-type: none"> <li>リアルサーバのあるサブネットよりサービスへのアクセスが可能</li> <li>デフォルト・ゲートウェイの変更が不要</li> </ul>
短所	<ul style="list-style-type: none"> <li>リアルサーバのあるサブネットから、サービスへのアクセスができない</li> <li>デフォルト・ゲートウェイは、ロードマスターでなければならない</li> </ul>	<ul style="list-style-type: none"> <li>クライアント・ソース IP アドレスをそのまま保てない</li> <li>レイヤー7でのみ有効</li> </ul>

ロードマスターを介してリアルサーバがどのようにトラフィックをクライアントに正しく戻すかは、透過、非透過モードで異なります。ロードマスターに入ってきたトラフィックが同じルートを通して如何にクライアントに戻すかは、ロードバランサーの基本的な必須機能です（ダイレクト・サーバ・リターンは、唯一の例外です）。

#### ■ レイヤー4とレイヤー7

ロードマスターの処理は、レイヤー4とレイヤー7では異なります。レイヤー4とレイ  
ロードマスターズシリーズ クイック・スタート・ガイド

ヤー7を OSI モデルで見てください。レイヤー4は、TCP/UDP ポートが絡むだけですが、レイヤー7は、HTTP プロトコルで使用されるクッキー、SSL アクセラレーション、コンテンツスイッチなどのアプリケーションスイッチとしての要素が絡みます。

レイヤー4として作成された全ての仮想仮想サービスは、透過モードのネットワークとしてのみ動作します。レイヤー4の意味は何でしょうか？それは、セッションの維持にクッキーを使って行ったり、コンテンツスイッチ、もしくはコンテンツスイッチのルール、及び SSL アクセラレーションなどが絡まない負荷分散のトラフィックです。レイヤー4では、ソース IP アドレスを使ったセッション維持のみが行えます。

仮想仮想サービスが、レイヤー4なのかレイヤー7かは **Virtual Services** サブメニュー下の **“View/Modify Services”** を選択して仮想仮想サービス・リストを表示させると、下記のように **“Layer”** 欄で識別可能です。

	Virtual IP Address	Prot	Name	Layer	Certificate Installed	Scheduler	Status	Real Servers	Action
1	192.168.1.80:80	tcp	www	L7		round robin	Up	192.168.1.10 192.168.1.11	Modify Delete
2	192.168.1.80:443	tcp	DA	L4	on Real Server	round robin	Down	192.168.1.10 192.168.1.11	Modify Delete
3	192.168.1.81:443(+2)	tcp	Lync Director	L7	on Real Server	round robin	Up	192.168.1.14 192.168.1.15	Modify Delete
4	192.168.1.81:5061	tcp	Lync Internal Director SIP	L7		round robin	Up	192.168.1.14 192.168.1.15	Modify Delete

もし、現在のモードを変更したければ、下記のように各仮想仮想サービスの属性画面の **Standard Properties** にある **“Force L7”** を使用します。もし、このパラメータが表示されている場合、その仮想仮想サービスは現在レイヤー4として稼働していることとなります。そして、ネットワークは透過モードです。もし、仮想仮想サービスが何らかのクッキーを使用したセッション維持、SSL アクセラレーション、もしくはコンテンツスイッチを使用していると、自動的にレイヤー7となり、この **“Force L7”** のパラメータは表示されません。

Standard Options	
Force L7	<input type="checkbox"/>
Transparency	Enabled
Extra Ports	<input type="text"/> <input type="button" value="Set Extra Ports"/>
Persistence Options	Mode: <input type="text" value="Source IP Address"/> Timeout: <input type="text" value="6 Minutes"/>
Scheduling Method	<input type="text" value="round robin"/>
Use Address for Server NAT	<input type="checkbox"/>

## 5.2 透過モードの要求

ネットワークを透過モードにする場合は、仮想仮想サービスに属するリアルサーバのゲートウェイの設定をロードマスターとしなければなりません。これは、ネットワーク形態が1アームであろうが2アームであろうが変わりません。ロードマスターがデフォルトゲートウェイでなければ、サーバがクライアントへのレスポンスを返すときにロードマスターへのパスが保障されずに、ロードバランサーとしての働きが出来ません。

ネットワークを透過モードとして働かせるためには、更にクライアントがリアルサーバの

ロードマスターズシリーズ クイック・セットアップ・ガイド

© 2014 KEMP Technologies Inc.

