



IP Routing

標準のインストールでは、VPN Concentrator は、外部ルータを経由してパブリック ネットワークに接続されています。その外部ルータによりネットワーク相互間のデータ トラフィックは、ルート指定されています。VPN Concentrator は、またルータを経由してプライベート ネットワークにも接続することもできます。

VPN Concentrator 自体には、IP ルーティング サブシステムが組み込まれていて、スタティック ルーティング機能、RIP (ルーティング情報プロトコル) 機能、および OSPF (Open Shortest Path First) 機能を備えています。RIP と OSPF はルーティング プロトコルであり、ルータにより、ネットワークの接続、状況、およびデータ トラフィックの送信用の最適パスを判断するために、内部ネットワークまたはプライベート ネットワーク内の他のルータへのメッセージに使用されます。

IP ルーティング サブシステムがデータ パスを確立した後、ルーティング自体はワイヤ スピードで行われます。このサブシステムは、VPN Concentrator を経由して着信するすべてのパケット (トンネル伝送されたパケットであっても) 内の宛先 IP アドレスを調べて、送信先を判断します。パケットが暗号化されている場合、VPN Concentrator は、処理とその後のルーティングのために、それらのパケットを適切なトンネリング プロトコル サブシステム (PPTP、L2TP、IPSec) に送信します。パケットが暗号化されていない場合は、設定済みの IP ルーティング パラメータにしたがって、それらのパケットをルート指定します。

パケットをルート指定する場合、サブシステムは、まず、確認されているルート (RIP および OSPF から確認されているもの) を使用し、次にスタティック ルートを使用し、その次にデフォルト ゲートウェイを使用します。デフォルト ゲートウェイが設定されていない場合、サブシステムは、デフォルト ゲートウェイ以外の方法ではルート指定できないパケットを削除します。また、VPN Concentrator は、トンネル用のデフォルト ゲートウェイも備えています。これは、トンネル伝送に使用されるトラフィックに専用の独立したデフォルト ゲートウェイです。

このセクションでは、スタティック ルート、デフォルト ゲートウェイ、およびシステム全体の OSPF パラメータを設定します。また、このセクションには、システム全体の DHCP (ダイナミック ホスト コンフィギュレーション プロトコル) パラメータも含まれています。RIP、およびインターフェイス固有の OSPF パラメータは、ネットワーク インターフェイス上で設定します。Configuration | Interfaces を参照してください。

VPN Concentrator Manager のこのセクションでは、VRRP (Virtual Router Redundancy Protocol) を使用して、VPN Concentrator の冗長性も設定します。この機能は、並列冗長設定で複数の VPN Concentrator をインストールする場合に適用されます。この機能は、1 次システムが停止した場合にバックアップ システムに自動的に切り替えます。したがって、VPN へのユーザ アクセスが確保されます。この機能は、IPSec LAN-to-LAN 接続、IPSec クライアント (単一ユーザによるリモート アクセス) 接続、および PPTP クライアント接続を経由した、ユーザ アクセスをサポートします。

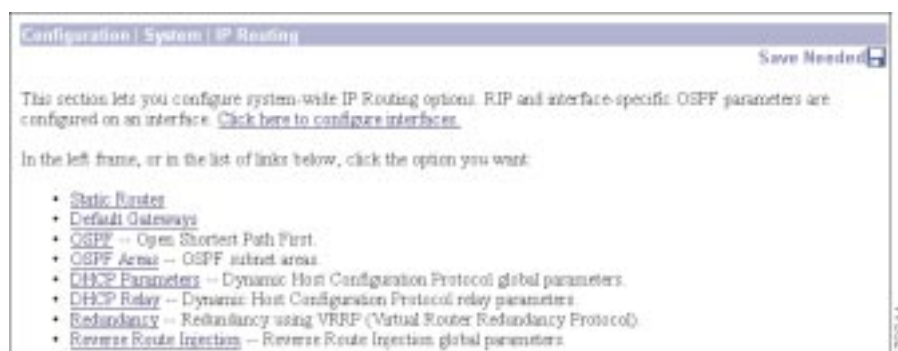
Configuration | System | IP Routing

このセクションでは、システム全体の IP ルーティング パラメータを設定します。

- Static Routes: 手入力で設定されたルーティング テーブル
- Default Gateways: 他の手段ではルート指定できないトラフィック用のルート
- OSPF: Open Shortest Path First ルーティング プロトコル
- OSPF Areas: OSPF ドメイン内のサブネット エリア
- DHCP: DHCP Proxy および DHCP Relay 用のグローバル ホスト コンフィギュレーション プロトコルのグローバル パラメータ
- Redundancy: Virtual Router Redundancy Protocol のパラメータ
- Reverse Route Injection: Reverse Route Injection のグローバル パラメータ

RIP、およびインターフェイス固有の OSPF パラメータは、ネットワーク インターフェイス上で設定します。強調表示されているリンクをクリックして、Configuration | Interfaces の画面に進んでください。

