8 Module 8– ダイレクト･サーバ･リターン (DSR)

8.1 ダイレクト･サーバ･リターン

レッスン目標：

このレッスンを通して、ロードマスターのダイレクト･サーバ･リターン機能がどのように働き、又、どのように設定するのかを習得します。

8.1.1 ダイレクト･サーバ･リターン概念

ダイレクト･サーバ･リターン（DSR）とは、インバウンドのトラフィックはロードマスター経由で、アウトバウンドトラフィックはロードマスターを経由しない方法です。DSR を使用する一番のアドバンテージは、ロードマスターが負荷分散のためにインバウンドのトラフィックのみを ハンドルするだけで良いと言う点です。サーバは、ロードマスターを介さずに直接レスポンスをクライアントへ返します。

もし、あるトラフィックの特徴として、一つのパケットが入ってきて、その応答として 8 つのパケットが出て行く場合には、DSR を使用することで８７％のトラフィックをロードマスターはハンドリングしなくて良い事になります。

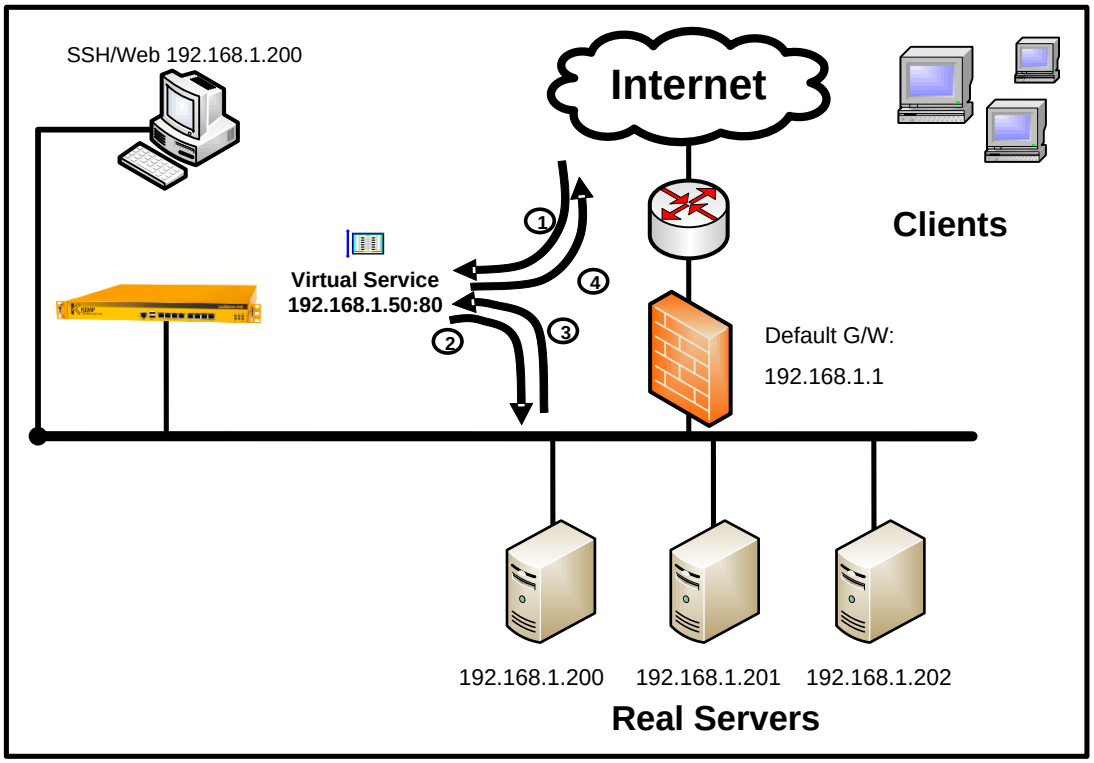
DSR の短所

DSR 機能を使用する前に、幾つかの欠点を知っておく必要があります。

- DSR はセットアップが複雑です。リアルサーバ側で高度な設定変更が要求され、働くためにウェブサービスが稼動している必要があります。
- DSR は、レイヤ 4 のみのバーチャルサービスでしか働きません。理由として、ロードマスターへサーバからのレスポンスが帰ってこないために、クッキーやコンテントスイッチなどのレイヤ 7 機能を働かせることが出来ないからです。

8.1.2 DSR はどのように働くか

DSR でないモードでは、ソース IP アドレスと、もしくは宛先 IP アドレスを書き換える NAT 技術を使用して働き、DSR は MAT（MAC アドレス･トランスレーション）を使用して働きます。 DSR ではないモードでは、ロードマスターはサーバのレイヤ 2 である MAC アドレスへ、サーバの IP アドレスを使ってトラフィックを導きます。

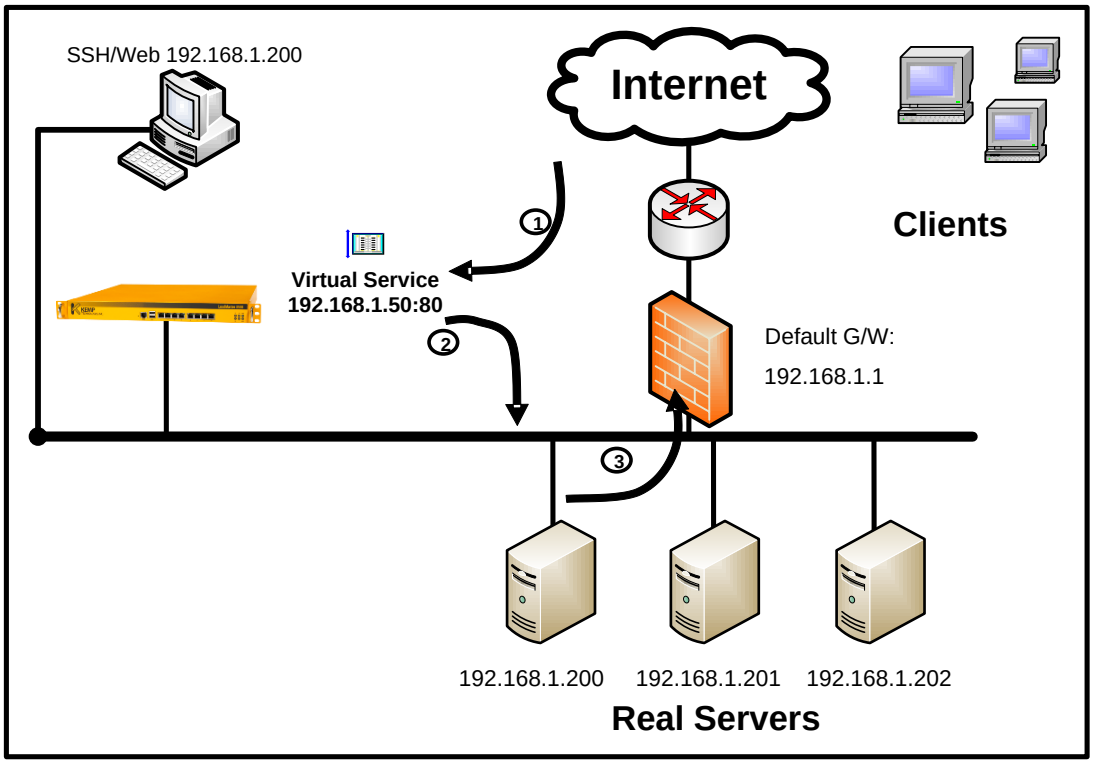


参照図－１：DSR ではないモード

Step	Source Address	Destination Address
1	70.119.66.60 (Router MAC)	192.168.1.50 (Load Master MAC)
2	192.168.1.50 (Load Master MAC)	192.168.1.201 (Server MAC)
3	192.168.1.201 (Server MAC)	192.168.1.50 (Load Master MAC)
4	192.168.1.50 (Load Master MAC)	70.119.66.60 (Router MAC)