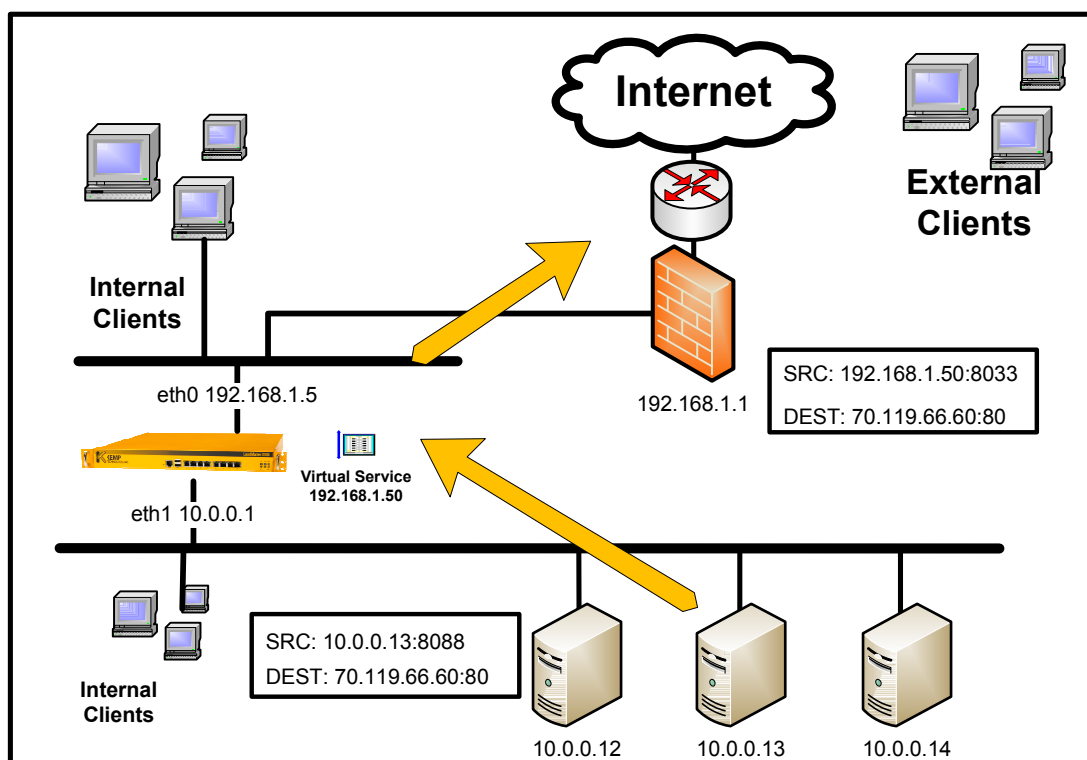


接続されているサブネット以外からアクセスする必要があります。これは、上記で述べたようにトラフィックの出と入りがロードマスターを通過する必要があるからです。もし、クライアントがリアルサーバと同じサブネット上に存在し、ネットワークが透過モードとなっていると、リアルサーバからの返りのパケットはロードマスターを介さずクライアントに直接戻ってしまいます。クライアントは仮想仮想サービスからのレスポンスを待っているにもかかわらず、リアルサーバからのパケットが返ってくるので、結果としてそのパケットは無視されます。

### 5.2.1 ネットワーク透過、SNAT、1アームネットワーク

もし、仮想仮想サービスとリアルサーバが同じサブネット上に存在する1アームでのネットワークを構築し、そして透過モードを採用した場合は、SNAT (Source NAT) を無効にする必要があります。