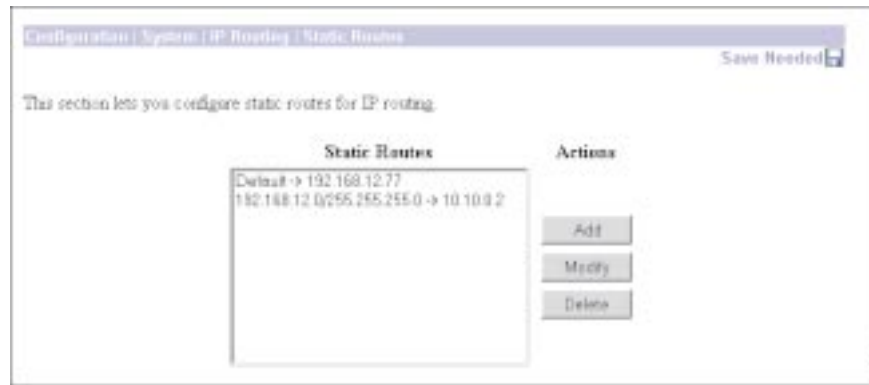
図 8-1 Configuration | System | IP Routing の画面



Configuration | System | IP Routing | Static Routes

このセクションでは、IP ルーティング用のスタティック ルートを設定できます。通常、RIP または OSPF を介して確認できない、プライベート ネットワーク用のスタティック ルートを設定します。

図 8-2 Configuration | System | IP Routing | Static Routes の画面



Static Routes

Static Routes リストは、手入力で設定された IP ルートを表示します。形式は [destination network address/subnet mask -> outbound destination] です (例: 192.168.12.0/255.255.255.0 -> 10.10.0.2)。192.168.12.0/255.255.255.0 デフォルト ゲートウェイを設定した場合は、このリストの先頭に、Default -> default router address として表示されます。設定済みのスタティック ルートがない場合、このリストには、--Empty-- と表示されます。



(注) プラットフォームによっては、次のようなスタティック ルーティング テーブルの制限事項があります。すべてのルートを読み込むことができるかどうかは、十分なシステム メモリ容量があるかにより異なります。

3002 - 50 ルート

3005 -200 ルート

30XX - 10,240 ルート

ルーティング テーブルが満杯の場合は、ログに次のメッセージが表示されます。

```
12539 08/30/2001 22:07:55.270 SEV=2 IP/26 RPT=12
```

```
Routing Table Full, add new route failed.
```

Add / Modify / Delete

新しいスタティック ルートを設定し、追加するには、**Add** をクリックしてください。VPN Concentrator Manager は、Configuration | System | IP Routing | Static Routes | Add の画面が表示されます。

設定済みのスタティック ルートを変更する場合は、リストからそのルートを選択し、**Modify** をクリックしてください。VPN Concentrator Manager により、Configuration | System | IP Routing | Static Routes | Modify の画面が表示されます。デフォルト ゲートウェイを選択すると、VPN Concentrator Manager は、Configuration | System | IP Routing | Default Gateways の画面が表示されます。

設定済みのスタティック ルートを削除する場合は、リストからそのルートを選択し、**Delete** をクリックしてください。



(注) 削除を確認するメッセージなどは表示されません。また削除したスタティック ルートを元に戻すこともできません。

VPN Concentrator Manager により、表示画面が更新され、リスト内に残っているスタティック ルートが表示されます。この画面で、デフォルト ゲートウェイを削除することはできません。デフォルト ゲートウェイを削除する場合は、Configuration | System | IP Routing | Default Gateways の画面を参照してください。

注意：

VPN Concentrator Manager により、システム管理者が加えた変更は、ただちにアクティブ コンフィギュレーションに組み込まれます。アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

Configuration | System | IP Routing | Static Routes | Add or Modify

これらの画面では、次の作業ができます。

- Add: 新しいスタティック (つまり手入力で設定される) ルートを設定し、IP ルーティング テーブルに追加します。
- Modify: 設定済みのスタティック ルートのパラメータを変更します。

図 8-3 Configuration | System | IP Routing | Static Routes | Add または Modify の画面

The screenshot shows a configuration window titled "Configuration | System | IP Routing | Static Routes | Add". The main instruction is "Configure and add a static route." Below this are several input fields: "Network Address" (with a placeholder "Enter the network address"), "Subnet Mask" (with a placeholder "Enter the subnet mask"), "Metric" (with a placeholder "Enter the numeric metric for this route (1 through 16)"), "Destination Router Address" (with a placeholder "Enter the router/gateway IP address"), and "Interface" (a dropdown menu currently showing "Ethernet1 (Private) [10.10.99.10]" and a placeholder "Select the interface to route to."). At the bottom left are "Add" and "Cancel" buttons. A small number "67103" is visible in the bottom right corner of the window.

Network Address

このスタティック ルートが適用される宛先ネットワーク IP アドレスを入力します。この宛先アドレスを持つパケットは、下記の Destination に送信されます。ドット付き 10 進表記を使用してください (例: 192.168.12.10)。

Subnet Mask

宛先ネットワーク IP アドレス用のサブネット マスクを入力します。ドット付き 10 進表記を使用してください (例: 255.255.255.0)。サブネット マスクは、IP アドレスのどの部分がネットワークを表し、どの部分がホストを表すかを指定します。ルータ サブシステムは、このネットワーク部分だけを参照します。

VPN Concentrator Manager により、入力された IP アドレスに応じた標準サブネット マスクが自動的に表示されます。たとえば、IP アドレス 192.168.12.0 はクラス C アドレスであり、標準サブネット マスクは 255.255.255.0 です。このエントリをそのまま使用することも、変更することもできます。ここでは、0.0.0.0 は使用できないことに注意してください。これは、このサブネット マスクがデフォルト ゲートウェイと同じサブネット マスクに解決されてしまうからです。

Metric

このルートのメトリック、または、コストを入力します。1 ~ 16 の数字を入力してください。この場合、1 が最低コストです。ルーティング サブシステムは、常に、コストが一番低いルートを使用しようとしています。たとえば、あるルートが低速回線を使用する場合、すべての高速ルートが使用できない場合だけ、システムがその低速ルートを使用するように、高いメトリックを割り当てることができます。