参照テーブル１：DSR ではないモードの接続

DSR モード（参照図―２）では、サーバはソース IP アドレスをバーチャルサービスとしてクライアントへ応答を返します。



参照図―２ ： DSR

Step	Source Address	Destination Address
1	70.119.66.60 (Router MAC)	192.168.1.50 (LoadMaster MAC)
2	**70.119.66.60 (Router MAC)**	**192.168.1.50** (Server MAC)
3	192.168.1.50 (Server MAC)	70.119.66.60 (Router MAC)

参照テーブル２ ：DSR 接続

ロードマスターは、上の図－２の 2 番目のパケットで示しているようにバーチャルサービスの IP アドレスへトラフィックを送信しますが、MAC アドレスはサーバのものです。サーバは、IP アドレスの衝突を防ぐために、ARP クエリーに対して応答しないようにバーチャルサービス用 IP アドレスを設定しおり、IP アドレスがサーバの MAC アドレスに関連しているために、そのトラフィックを受け付けます。

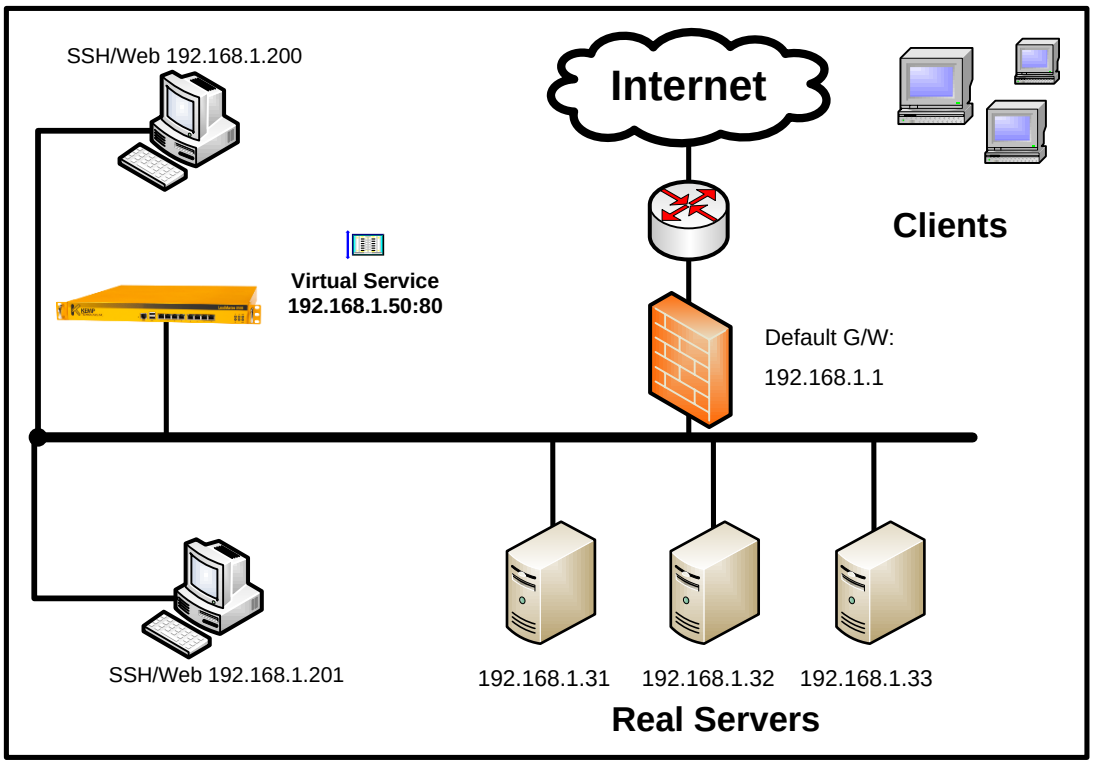
ここで重要なポイントは、サーバが応答した時にバーチャルサービスの IP アドレスをソース IP アドレスに使うことです。これにより、トラフィックは、ロードマスターをバイパスしてクライアントへ直接送信されますが、クライアントは、あたかもロードマスターからの応答のようにそのトラフィックを受け付けます。

8.2 DSR の設定

レッスン目標：

このレッスンを通じて、ロードマスターのダイレクト·サーバ·リターン（DRS）とそれに関連するリアルサーバ側の設定方法を習得します。宛先 IP アドレスとしてバーチャルサービス IP アドレスを使ってロードマスターからリアルサーバへ来るパケットを許可するために、リアルサーバは、バーチャルサービス IP アドレスをエイリアスとして持つ必要があります。

実習環境のセットアップ：



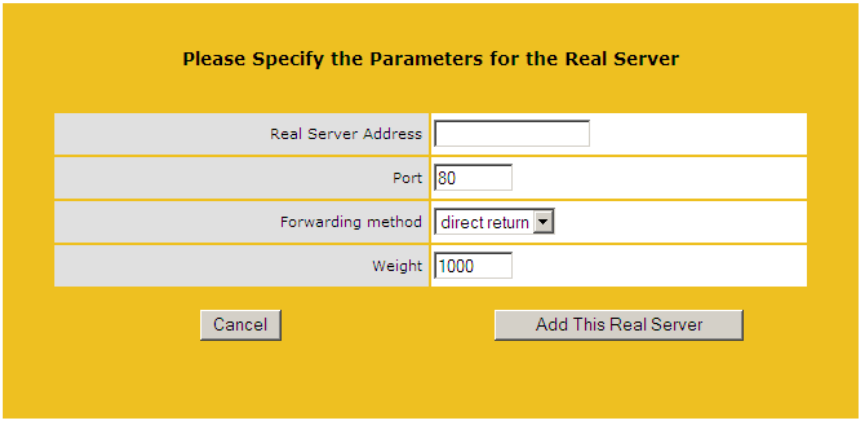
8.2.1　　ロードマスター上の DSR 設定方法

DSR は、バーチャルサービス上にリアルサーバを通して設定されます。DSR として、リアルサーバを 設定するために、**“Forwarding Method”** を通常の **“nat”** ではなく **“directreturn”** とします。もし、リアルサーバが既に設定されている場合は、**“modify”** ボタンより **“Forwarding Method”** を **“nat”** から **“directreturn”** に変更します。もし、選択肢として **“directreturn”** が無い場合は、パーシステンスオプションをチェックします。DSR 設定は、パーシステンスオプションとして **“None”** もしくは、**“Source IP Address”** しか許可していません。