SNAT は、ネットワークを2アームで構成した場合、プライベートネットワーク上にあるリアルサーバからインターネットへの接続を可能にするメカニズムです。オフィスで使用しているファイヤーウォールと同じような働きをし、あたかもパブリック IP アドレスから接続されたように振舞います。



1アームのネットワーク構成では、SNAT は必要ありませんし、通常の実運用でSNAT が絡んでくるような状態にはなりません。逆にネットワークが透過モードでSNAT が有効になっており、リアルサーバのデフォルト G/W がロードマスターに設定されている場合、インターネット上のクライアントからリアルサーバに直接アクセスしても接続が失敗してしまいます。これは、ロードマスターがリアルサーバからの返りのパケットのソース IP アドレスを、仮想仮想サービスのアドレスに変えてしまうからです。従い、SNAT は1

アームネットワークでは無効にしておかなければなりません。

## 5.2.2 非透過モード

非透過モードは、下記の2つの利益を与えてくれます。

- リアルサーバと同じサブネットより、サービス（仮想仮想サービス）へのアクセスが可能。
- 1アームでのネットワーク構成の場合、リアルサーバのデフォルト G/W をロードマスターにしなくてもよい。これは、トラフィックがもしロードマスターから来た場合は、ロードマスターがソース IP アドレスを仮想仮想サービスのアドレスに変換していることで、必ずロードマスターへ返るようになるからです。

不利益としては、ロードマスターがソース IP アドレスを仮想仮想サービス IP アドレスに書き換えるために、クライアントからのソース IP アドレスがリアルサーバへ届かないことです。

非透過モードは、レイヤー7でのみしか動作しません。もし、クッキーによるパーシステンスや、コンテンツスイッチ、もしくは SSL アクセラレーションを使用しない仮想仮想サービスを作成すると、レイヤー4の透過モードになります。非透過モードに変更したい場合は“Force L7”で強制的にレイヤー7にしなければなりません。

反対にクッキーによるパーシステンス、コンテンツスイッチ、もしくは SSL アクセラレーションの何れかを使用している仮想仮想サービスは、自動的にレイヤー7になり、“force L7”のパラメータは表示されません。

### ■ HTTP ヘッダーによる X-ClientSide/ X-Forwarded-For

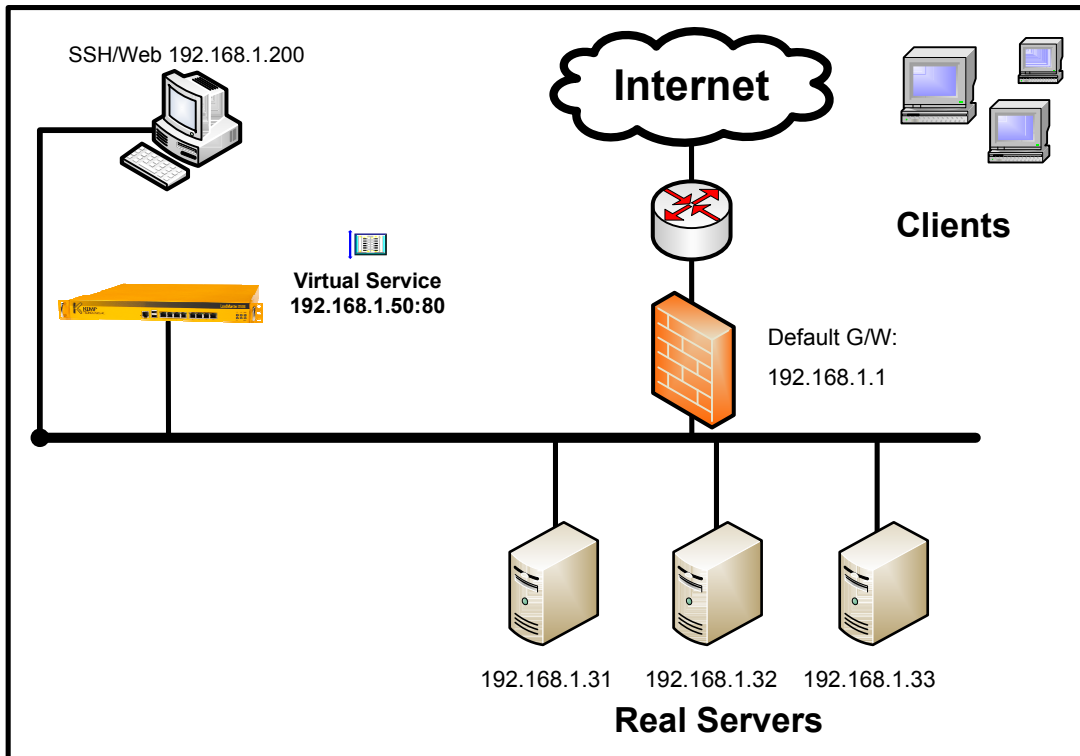
透過モードでは、クライアントの IP アドレスをソース IP アドレスとして保てないことは既に説明をしました。しかし、クライアント IP アドレスを HTTP ヘッダーより取り出せることはまだ説明していません。