Destination

オプション ボタンをクリックして、これらのパケットの発信宛先を選択します。発信宛先として、特定のルータまたはゲートウェイあるいは、VPN Concentrator インターフェイスのいずれか 1 つしか選択できません。

Router Address

これらのパケットをルート指定する先の特定のルータまたはゲートウェイの IP アドレスを入力します。つまり、VPN Concentrator と、パケットの最終宛先との間にある、次のホップの IP アドレスです。ドット付き 10 進表記を使用してください (例 : 10.10.0.2)。

Interface

Interface ドロップダウン メニュー ボタンをクリックし、設定済みの VPN Concentrator インターフェイスを発信宛先として選択します。このメニューには、設定されているすべてのインターフェイスが表示されます。スタティック ルートのデフォルト インターフェイスは、Ethernet 2 (パブリック) インターフェイスです。

たとえば、LAN-to-LAN 設定で、プライベート ネットワーク上にない IP アドレスがリモート アクセス クライアントに割り当てられている場合、Ethernet 1 (Private) インターフェイスへの発信アドレスを使って、スタティック ルートを設定できます。その後、このクライアントは、ピア VPN Concentrator とそのネットワークにアクセスできます。

Add または Apply / Cancel

設定済みルートのリストに新しいスタティック ルートを追加する場合は、**Add** をクリックしてください。スタティック ルートに変更を適用する場合は、**Apply** をクリックしてください。いずれの操作でも、アクティブ コンフィギュレーション内に入力内容が組み込まれます。VPN Concentrator Manager により、Configuration | System | IP Routing | Static Routes の画面に戻ります。新しいルートはすべて、Static Routes リストの一番下に表示されます。

注意 :

アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

入力内容を破棄する場合は、**Cancel** をクリックしてください。VPN Concentrator Manager により、Configuration | System | IP Routing | Static Routes の画面に戻り、Static Routes リストは変更されません。

Configuration | System | IP Routing | Default Gateways

この画面では、IP ルーティング用のデフォルト ゲートウェイを設定し、トンネル伝送されるトラフィック用のトンネル デフォルト ゲートウェイを設定します。この画面は、初めてデフォルト ゲートウェイを設定する場合と、デフォルト ゲートウェイを変更する場合の両方に使用されます。また、Configuration | Quick | System Info の画面でもデフォルト ゲートウェイを設定できます。

IP ルーティング サブシステムは、データ パケットのルート指定に、最初に確認済みのルート、次にスタティック ルート、その次にデフォルト ゲートウェイを使用します。デフォルト ゲートウェイを指定しないとき、システムは、他の方法ではルート指定できないパケットを削除します。

トンネル伝送されるデータの場合、システムが宛先アドレスを認識していないときは、最初に、パケットをトンネル デフォルト ゲートウェイにルート指定しようとします。そのルートが設定されていない場合は、通常のデフォルト ゲートウェイを使用します。

図 8-4 Configuration | System | IP Routing | Default Gateways の画面

Default Gateway

デフォルトのゲートウェイまたはルータの IP アドレスを入力します。ドット付き 10 進表記を使用してください (例: 192.168.12.77)。このアドレスには、任意の VPN Concentrator インターフェイス上で設定されている IP アドレスと同一のアドレスを使用しないでください。デフォルト ゲートウェイを使用しない場合は、0.0.0.0 を入力します (デフォルト エントリ)。

設定済みのデフォルト ゲートウェイを削除する場合は、0.0.0.0 を入力してください。

デフォルト ゲートウェイは、VPN Concentrator インターフェイスから到達可能でなければなりません。通常、パブリック ネットワーク上にあります。入力された IP アドレスがインターフェイス ネットワークのいずれかにない場合、VPN Concentrator Manager により警告画面が表示されます。入力された IP アドレスがパブリック ネットワーク上にない場合は、ダイアログボックスが表示されません。

Metric

デフォルト ゲートウェイへのルートのメトリック、または、コストを入力します。1 ~ 16 の数字を入力してください。この場合、1 が最低コストです。ルーティング サブシステムは、常に、コストが一番低いルートを使用しようとします。たとえば、あるルートが低速回線を使用する場合、すべての高速ルートが使用できない場合だけ、システムがその低速ルートを使用するように、高いメトリックを割り当てることができます。

Tunnel Default Gateway

トンネル伝送されるデータ用のデフォルト ゲートウェイの IP アドレスを入力します。ドット付き 10 進表記を使用してください (例: 10.10.0.2)。トンネル デフォルト ゲートウェイを使用しない場合は、0.0.0.0 を入力してください (デフォルト エントリ)。

設定済みのトンネル デフォルト ゲートウェイを削除する場合は、0.0.0.0 を入力してください。

多くの場合、このゲートウェイは、VPN Concentrator と並行したファイアウォールであり、パブリック ネットワークとプライベート ネットワークとの間にあります。トンネル デフォルト ゲートウェイは、IPSec LAN-to-LAN トラフィックを含めて、トンネル伝送されるすべてのトラフィックに適用されます。



(注) NAT (Network Address Translation) に対して、VPN Concentrator ではなく、外部デバイスを使用する場合は、トンネル デフォルト ゲートウェイを設定する必要があります。