1.バーチャルサービスを作成します。

2.属性画面で、“**Real Server**”セクションの“**Add New**”をクリックします。

3.リアルサーバの IP アドレスを入力し“**Forwarding method**”を“**directreturn**”にします。



4. “**Add This Real Server**”ボタンをクリックします。

8.2.2 リアルサーバ上の DSR 設定方法

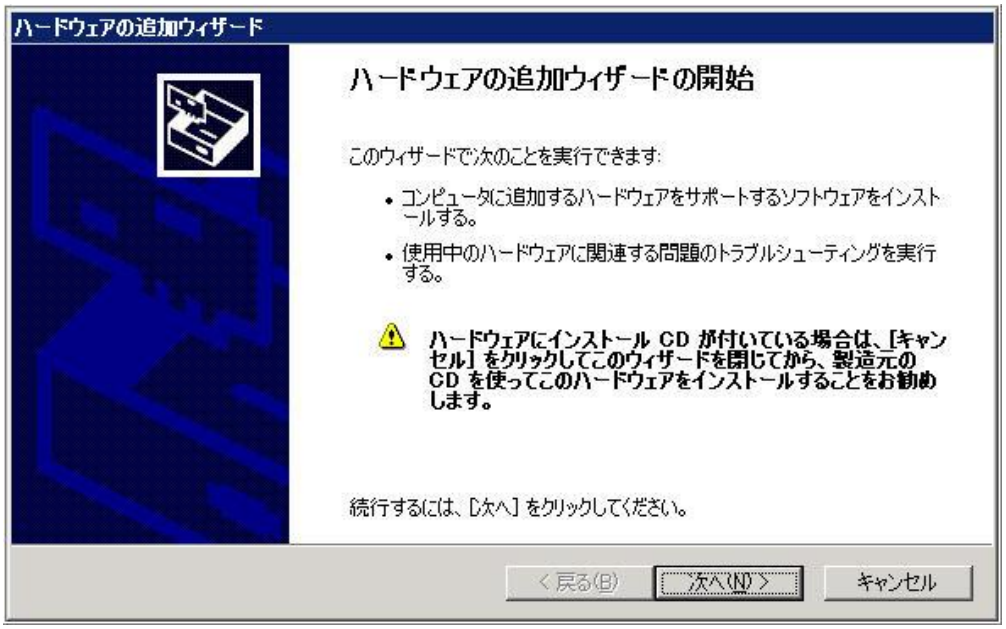
DSR のリアルサーバ側設定は、少し複雑です。DSR がネットワーク側で問題なく動作するためには、クライアントからのリクエストが、ロードマスターを介してバーチャルサービスの IP アドレスを宛先 IP アドレスとするパケットをサーバが受け付けなければなりません。しかし、同じネットワークで一つの IP アドレスを 2 つのデバイスで持つことは出来ません。

この問題は、二つの方法で解決できます。一つは、エイリアスとしてインターフェースへこの IP アドレスを設定する方法です。このインタフェースは、管理上ダウンさせていなければなりません。もう一つの方法は、ループバック･インターフェース上にエイリアスとして設定します。そして、サーバは他のデバイスがバーチャルサービスの IP アドレスを ARP リクエストで問い合わせて来ても、レスポンスを返さないようにしなければなりません。もし、レスポンスを返してしまうと、サービスのリクエストがバーチャルサービスではなく、リアルサーバへ直接送信されてしまうようになってしまいます。

Windows 200/2003 での DSR 設定

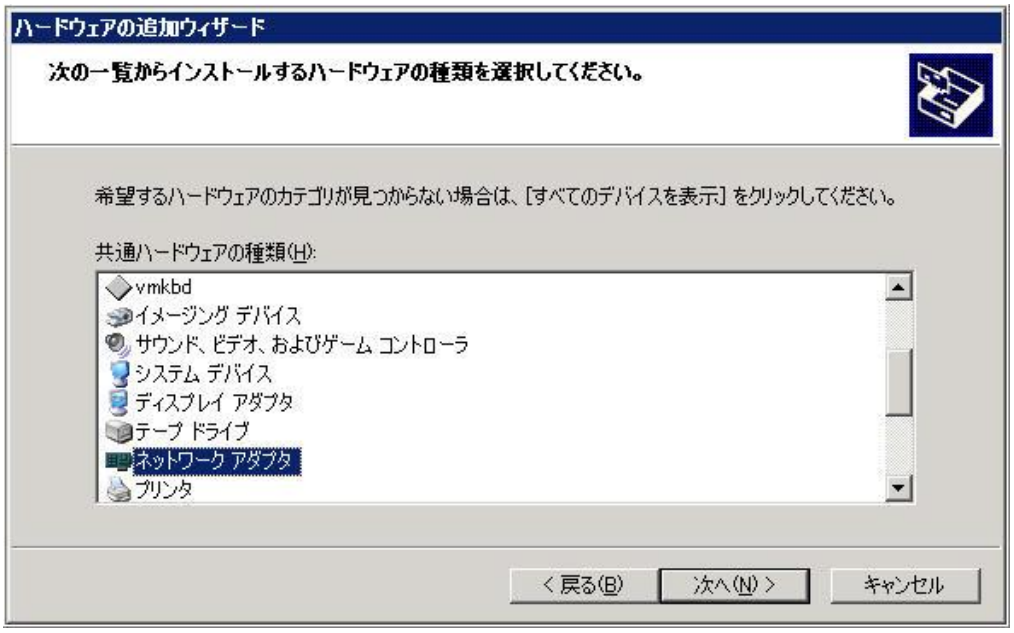
Windows サーバでは、ループバック･アダプタを使用するのが一般的です。ループバックアダプタを設定し、バーチャルサービス IP アドレスをアサインする方法を示します。