1. ロードマスターは、デフォルト設定として、もし仮想仮想サービスがレイヤー7で尚且つ非透過モードの場合、HTTP GET リクエストをリアルサーバに送出するときに、HTTP ヘッダー内に **X-ClientSide** というロードマスター専用ヘッダーを追加します。非透過モードで、どうしてもクライアントの IP アドレスがログとして必要ならば、この **X-ClientSide** ヘッダーを使ってログに出力するように出来ます。又、**X-ClientSide** に代わり、一般的な **X-Forwarded-For** を HTTP ヘッダー内に挿入することも可能です。

## 6 ネットワーク透過設定

### 6.1.1 ネットワーク透過

ネットワークを透過モードに設定するには、まず、対応する仮想仮想サービスに所属するリアルサーバ全てのデフォルト G/W をロードマスターにしなければなりません。次に、下記のステップに従って仮想仮想サービスを設定します。



1. 上記、説明用構成図に沿った仮想仮想サービスを、このガイドの「6.3 仮想仮想サービス作成」に従って作成します。**Virtual Services** サブメニュー下の**“View/Modify Services”**より見た結果は、下記のようなになるはずです。

1	192.168.1.50:80	tcp	L7	round robin	Up	192.168.1.31 192.168.1.32 192.168.1.33	Modify	Delete
---	-----------------	-----	----	-------------	----	--	--------	--------

2. 仮想仮想サービスはレイヤー7 で作成され、ネットワーク透過モードとなります。
3. この仮想仮想サービスの属性を変更するために、上記の仮想仮想サービス一覧画面で対応する仮想仮想サービスの**“Modify”** ボタンをクリックします。

Basic Properties	
Service Name	www <input type="button" value="Set Nickname"/>
Alternate Address	<input type="text"/> <input type="button" value="Set Alternate Address"/>
Service Type	HTTP/HTTPS
Activate or Deactivate Service	<input checked="" type="checkbox"/>

Standard Options	
Force L7	<input checked="" type="checkbox"/>
Transparency	<input checked="" type="checkbox"/>
Extra Ports	<input type="text"/> <input type="button" value="Set Extra Ports"/>
Persistence Options	Mode: None
Scheduling Method	round robin
Idle Connection Timeout (Default 660)	<input type="text"/> <input type="button" value="Set Idle Timeout"/>
Use Address for Server NAT	<input type="checkbox"/>
Quality of Service	Normal-Service