Override Default Gateway

RIP または OSPF を介して確認されたデフォルト ゲートウェイが、設定済みのデフォルト ゲートウェイを上書きできるようにする場合は、**Override Default Gateway** チェックボックスにチェックマークを付けてください (デフォルト)。設定済みのデフォルト ゲートウェイを常に使用する場合は、このボックスのチェックマークを外してください。

Apply / Cancel

デフォルト ゲートウェイの設定値を適用し、アクティブ コンフィギュレーションに組み込む場合は、**Apply** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。Default Gateway を設定すると、そのデフォルト ゲートウェイは、Configuration | System | IP Routing | Static Routes 画面上の Static Routes リストにも表示されます。

注意:

アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

入力内容を破棄する場合は、**Cancel** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

Configuration | System | IP Routing | OSPF

この画面では、OSPF (Open Shortest Path First) ルーティング プロトコル用のシステム全体のパラメータを設定します。Configuration | Interfaces 画面で、インターフェイス固有の OSPF パラメータも設定する必要があります。

OSPF は、IP ルーティング サブシステムが、ネットワークの接続、状況、およびデータ トラフィックの送信用の最適パスを判別するために、内部ネットワークまたはプライベート ネットワーク内の他の OSPF ルータへのメッセージに使用するプロトコルです。VPN Concentrator は、OSPF バージョン 2 (RFC 2328) をサポートします。

完成度の高いプライベート ネットワークは、OSPF 自律システム (AS)、またはドメインと呼ばれます。AS 内のサブネットは、エリアと呼ばれます。OSPF エリアは、Configuration | System | IP Routing | OSPF Areas の画面で設定します。

図 8-5 Configuration | System | IP Routing | OSPF の画面



Enabled

VPN Concentrator の OSPF ルータを使用可能にするには、Enabled チェックボックスにチェックマークを付けます (デフォルトでは、チェックマークが付いていません)。次で説明する Router ID も入力する必要があります。OSPF が、OSPF を使用する任意のインターフェイス上で機能するには、このボックスにチェックマークを付ける必要があります。

次で設定されている Router ID を変更する場合は、ここで、OSPF を使用不可にする必要があります。

インターフェイス上で OSPF ルーティングを使用可能にするには、該当する Configuration | Interfaces 画面でも、OSPF を設定し、使用可能にする必要があります。

Router ID

ルータ ID は、ドメイン内の他の OSPF ルータに対して、VPN Concentrator の OSPF ルータを固有に識別するものです。ルータ ID の形式は IP アドレスの形式ですが、アドレスとしてではなく、識別子としてだけ機能します。しかし、規定により、この ID は、OSPF ルータ ネットワークに接続されるインターフェイスの IP アドレスと同じです。

このフィールドにルータ ID を入力します。ドット付き 10 進表記の IP アドレス形式を使用してください (例: 10.10.4.6)。デフォルトは、0.0.0.0 (設定されたルータなし) です。OSPF ルータを使用可能にする場合は、ID を入力する必要があります。



(注) ルータ ID を設定し、適用した後に、このルータ ID を変更する場合は、事前に OSPF を使用不可にしておく必要があります。この ID を 0.0.0.0 に戻すことはできません。

Autonomous System

OSPF 自律システム (AS)、またはドメインは、完全な内部ネットワークです。AS 境界ルータは、他の自律システムに属しているルータとルーティング情報を交換し、その AS 全体に外部の AS ルーティング情報を公示します。OSPF で Reverse Rroute Injection (RRI) を使用している場合は、Autonomous System を使用可能にする必要があります。

VPN Concentrator の OSPF ルータが自律システムの境界ルータであることを指定する場合に、**Autonomous System** チェックボックスにチェックマークを付けてください。このボックスにチェックマークを付けると、VPN Concentrator は、RIP とスタティックルートも OSPF エリアに再配布します。デフォルトでは、このボックスにチェックマークは付いていません。

Apply / Cancel

OSPF 設定値を適用し、アクティブ コンフィギュレーションに組み込む場合は、**Apply** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

注意：

アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

設定を破棄する場合は、**Cancel** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

Configuration | System | IP Routing | OSPF Areas

このセクションでは、OSPF 自律システムまたはドメイン内のサブネットである、OSPF エリアを設定します。この VPN Concentrator の OSPF ルータに接続されているすべてのエリアに対して、エントリを設定する必要があります。

また、VPN Concentrator のネットワーク インターフェイス上で OSPF エリアを指定することもできます (Configuration | Interfaces を参照)。これらのエリア ID は、この画面の OSPF Area リストに表示されます。

図 8-6 Configuration | System | IP Routing | OSPF Areas の画面



OSPF Area

OSPF Area リストには、この VPN Concentrator の OSPF ルータに接続されているすべてのエリアの ID が表示されます。表示される形式は、ドット付き 10 進表記の IP アドレスと同じです (例 10.10.0.0)。デフォルトのエントリは 0.0.0.0 です。このデフォルト エントリは、複数のエリアに接続されているルータである、エリア境界ルータがすべて入っている特殊なエリア (バックボーンと呼ばれます) を指定します。

Add / Modify / Delete

新しい OSPF エリアを設定し、追加する場合は、**Add** をクリックしてください。Configuration | System | IP Routing | OSPF Areas | Add の画面が表示されます。

設定済みの OSPF エリアを変更する場合は、リストからそのエリアを選択し、**Modify** をクリックしてください。VPN Concentrator Manager は、Configuration | System | IP Routing | OSPF Areas | Modify の画面が表示されます。