1. コントロールパネルの“ハードウェアの追加”を選択します。

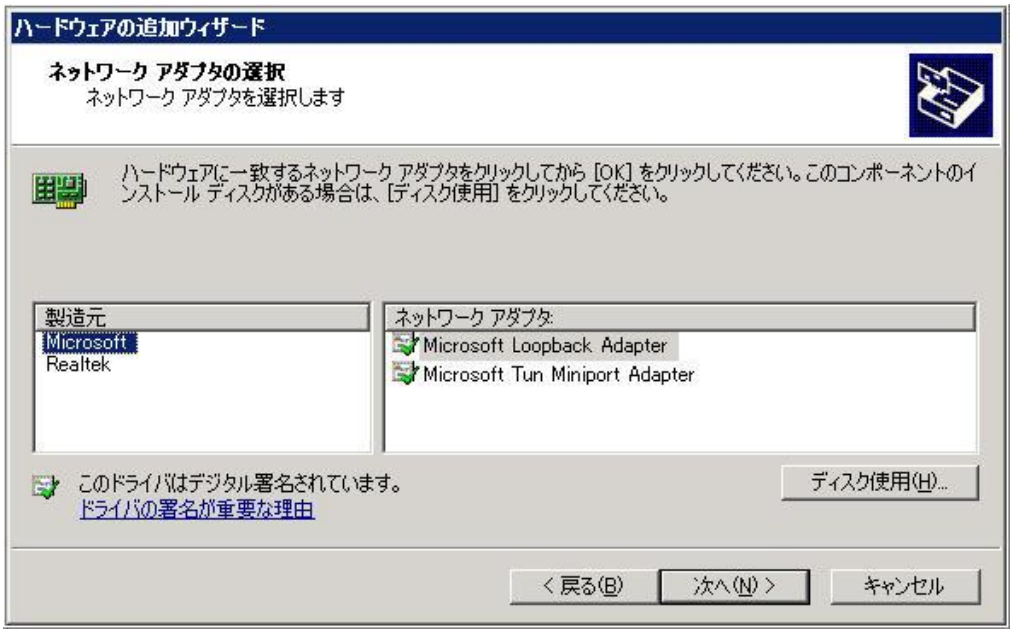


2. “次へ”をクリックすると、ウィザードは新しいハードウェアを探します。そして、“既にこのハードウェアをコンピュータに接続していますか？”と問い合わせてきます。“はい、――”を選択し“次へ”をクリックします。ハードウェアのリストが表示されるので、スクロールダウンして“新しいハードウェアデバイスの追加”を選択します。

3. 次の画面で“一覧から選択したハードウェアをインストールする”を選択し“次へ”をクリックします。リストから“ネットワークアダプタ”をダブルクリックします。

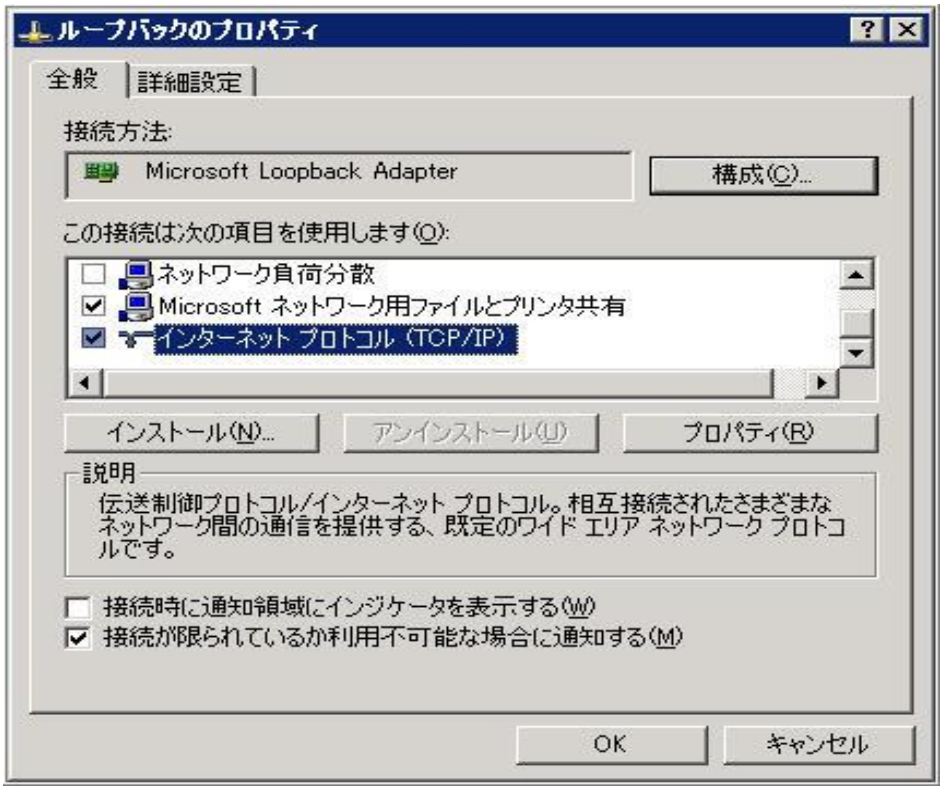


4. 次の画面で、ネットワークインターフェースのベンダー名がリストされますので、“Microsoft”の中から“Microsoft Loopback Adapter”をダブルクリックします。

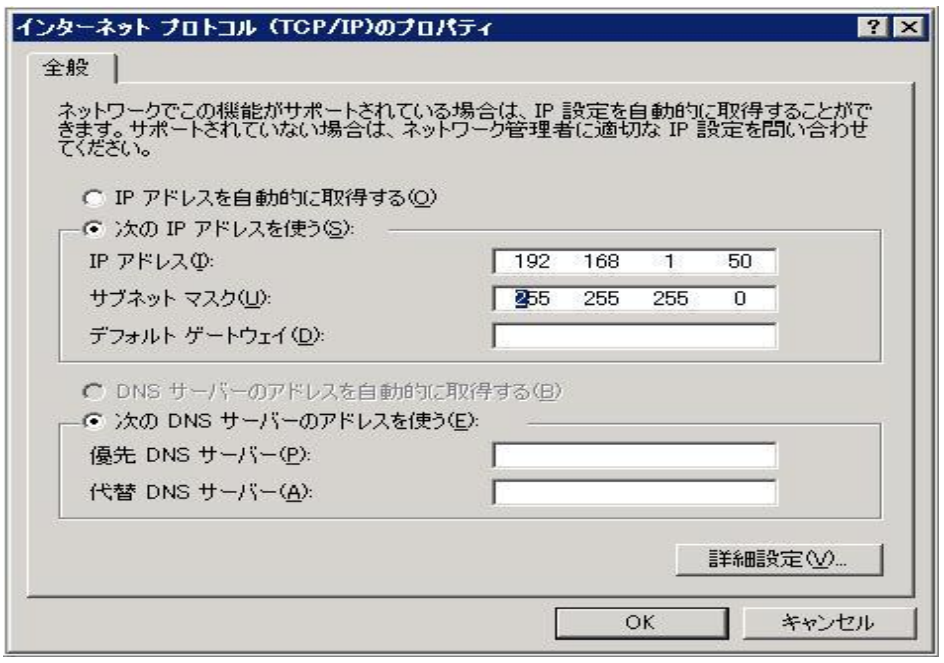


5. “次へ”をクリックし、アダプタをインストールします。問題なくインストールされると、完了画面が現れますので、“完了”をクリックします。

6. コントロールパネルの“ネットワーク接続”を選択すると、“ローカルエリア接続２”が追加されています。これは“ループバック”に名前を変更しておくと管理上便利です。そして、その状態画面から“プロパティ”をクリックし、“インターネットプロトコル(TCP/IP)”を選択します。