SSL Properties  
 Advanced Properties  
 ESP Options  
 Real Servers

4. デフォルトでは、L7 の透過モードですので、透過モードにするために “L7 Transparency” パラメータのチェックマークを抜きます。

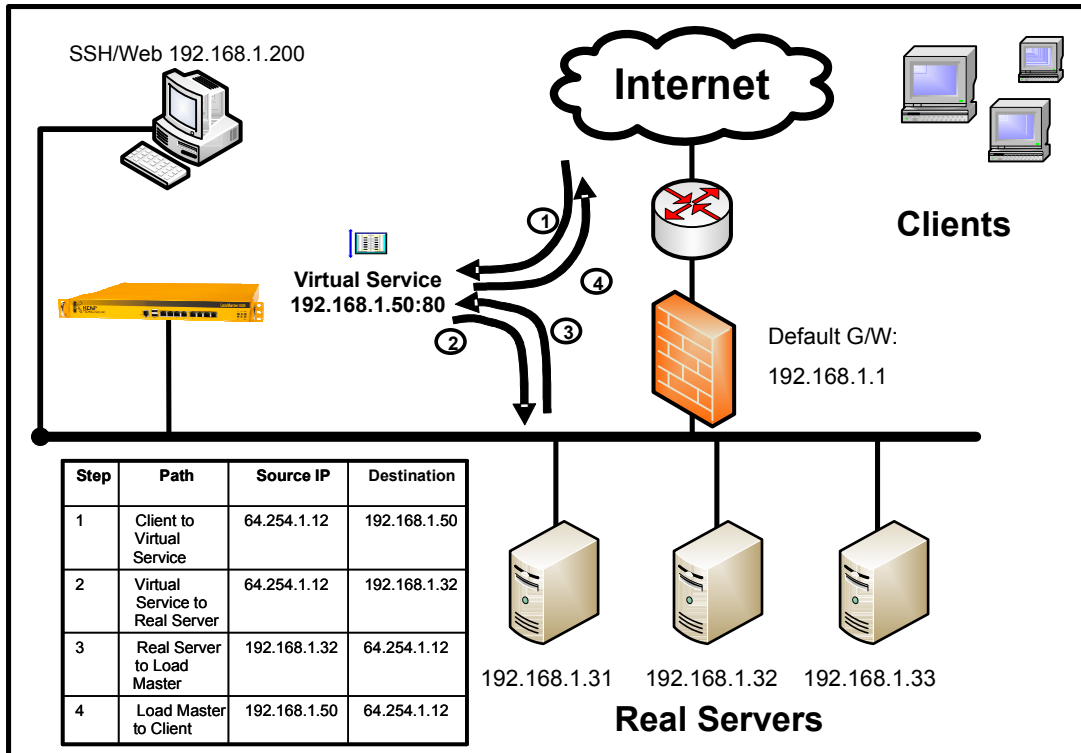
## リアルサーバと同じサブネットよりサービスにアクセスできない理由は何でしょう？

上記の仮想仮想サービスを透過モードに設定すると、サービスへのアクセスがリアルサーバと同じサブネットのクライアントよりできない理由は、トラフィックフローの問題にあります。前にも述べたように、ロードマスターが負荷分散としての役目を果たすには、トラフィックの入りと出が同じパスを通る必要があります。