設定済みの OSPF エリアを削除する場合は、リストからそのエリアを選択し、**Delete** をクリックしてください。



(注) 削除を確認するメッセージなどは表示されません。また削除した OSP エリアは元に戻すことはできません。

表示画面が更新され、OSPF Area リストに残っているエントリが表示されます。

注意：

VPN Concentrator Manager により、システム管理者が加えた変更は、ただちにアクティブ コンフィギュレーションに組み込まれます。アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

Configuration | System | IP Routing | OSPF Areas | Add または Modify

これらの画面では、次の作業ができます。

- Add: OSPF エリアを設定し、追加する。
- Modify: 設定済みの OSPF エリアのパラメータを変更する。



(注) OSPF エリアを設定した後、その ID を変更できません。エリア ID を変更する場合は、既存のエリアを削除した後、新しいエリアを追加してください。

図 8-7 Configuration | System | IP Routing | OSPF Areas | Add または Modify の画面

Area ID

- Add: このフィールドにエリア ID を入力する。ドット付き 10 進表記の IP アドレス形式を使用してください (例: 10.10.0.0)。デフォルト値は、0.0.0.0 (バックボーン) です。
- Modify: エリア ID を設定した後、そのエリア ID を変更できません。前述の注を参照してください。

Area ID は、OSPF 自律システムまたはドメイン内のサブネットエリアを指定します。エリア ID の形式は IP アドレスと同じですが、アドレスではなく、識別子としてだけ機能します。エリア ID 0.0.0.0 は、すべてのエリア境界ルータが入っている特殊なエリア (バックボーン) を指定します。

Area Summary

OSPF ルータが要約 LSA (リンク状態アダプタイズメント) を生成し、OSPF スタブ エリアに伝播するように指定する場合、**Area Summary** チェックボックスにチェックマークを付けます。LSA は、ルータのインターフェイスとルーティングパスの状態を記述します。スタブ エリアには、最終宛先ホストだけが入っています。他のエリアにトラフィックを渡しません。通常、LSA を他のエリアに送信する必要はありません。デフォルトでは、このボックスにチェックマークは付いていません。

External LSA Import

近隣の自律システムから LSA をインポートするかを選択するには、**External LSA Import** ドロップダウンメニュー ボタンをクリックします。LSA は、AS ルータのインターフェイスとルーティングパスの状態を記述します。LSA をインポートすると、完成度の高いリンクステート データベースが構築されますが、必要な処理が増えます。選択項目は次のとおりです。

- External : 近隣の AS から LSA をインポートする (デフォルト)
- No External : 外部 LSA をインポートしない。

Add または Apply / Cancel

設定済みエリアのリストにこの OSPF エリアを追加する場合は、**Add** をクリックしてください。この OSPF エリアに変更を適用する場合は、**Apply** をクリックしてください。どちらのアクションでも、アクティブ コンフィギュレーション内に入力内容が組み込まれます。表示画面は、Configuration | System | IP Routing | OSPF Areas の画面に戻ります。新しいエントリはすべて、OSPF Area リストの一番下に表示されます。

注意：

アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

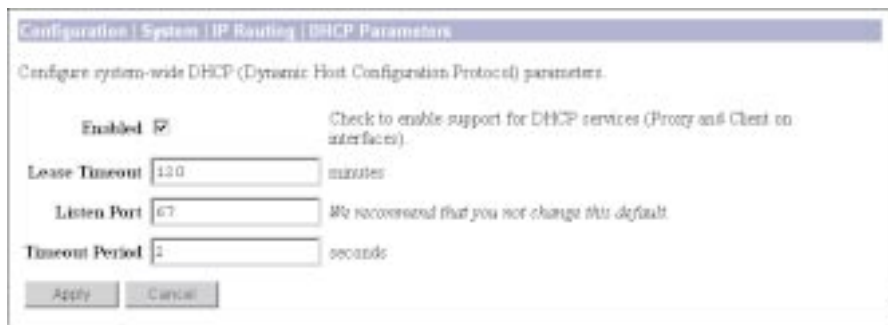
入力内容を破棄する場合は、**Cancel** をクリックしてください。VPN Concentrator Manager は、Configuration | System | IP Routing | OSPF Areas の画面に戻り、OSPF Area リストは変更されません。

Configuration | System | IP Routing | DHCP Parameters

この画面では、VPN Concentrator 内の DHCP 機能に適用される DHCP (ダイナミック ホスト コンフィギュレーション プロトコル) Proxy パラメータを設定します。外部 DHCP サーバを使用すると、VPN トンネルの確立時に、IP アドレスを割り当てることができます。

Configuration | System | Address Management | Assignment の画面で Use DHCP チェックボックスにチェックマークを付ける場合、Configuration | System | Servers | DHCP の画面上で少なくとも 1 つの DHCP サーバを設定する必要があります。ここでは、グローバル DHCP パラメータを設定します。

図 8-8 Configuration | System | IP Routing | DHCP Parameters の画面



Enabled

VPN トンネルに DHCP サーバからその IP アドレスを取得させることができる DHCP Proxy を使用可能にする場合は、**Enabled** チェックボックスにチェックマークを付けてください。デフォルトでは、このボックスにチェックマークが付いています。

Lease Timeout

DHCP サーバから取得されるアドレスのタイムアウトを、分単位で入力します。最小値は 5 分、デフォルト値は 120 分、最大値は 500000 分です。DHCP サーバは、この期間、IP アドレスを「リース」します。このリース期間が終了する前に、VPN Concentrator は、クライアントに代わってリースを更新することを要求します。なんらかの理由でこのリースが更新されない場合、リースの期限が終了すると接続が終了します。DHCP サーバのリース期間は、この設定値より優先されます。