7. “プロパティ”をクリックし、IP アドレスにバーチャルサービスのアドレスを入力します。この例では、バーチャルサービスは‘192.168.1.50’です。サブネットマスクを入力し、“詳細設定”をクリックします。



8. TCP/IP 詳細画面の中の“自動メトリック”のチェックを外します。そして、ARP リクエストが来てもレスポンスを返さないようにするために‘254’と入力

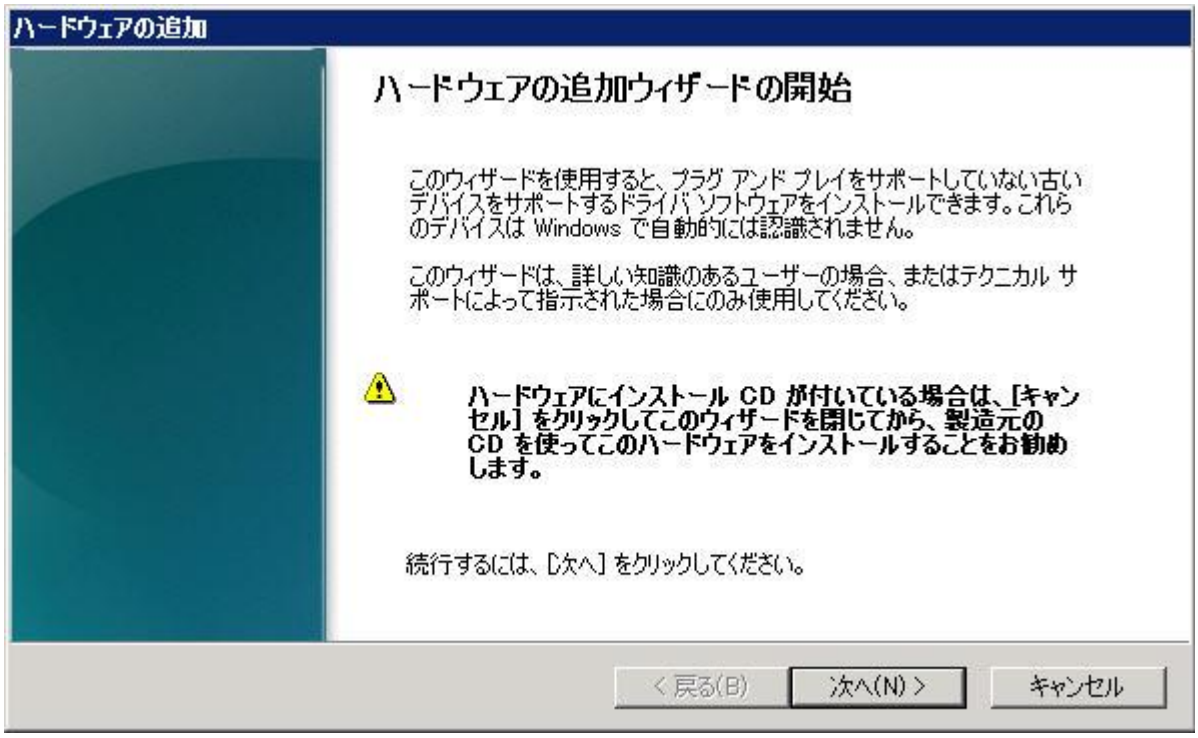
します。そして、“OK”をクリックし変更を終了させます。

9. TCP/IP 詳細設定画面に戻りますので、“OK”をクリックし完了させます。

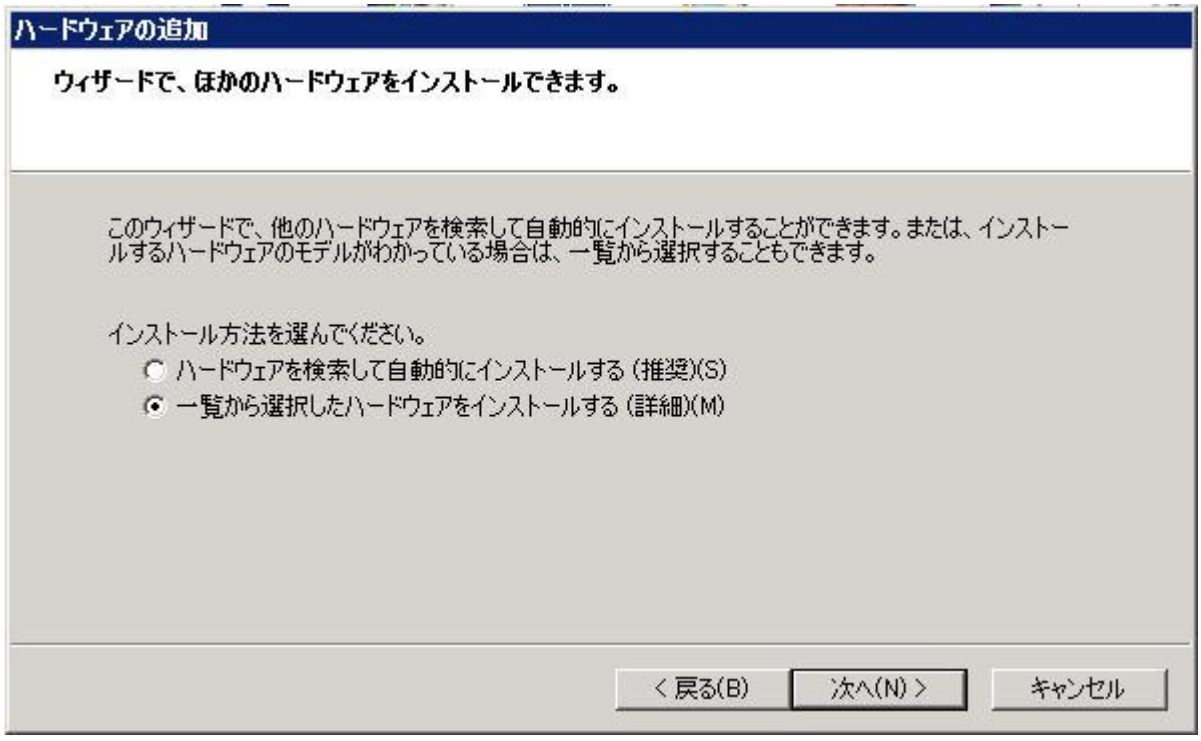
Windows サーバ２００８でのループバックインターフェースの設定

Windows サーバ２００８でも、ループバック･アダプタを使用するのが一般的です。ループバックアダプタを設定し、バーチャルサービス IP アドレスをアサインする方法を示します。