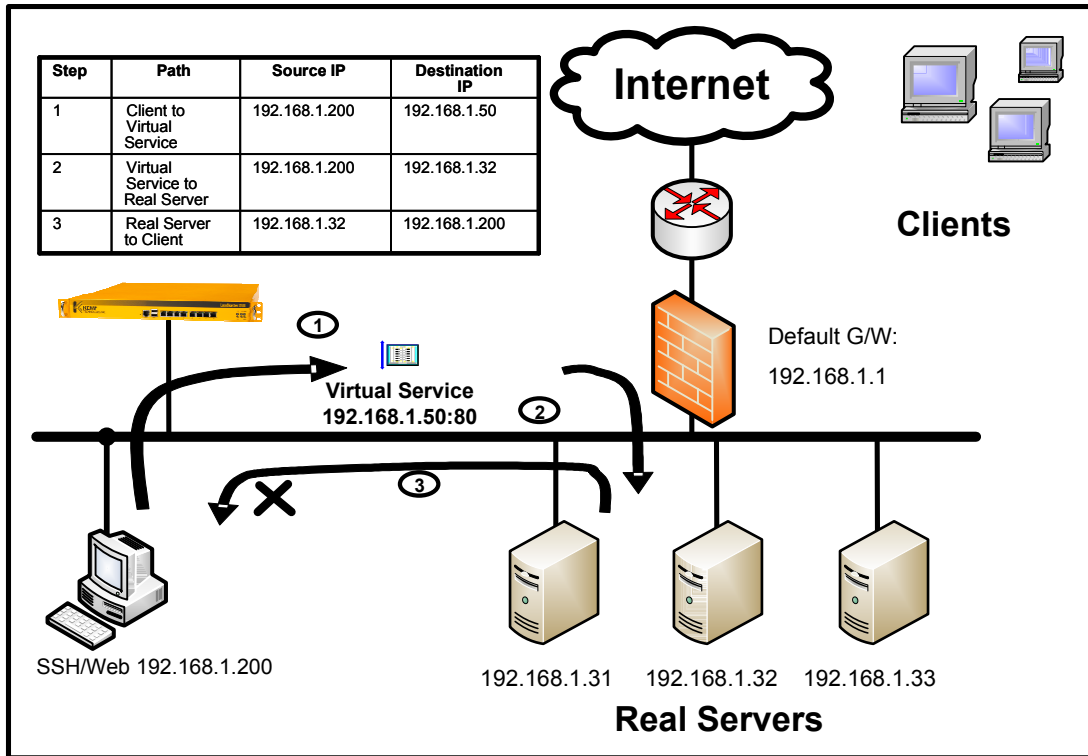
負荷分散装置は、通常下記のステップを踏みます。

1. クライアントよりロードマスターの仮想仮想サービスへ
2. ロードマスターよりリアルサーバへ
3. リアルサーバよりロードマスターへ
4. ロードマスターよりクライアントへ

下図の 1 アームネットワーク構成の例を見てみましょう。クライアント IP アドレスは 64.254.1.12, 仮想仮想サービスは 192.168.1.50, そしてリアルサーバは 192.168.1.32 です。ソース IP アドレスと行き先 IP アドレスの変換について順を追ってみてください。クライアントが、リアルサーバ以外のネットワークからアクセスすると何の問題もありません。



では、同じネットワーク構成を使って、クライアントがリアルサーバと同じサブネット内の IP アドレスである **192.168.1.200** の場合を下図で見てください。この場合は、3 番目のフローは上図とは異なります。これは、クライアントが同じサブネット上に存在するために、リアルサーバはパケットを直接クライアントへ送り返します。クライアントは、レスポンスがロードマスターより返ってくることを期待していますので、このパケットは無視してしまいます。よって、リアルサーバより送られてきた情報は破棄されてしまいます。



### 6.1.2 非透過モード

このモードに設定する場合は、リアルサーバのデフォルト G/W はそのままとします (1 アームでは)。デフォルト G/W は、ルータ、もしくはプロキシサーバとなっているはず。そして、下記のステップに沿って仮想仮想サービスを作成します。

1. 上記、説明用構成図に沿った仮想仮想サービスを、このガイド内「6.3 仮想仮想サービス作成」に従って作成します。Virtual Services サブメニューの“View/Modify Services”より見た結果は下記のようなになるはず。

9	192.168.3.50:80	tcp	L7	round robin	Up	192.168.3.90 192.168.3.91 192.168.3.92	Modify Delete
---	-----------------	-----	----	-------------	----	--	------------------

2. ロードマスターは、デフォルトではレイヤー7の透過モードで仮想仮想サービスを作成します。

The image shows two configuration panels. The top panel, titled 'Basic Properties', includes fields for 'Service Name' (www), 'Alternate Address', 'Service Type' (HTTP/HTTPS), and an 'Activate or Deactivate Service' checkbox which is checked. The bottom panel, titled 'Standard Options', includes 'Force L7' (checked), 'Transparency' (checked), 'Extra Ports', 'Persistence Options' (Mode: None), 'Scheduling Method' (round robin), 'Idle Connection Timeout (Default 660)', 'Use Address for Server NAT' (unchecked), and 'Quality of Service' (Normal-Service). Below these are expandable sections for 'SSL Properties', 'Advanced Properties', 'ESP Options', and 'Real Servers'.