Listen Port

DHCP サーバの応答メッセージを受け入れるのに使用され、UDP ポート番号を入力します。デフォルトは 67 です。これは、割り当て済みポートです。**DHCP サーバとの適切な通信を確保するために、このデフォルト値を変更しないことを強くお勧めします。**

Timeout Period

次の設定済み DHCP サーバに DHCP 要求を送信する前に、その要求に対する応答を待機する初期時間を、秒単位で入力します。最小値は 1 秒、デフォルト値は 2 秒、最大値は 30 秒です。設定済み DHCP サーバのリスト全体のサイクルごとに、この時間が 2 倍になります。

Apply / Cancel

DHCP パラメータの設定値を適用し、アクティブ コンフィギュレーションに組み込む場合は、**Apply** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

注意：

アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

入力内容を破棄する場合は、**Cancel** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

Configuration | System | IP Routing | DHCP Relay

DHCP Relay により VPN クライアント（特にワイヤレス クライアント）は、VPN トンネルを作成する前に、VPN Concentrator のプライベート ネットワーク上の DHCP サーバからネットワーク設定を取得できます。クライアントは DHCP 要求をパブリック ネットワーク、または外部のネットワークに送信します。VPN Concentrator は DHCP 要求をそのパブリック インターフェイス、または外部のインターフェイスで受信し、転送します。DHCP からの要求に応答するためには、企業ネットワーク上の 1 台、または複数の DHCP サーバには、パブリック ネットワーク範囲にある IP アドレスが必要です。DHCP サーバが DHCP 要求に応答しない場合は、VPN クライアントと DHCP サーバは DHCP ネゴシエーションに進みます。VPN Concentrator はルータの役目をし、VPN クライアントと DHCP サーバ間の DHCP メッセージをリレーします。

DHCP Relay の主なメリットは、VPN クライアントごとに別々の DHCP サーバを保守する必要がないことです。しかし DHCP Relay が動作させるために、VPN Concentrator は VPN Concentrator を介して未承認の DHCP トラフィックを許可します。これにはセキュリティ上の危険を引き起こす可能性があります。たとえば、使用可能なすべての DHCP アドレスを要求したり、CPU またはネットワーク帯域幅（あるいはその両方）を使い果たすことで、サービス拒絶攻撃に対して脆弱になります。これらのセキュリティ上の問題に注意する必要があります。



(注) DHCP Relay を使用可能にするには、Configuration | Policy Management | Traffic Management | Filters 画面で DHCP In および DHCP Out ルールをインターフェイス フィルタに割り当てる必要もあります。

Enabled

VPN Concentrator の DHCP Relay を使用可能にする場合、Enabled チェックボックスにチェックマークを付けてください。

DHCP Info Transmission

このパラメータは、VPN Concentrator による DHCP 要求の転送方法を決定します。次のオプションから選択してください。

- Broadcast to all interfaces:パブリック インターフェイスに入ってくる DHCP 要求は、プライベート インターフェイス、および外部インターフェイスにブロードキャストされます。外部インターフェイスに入ってくる DHCP 要求はプライベート インターフェイスにブロードキャストされます。
- Forward to a specific network/host address, including the subnet mask : DHCP 要求は特定のネットワーク、またはホストに送信されます。ネットワーク、またはホスト用の IP アドレスとサブネット マスクを入力します。特定のホストのサブネット マスクは 255.255.255.255 です。

Apply / Cancel

DHCP Relay パラメータの設定値を適用し、アクティブ コンフィギュレーションに組み込む場合は、**Apply** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

注意:

アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

Configuration | System | IP Routing | Redundancy

この画面では、VRRP (Virtual Router Redundancy Protocol) 用のパラメータを設定します。このプロトコルは、冗長インスタレーション内の VPN Concentrator から別の VPN Concentrator への自動切り替えを管理します。プライマリ VPN Concentrator が停止している場合であっても、自動切り替え機能により、ユーザは VPN にアクセスできます。

この機能が適用されるのは、複数の VPN Concentrator が並行しているインスタレーションだけです。1 つの VPN Concentrator がマスター システムであり、その他の VPN Concentrator はバックアップ システムです。切り替えが行われると、1 つのバックアップ システムが、仮想マスター システムの役目をします。



(注)

VPN Concentrator 上で VRRP が設定されている場合、ロード バランシングも同時に使用可能にすることはできません。VRRP 設定では、アクティブ VPN Concentrator に障害が起きない限り、バックアップ デバイスはアイドル状態のままです。ロード バランシングでは、アイドル状態のデバイスを許可しません。

この機能は、IPSec LAN-to-LAN 接続、IPSec クライアント (単一ユーザによるリモート アクセス) 接続、および PPTP クライアント接続を経由した、ユーザ アクセスをサポートします。

- IPSec LAN-to-LAN 接続の場合、切り替えは完全に自動で行われる。ユーザは、何もする必要がありません。通常、切り替えは 3 ~ 10 秒以内に行われます。
- 単一ユーザの IPSec 接続と PPTP 接続の場合、ユーザは、障害システムから切り離されるが、接続パラメータを変更せずに再接続できる。

この画面上で VRRP を設定し、使用可能にする場合は、事前に、すべての冗長 VPN Concentrator 上で、ご使用のインスタレーションに適用されるすべての Ethernet インターフェイスを設定しておく必要があります。Configuration | Interfaces の画面を参照してください。