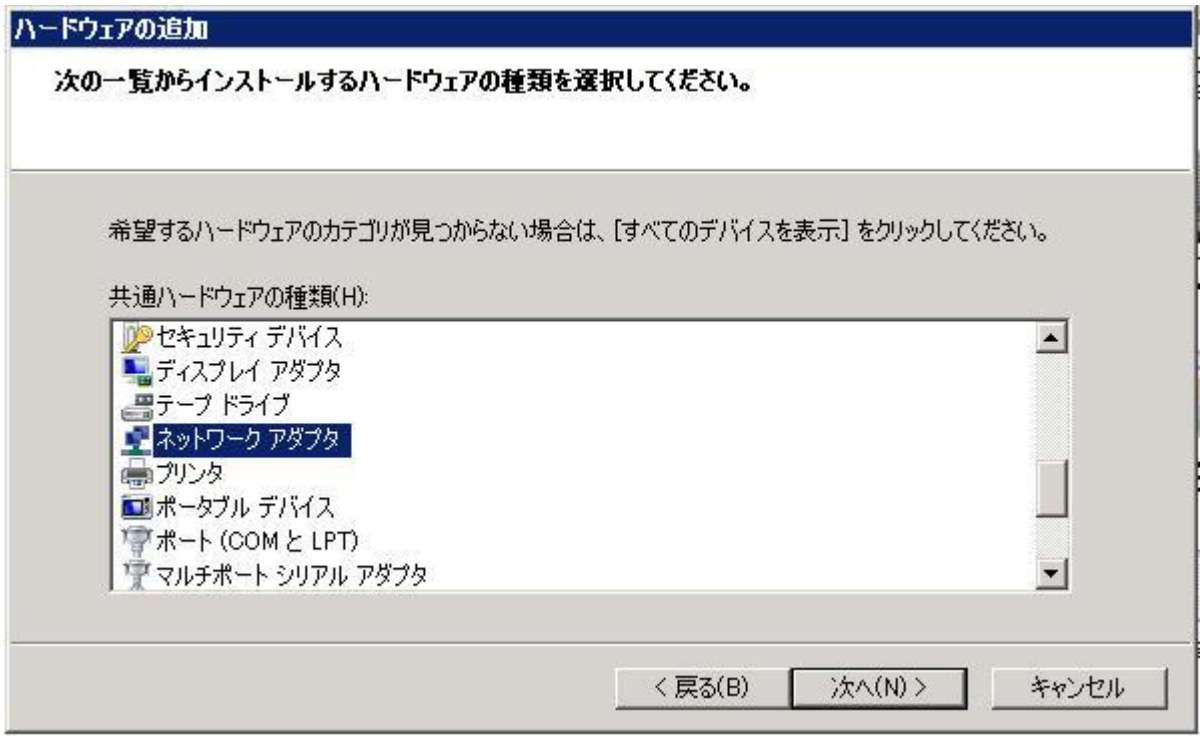
1. コントロールパネルの“ハードウェアの追加”を選択します。



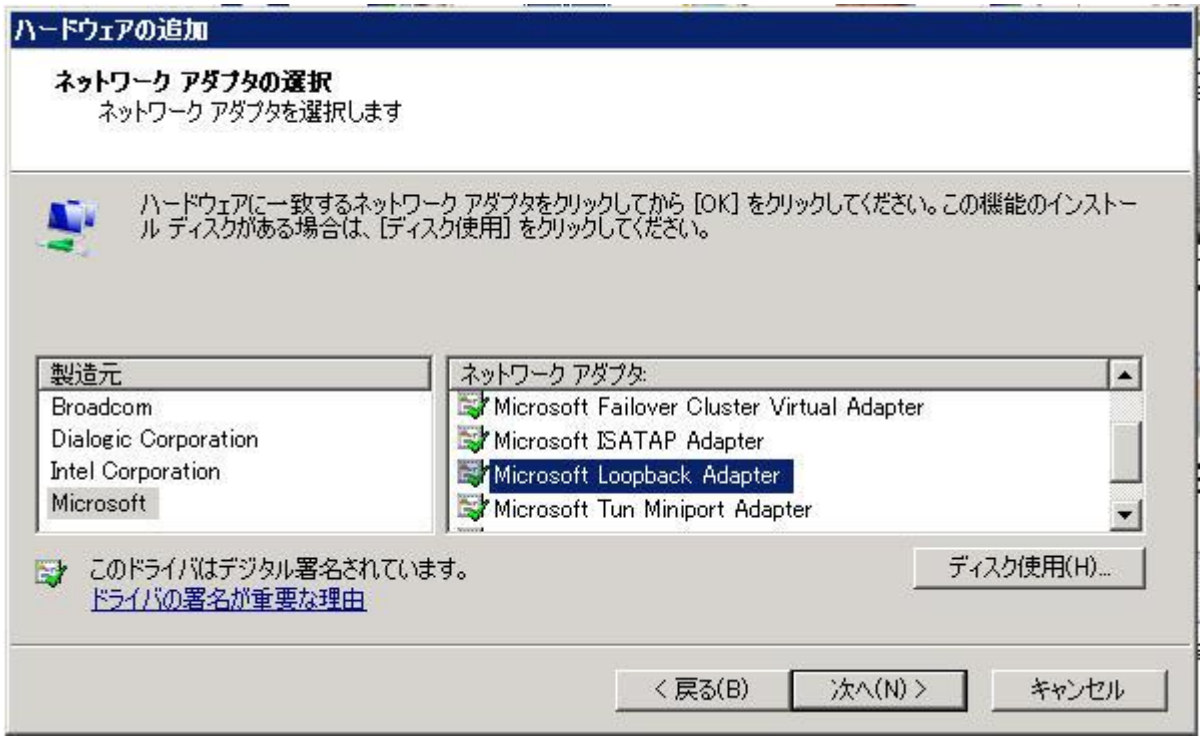
2. Microsoft のループバックアダプタを一覧から選択します。



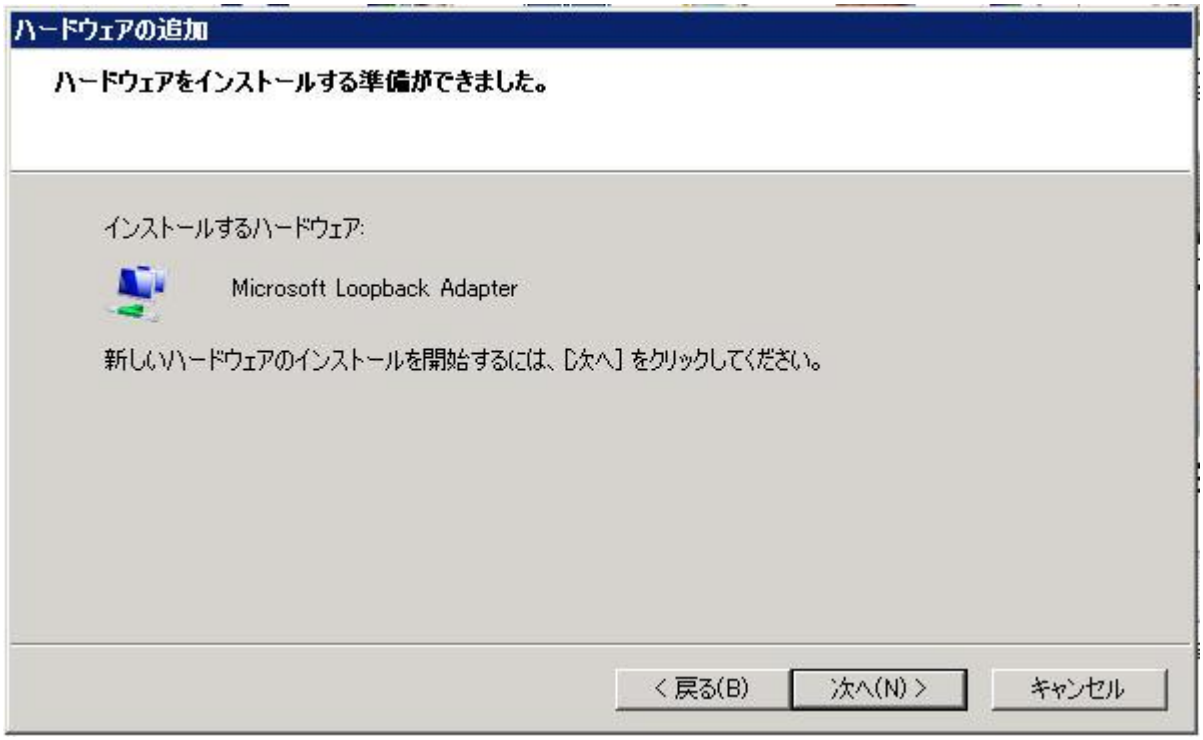
3. ネットワークアダプタを選択します。



4. Mocrosoft の Loopback Adapter を選択します。



5. 選択したハードウェアを確認後、次に進みます。

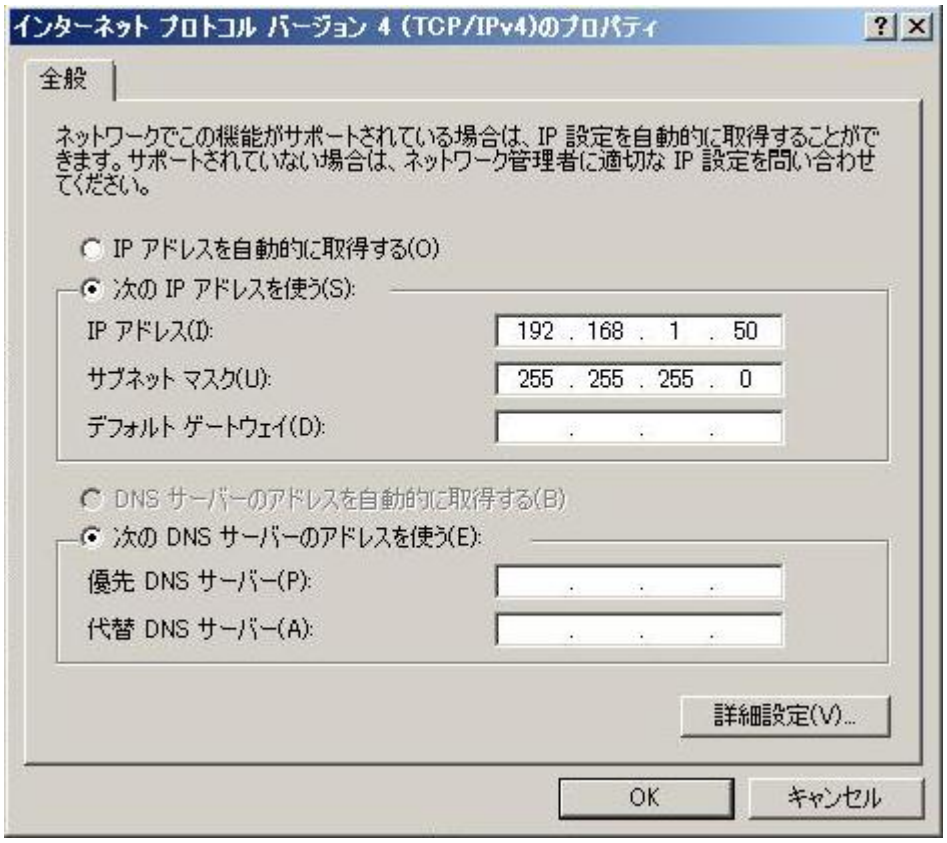


6. LAN, または高速インターネットに Loopback Adapter が追加されたのを確認します。

追加した Loopback Adapter を選択してプロパティ画面を開きます。

7. ループバックアダプターに VIP（バーチャル IP）を設定します。
プロパティ画面で“インターネットプロトコルバージョン 4（TCP/IPv4）”を選択します。

IP アドレスに VIP を設定します。



1. 下記のコマンドをコマンドプロンプトから実行します。

netsh interface ipv4 set interface "物理インターフェース名" weakhostreceive=enabled
netsh interface ipv4 set interface "ループバックアダプタ名" weakhostreceive=enabled
netsh interface ipv4 set interface "ループバックアダプタ名" weakhostsend=enabled

例：物理インターフェース名が【ローカル エリア接続】
ループバックアダプタ名が【ローカル エリア接続 2】の場合

netsh interface ipv4 set interface ″ローカル エリア接続″ weakhostreceive=enabled
netsh interface ipv4 set interface ″ローカル エリア接続 2″ weakhostreceive=enabled