- この仮想仮想サービスを、非透過モードにするためには、“L7 Transparency”のチェックマークを抜きます。
- 非透過モードでは、HTTP ヘッダーにクライアントの IP アドレスを挿入させることが可能です。そのためには、VS を真の L7 モードにするためにパーシステンシー方式にクッキーを使用するように設定しなければなりません。下図の例では、パーシステンシーを Active Cookie モードに設定しています。

The image shows the 'Persistence Options' configuration panel. It includes a 'Mode' dropdown menu set to 'Active Cookie', a 'Timeout' dropdown menu set to '6 Minutes', and a 'Cookie name' input field with a 'Set Cookie' button.

- System Configuration サブメニューの“Miscellaneous Options”を選択します。その中にある“L7 Configuration”をクリックすると、下記のような画面が表示されます。

The image shows the 'Miscellaneous Options' configuration panel. It includes several checkboxes: 'Allow connection scaling over 64K Connections', 'Always Check Persist', 'Add Port to Active Cookie', 'Conform to RFC' (checked), 'Close on Error', 'Add Via Header In Cache Responses', 'Real Servers are Local', 'Drop Connections on RS failure', and 'Drop at Drain Time End'. It also includes input fields for 'L7 Connection Drain Time (secs)' (300) and 'Least Connection Slow Start' (0), both with 'Set Time' and 'Set Slow Start' buttons. There are also dropdown menus for 'Additional L7 Header' (X-ClientSide) and '100-Continue Handling' (RFC Conformant).

- “Additional L7 Header”を“X-ClientSide”もしくは“X-Forwarded-For”に設定してください。

注：もしクライアント IP アドレスの挿入が不要ならば、“None”を選択します。

7. リアルサーバのアクセスログにクライアントの IP アドレスが挿入されることを確認します。下図は、Client として 192.168.1.30 を使用して VS の 192.168.3.50 にアクセスした例です。