また、冗長 VPN Concentrator 上で、同一の IPSec LAN-to-LAN パラメータも設定する必要があります。Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN の画面を参照してください。



(注)

VPN Concentrator のインターフェイス上で DHCP が使用可能になっている場合、VRRP を使用できません。VRRP が使用可能になっている場合は、スタティック IP アドレス指定を使用してください。

VRRP 設定では、マスター システムのパブリック インターフェイスまたはプライベート インターフェイスに障害が起きると、その他のインターフェイスが自動的にシャットダウンし、バックアップ VPN デバイスが処理を引き継ぎます。バックアップ VPN デバイスが処理を引き継ぐのは、パブリック インターフェイスとプライベート インターフェイスの両方で VRRP メッセージを受信しなくなったときだけです。

VRRP では一部の障害は検出されません。VRRP マスター デバイスとバックアップ デバイスを接続するネットワーク上で、転送デバイス (ルータまたはスイッチ) に障害が起きると、マスター デバイスが、この障害をリンク レベルで検出しない場合があります。たとえば、マスター デバイスとバックアップ デバイスとの間に Cisco Catalyst スイッチがあるときに、そのスイッチ ポートをシャットダウンしても、このシャットダウンではリンク層はダウンしません。リンク層がダウンしていない限り、VPN Concentrator は、インターフェイスを (Configuration | Interfaces 画面に表示される) 「DOWN」として検出しません。したがって、VPN Concentrator は、すべてのインターフェイス

上でバックアップ デバイスへのメッセージの送信を停止しません。この場合、バックアップ デバイスは少なくとも 1 つのインターフェイス上で引き続き VRRP メッセージを受信するので、マスターとしての処理を引き継ぐことはありません。

また、VRRP シナリオで Cisco Catalyst スイッチがスパンニングツリー プロトコル (STP) を使用する場合、STP に固有の遅延により、バックアップ VPN Concentrator がマスターとしての処理を引き継いだことを認識するのが遅れます。この遅延を 15 秒に短縮するには、STP を使用するスイッチ上で Portfast を使用可能にします。Cisco スイッチ上で Portfast を設定するには、次の資料を参照してください。

<http://www.cisco.com/warp/public/473/12.html>

図 8-9 Configuration | System | IP Routing | Redundancy の画面

Enable VRRP

VRRP 機能を使用可能にするには、**Enable VRRP** チェックボックスにチェックマークを付けます。デフォルトでは、このボックスにチェックマークが付いていません。

Group ID

冗長 VPN Concentrator のこのグループを固有に識別する番号を入力します。この番号は、このグループ内のすべてのシステム上で同一でなければなりません。1 (デフォルト) ~ 255 の数字を使用してください。LAN 上に複数の仮想グループがあることはめったにないので、デフォルトを受け入れるようにお勧めします。

Group Password

冗長 VPN Concentrator のこのグループを識別する際のセキュリティを向上させるために、パスワードを入力します。最長 8 文字までのパスワードを入力できます。この入力内容は平文で表示されます。VRRP アドバイズメントには、このパスワードが平文で記載されます。このパスワードは、このグループ内のすべてのシステム上で同一でなければなりません。パスワードを使用しない場合は、このフィールドをブランクのままにしてください。

Role

Role ドロップダウン メニュー ボタンをクリックします。表示されたリストからこの冗長グループにおける、VPN Concentrator の役割を選択します。

- Master : これは、このグループ内の Master システムです(デフォルトの選択項目)。所定の Group ID を持つグループで設定される Master システムは、1 つだけです。
- Backup 1 ~ Backup 5 : これは、このグループ内の Backup システムです。

Advertisement Interval

このグループ内の他のシステムへの VRRP アドバタイズメント相互間の時間間隔を、秒単位で入力します。Master システムだけがアドバタイズメントを送信します。システムが Backup である間は、Backup システム上でこのフィールドは無視されます。最小の間隔は 1 秒、デフォルト値は 1 秒、最大値は 255 秒です。Backup システムは Master システムになることがあるので、すべてのシステムに対してデフォルトを受け入れるようにお勧めします。

Group Shared Addresses

このグループ内のすべての仮想ルータによって、設定済みルータ アドレスとして扱われる IP アドレスを入力します。VPN Concentrator Manager は、設定されている Ethernet インターフェイス用のフィールドだけを表示します。

Master システム上で、これらのエントリは、その Ethernet インターフェイス上で設定されている IP アドレスです。デフォルトで、VPN Concentrator Manager がそれらの IP アドレスを指定します。

Backup システム上では、デフォルトでこれらのフィールドは空白になっています。システム管理者は、Master システムと同じ IP アドレスを入力する必要があります。

1 (Private)

このグループ内の仮想ルータによって共用される Ethernet 1 (Private) インターフェイスの IP アドレス

2 (Public)

このグループ内の仮想ルータによって共用される Ethernet 2 (Public) インターフェイスの IP アドレス

3 (External)

このグループ内の仮想ルータによって共用される Ethernet 3 (External) インターフェイスの IP アドレス

Apply / Cancel

VRRP の設定値を適用し、アクティブ コンフィギュレーションに組み込む場合は、**Apply** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

注意：

アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

入力内容を破棄する場合は、**Cancel** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

Configuration | System | IP Routing | Reverse Route Injection

VPN Concentrator は、スタティック ルートをルーティング テーブルに自動的に追加し、OSPF または RIP を使用してこれらのルートをプライベート ネットワークまたは境界ルータに告知することができます。この機能は、*reverse route injection (RRI)* と呼ばれます。設定可能な RRI オプションは、接続の種類によって異なります。