netsh interface ipv4 set interface ″ローカル エリア接続 2″ weakhostsend=enabled

となります。

ウィンドウズ以外のマシンでの設定方法

ダウン インターフェース（Down Interface）

インターフェースにエリアスとしてバーチャルサービスの IP アドレスを設定します。そして、管理上ダウン状態にしておきます。

コマンドラインで. “ifconfig eth0:1 192.168.1.31 down”と入力します。FreeBSD の場合は、“ifconfig xl0 alias 192.168.1.31 down と入力します。

どのようにエイリアス IP アドレスを設定し、管理上ダウン状態にしておくかは、各 OS のマニュアルを確認して実施して下さい。それぞれの OS で設定方法が異なります。Linux でも、配布ベンダーによっては操作方法が異なります。

ループバック･インターフェース（Loopback Interface）

サーバがバーチャルサービスの IP アドレスのパケットを取り組む別の方法として、ループバックインターフェースにバーチャルサービスの IP アドレスをエイリアス IP アドレスとして設定する方法があります。

Linux では、“ifconfig lo0:1 192.168.1.31 netmask 255.255.255.255 up”コマンドで行えます。

エイリアス IP アドレスの ARP レスポンス無効化

リアルサーバで、DSR のためにエイリアス IP アドレスに対する ARP リクエストに応答しないようにするのは簡単ではありません。OS ベンダーにコンタクトをして、その方法を入手して下さい。

Linux でのループバックへの VIP 設定方法例

root@RS1 $ ifconfig lo:1 195.30.70.200 broadcast 195.30.70.200 netmask 255.255.255.255
root@RS1 $ ifconfig lo:1
lo:1 Link encap:Local Loopback inet addr:195.30.70.200 Mask:255.255.255.255 UP LOOPBACK RUNNING MTU:3924 Metric:1