の内容が追加されている。

```

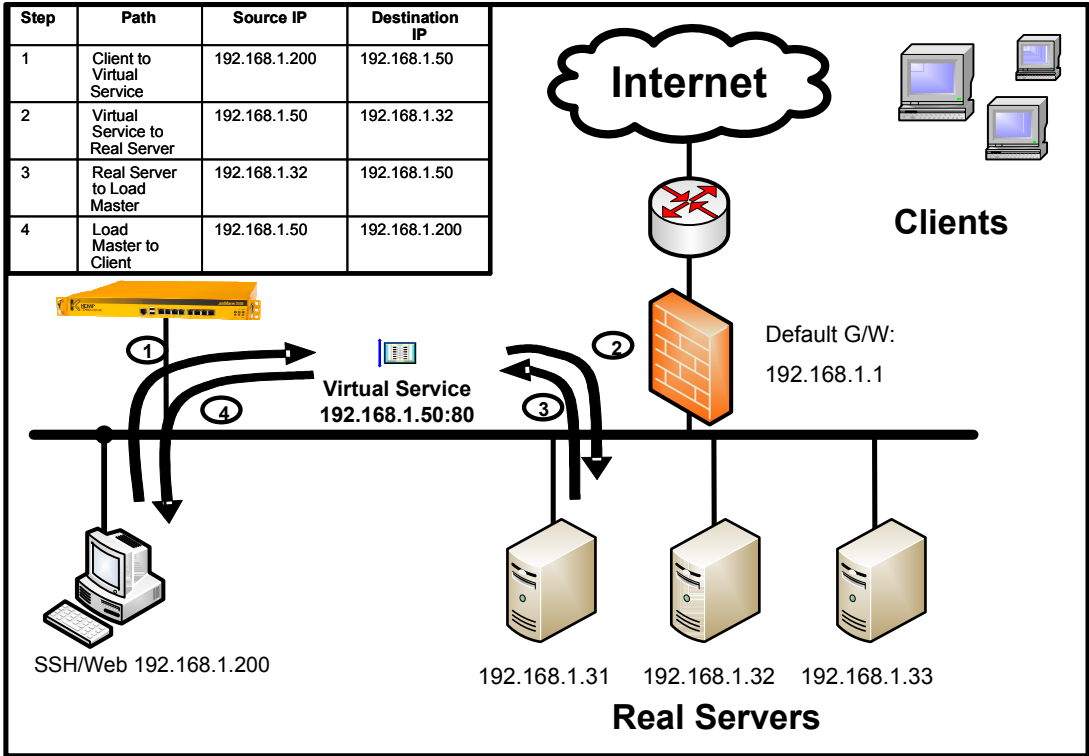
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:49 +0900] "GET /favicon.ico HTTP/1.1" 404 363 "http://192.168.3.50/2kb.html" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.102 -- [02/Jul/2008:12:13:50 +0900] "HEAD / HTTP/1.0" 302 - "-" "-"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:50 +0900] "GET /2kb.html HTTP/1.1" 200 2204 "-" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:50 +0900] "GET /favicon.ico HTTP/1.1" 404 363 "http://192.168.3.50/2kb.html" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:50 +0900] "GET /2kb.html HTTP/1.1" 200 2204 "-" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:50 +0900] "GET /favicon.ico HTTP/1.1" 404 363 "http://192.168.3.50/2kb.html" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:50 +0900] "GET /2kb.html HTTP/1.1" 200 2204 "-" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:51 +0900] "GET /favicon.ico HTTP/1.1" 404 363 "http://192.168.3.50/2kb.html" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:51 +0900] "GET /2kb.html HTTP/1.1" 200 2204 "-" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:51 +0900] "GET /favicon.ico HTTP/1.1" 404 363 "http://192.168.3.50/2kb.html" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:51 +0900] "GET /2kb.html HTTP/1.1" 200 2204 "-" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:51 +0900] "GET /favicon.ico HTTP/1.1" 404 363 "http://192.168.3.50/2kb.html" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:51 +0900] "GET /2kb.html HTTP/1.1" 200 2204 "-" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:52 +0900] "GET /favicon.ico HTTP/1.1" 404 363 "http://192.168.3.50/2kb.html" "Opera/9.50 (Windows NT 5.1; U; en)"
192.168.3.50 192.168.1.30 -- [02/Jul/2008:12:13:52 +0900] "GET /2kb.html HTTP/1.1" 200 2204 "-" "Opera/9.50 (Windows NT 5.1; U; en)"

```

非透過モードでは、ロードマスターがリアルサーバからのレスポンスを自分に必ず返してくるように、ソース IP アドレスを自分の IP アドレス (VIP) に変換してリアルサーバに転送します。よって、リアルサーバは、必ずレスポンスをロードマスターに返し、ロードマスターはそのレスポンスをクライアントへ転送します。

透過モードでは宛先 IP アドレスがロードマスターにより変換されます。しかしながら、下図の非透過モードでは、ソース IP アドレスもロードマスターにより変換されています (パケット 2)。これが、非透過モード時にロードマスターの IP アドレス (VIP) しかログに残らない理由です。下図は、1 アーム構成時に、クライアントが VS と同じサブネットに存在する場合の VS へのアクセス時の一連の IP アドレスの変換を表しています。

1. クライアントが VS にアクセス (192.168.1.200 より 192.168.1.50 にアクセス)。
2. ロードマスターが、RS の一つである 192.168.1.32 にリクエストを転送。(ソース IP が、VIP に変換)
3. RS がロードマスターにレスポンスを送信。
4. ロードマスターがクライアントにレスポンスを転送。



END