- Client (PAT) モードを使用する、リモート ソフトウェア クライアントまたは VPN 3002 Hardware Client
 - 個々のリモート クライアントに対して、Client Reverse Route Injection オプションを使用可能にする。
 - リモート クライアントのグループに対して、Address Pool Hold Down Routes フィールドにアドレス プールを入力する。
- Network Extension Mode (NEM) を使用するリモート VPN 3002 Hardware Client, Network Extension Reverse Route Injection オプションを使用可能にしてください。
- LAN-to-LAN 接続。Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add または Modify 画面の Routing オプションを参照してください。

ルートをプライベート ネットワークに公示することなく、VPN Concentrator のルーティング テーブルに追加するには、プライベート インターフェイス上でルーティングを使用不可にします。

ルートを公示するには、VPN Concentrator のプライベート インターフェイス上で OSPF または RIP を使用可能にしてください (Configuration | Interfaces | Ethernet 1 2 3 画面の RIP タブまたは OSPF タブを参照)。

図 8-10 Configuration | System | IP Routing | Reverse Route Injection の画面

Configuration | System | IP Routing | Reverse Route Injection

Configure system-wide *Reverse Route Injection* parameters. This feature adds specific routes to the routing table for distribution via RIP or OSPF to neighbouring routers for path discovery. Click on **Generate Hold Down Routes** to generate hold down routes based on configured address pools.

Client Reverse Route Injection

Network Extension Reverse Route Injection

Address Pool Hold Down Routes

Check to add non-local (to the private interface) client host routes to the routing table.

Check to add hardware client network extension connection routes to the routing table.

- Add or modify network address and subnet mask using the following standard format: **n.n.n.n/n.n.n.n** (e.g. 192.168.90.64/255.255.255.192).
- Enter each network address and subnet mask pair on a single line.
- If you are using the natural subnet mask, you may omit the subnet mask.

Apply
Cancel
Generate Hold Down Routes

66205

Client Reverse Route Injection



(注) このオプションは、Client (PAT) モードを使用する、すべてのリモートソフトウェアクライアントおよび VPN 3002 Hardware Client に適用されます。

VPN Concentrator のルーティング テーブルに、リモートクライアントごとのホスト ルートを追加するには、**Client Reverse Route Injection** チェックボックスにチェックマークを付けます。VPN Concentrator は、クライアントが接続するとホスト ルートを追加し、クライアントとの接続が解除されるとホスト ルートを削除します。

このオプションは、個々のクライアントを追加します。アドレス プールを追加する場合は、Address Pool Hold Down Routes オプションを使用してください。

デフォルトでは、このボックスにチェックマークが付いていません。

Network Extension Reverse Route Injection



(注) このオプションは、Network Extension Mode を使用する VPN 3002 Hardware Client だけに適用されます。

VPN 3002 Hardware Client の背後にある各ネットワークのネットワーク ルートを、VPN Concentrator 上のルーティング テーブルに追加するには、**Network Extension Reverse Route Injection** チェックボックスにチェックマークを付けます。VPN Concentrator は、VPN 3002 が接続するとルートを追加し、VPN 3002 との接続が解除されるとルートを削除します。

デフォルトでは、このボックスにチェックマークが付いていません。

Address Pool Hold Down Routes



(注) このオプションは、Client (PAT) モードを使用する、すべてのリモートソフトウェアクライアントおよび VPN 3002 Hardware Client に適用されます。

Address Pool Hold Down Routes フィールドに、VPN Concentrator のルーティング テーブルに追加するホールドダウン ルートを入力します。ルートを自動的または手入力を入力できます。

- 現在設定されているアドレス プールに基づいて、ホールドダウン ルートのリストを自動的に生成するには、**Generate Hold Down Routes** ボタンをクリックします。その後、必要に応じてこのリストを編集できます。
- 手動でルートを入力する場合は、*n.n.n.n/n.n.n.n* という形式を使用します (例: 192.168.90.64/255.255.255.192)。ネットワーク アドレスとサブネット マスクのペアを、1 行につき 1 つずつ入力してください。

Client Reverse Route Injection フィールドと Address Pool Hold Down Routes フィールドを両方とも設定する場合、リモートクライアントが VPN Concentrator に接続すると、VPN Concentrator は、最初に、クライアントアドレスが、ここにリストされているアドレス プール ルートのいずれかに該当するかどうかを調べます。該当しない場合、VPN Concentrator は、クライアントのルートルーティングテーブルに追加します。

Generate Hold Down Routes



(注) Address Pool Hold Down Routes ウィンドウにエントリを入力した場合、このボタンをクリックすると、入力したエントリが消去されます。以前のエントリを保持する場合は、そのエントリをファイルまたはクリップボードにコピーし、Generate Hold Down Routes ボタンをクリックした後、貼り付けて元に戻します。

Address Pool Hold Down Routes ウィンドウ内の設定済みアドレス プールに基づいて、ホールドダウン ルートを自動的に表示させるには、**Generate Hold Down Routes** ボタンをクリックします。

Apply / Cancel

Reverse Route Injection の設定値を適用し、アクティブ コンフィギュレーションに組み込む場合は、**Apply** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

注意：

アクティブ コンフィギュレーションを保存し、ブート コンフィギュレーションにするには、VPN Concentrator Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

入力内容を破棄する場合は、**Cancel** をクリックしてください。表示画面は、Configuration | System | IP Routing の画面に戻ります。