＜確認例＞
root@RS1 $ ifconfig –a
eth0 Link encap:Ethernet HWaddr 00:00:00:00:00:bb inet addr: 195.30.70.11 Bcast: 195.30.70.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:96561817 errors:526 dropped:0 overruns:5 frame:0 TX
packets:97174301 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:100 Interrupt:10 Base address:0x4000
lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:3924 Metric:1 RX packets:3985923
errors:0 dropped:0 overruns:0 frame:0 TX packets:3985923 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0

ウェブサーバ

ウェブサーバは、リアルサーバとバーチャルサービスの両方の IP アドレスをリスニングしなければなりません。リアルサーバの IP アドレスに対して、ロードマスターは ヘルスチェックを実行します。

そして、実際のサービスのリクエストは、バーチャルサービスの IP アドレスに対して発信されてきます。又、そのリクエストに応答するために、パケットの送信先 IP アドレスとしても使われます。

ウェブサーバをどのように設定するかで変わりますが、アパッチと IIS サーバの両方とも同一のドキュメントルーツながら複数の IP アドレスでリスニングするメカニズムを持っています。

8.3 DSR 実習

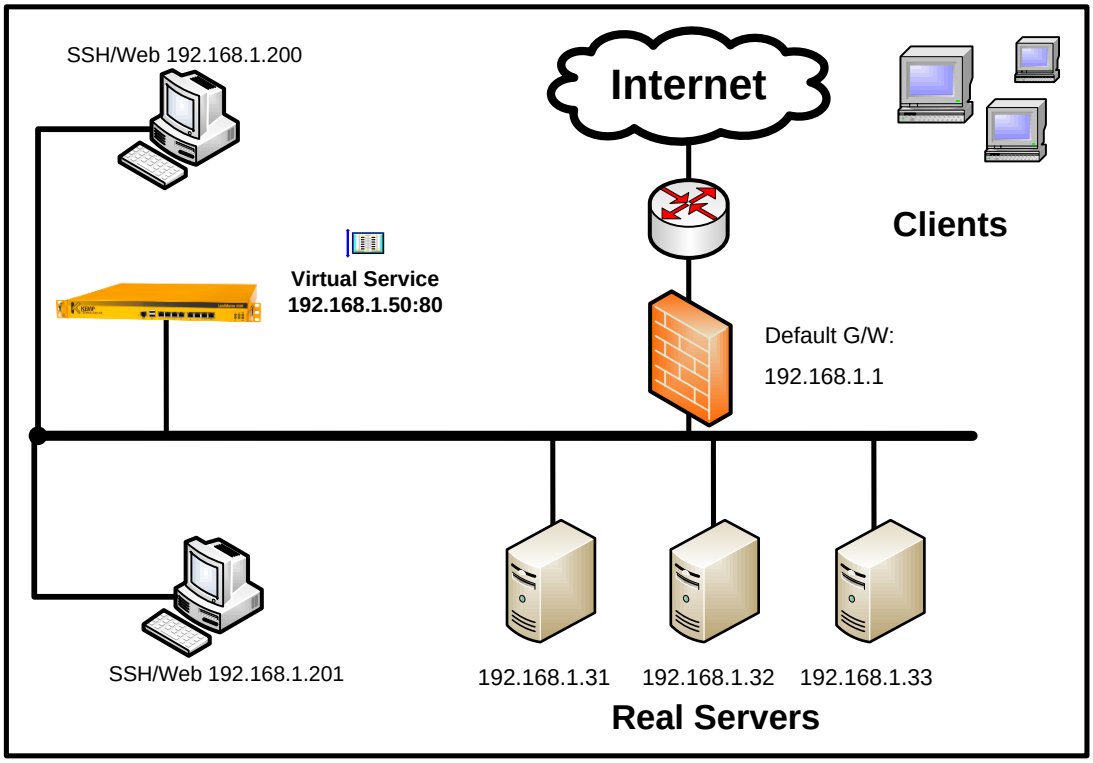
実習目標：

この実習を通して、DSR 用バーチャルサービスとリアルサーバのロードマスター上の設定と、そして Windows2003 IIS サーバ上の設定方法を習得します。

実習環境セットアップ

この実習を行うには、下記の準備が必要です。

- アクセス出来るロードマスター
- 一つのバーチャルサービス用 IP アドレスと同じサブネットに接続されている最低二つの Windows2003 IIS サーバ
- 同じサブネットに接続されていて、ブラウザが使える Windows マシン一台



一般の DSR 用ではないバーチャルサービス作成とリアルサーバのアサイン

1. モジュール２を参考に‘**192.168.1.50：80**’のバーチャルサービスを作成します。 **“Scheduleing Method”**はデフォルトの**“Round Robin”**のままとし、パーシステンスオプションには何も設定しません。

2. リアルサーバをアサインします。ポート番号は“**80**”を使用します。

3. Windows マシンからバーチャルサービスの“**192.168.1.50**”にブラウザを使ってアクセスします。

4. リアルサーバよりの応答を確認します。

リアルサーバの DSR 用への設定変更

1. “**Virtual Services**”の“**View/Modify Services**”オプションを選択します。

2. 表示されたリストから、該当するバーチャルサービスの“**Modify**”ボタンをクリックします。

3. 属性画面の“**Real Servers for This Virtual Service**”セクションの中のリアルサーバの“**Modify**”ボタンをクリックします。

4. “**Forwarding Method**”を“**nat**”より“**directreturn**”に変更し、“**OK** ”をクリックします。

5. 他のリアルサーバにも同じ変更を行います。

リアルサーバ（IIS）のループバックアダプターの作成

1. 上記 8.2.2 項を参考にバーチャルサービス用 IP アドレスのループバック･アダプタを IIS サーバに作成します。

2. IIS サーバが ARP リクエストに対して応答しないのを確認するために、バーチャルサービスを利用不可にし、そして PING を送信します。バーチャルサービスを利用不可にするには、属性画面の中の“**Activate or Deactivate Service**”のチェックマークを外します。PING に応答がないことを確認します。

3. バーチャルサービスの属性画面で“**Activate or Deactivate Service**”にチェックマークを付けて利用可能にします。

4. バーチャルサービスに接続が行える事を確認します。

DSR 接続の検証

1. ロードマスターのイーサポート 0 上のパケットフローをトレースするために、SSH クライアント“**PuTTY**”よりロードマスターへ接続します。

2. ログイン後、“**Utilities**”メニューを選択します。

3. “**Diagnostic**”オプションを選択し、“**Diagnostic shell**”オプションに行きます。

4. “**%**”プロンプトが現れますので、“**tcpdump –i eth0 –s 1500 –w <filename.cap> port 80** ”のコマンドを入力します。

5. Winodws マシンのブラウザから、何回かバーチャルサービスへアクセスします。
6. トレースを“**Ctrl” + C**”の入力でストップします。
7. 使用できる FTP サーバへ接続し、トレースしたファイルを転送します。
8. トレースファイルを解析し、リアルサーバからの応答がクライアントへ直接帰っていることをチェックします。