Reverse Route Injection 機能を使用してダイナミック ルートを読み込む方法

内容

概要
前提条件
要件
使用するコンポーネント
表記法
背景説明
設定
ネットワーク図
設定
RIPv2 を使用するVPN 3000 コンセントレータの設定
Client Reverse Route Injection
ネットワーク拡張RRI (NEM だけのVPN 3002 クライアント)
LAN-to-LANネットワーク自動検出
LAN-to-LANネットワークRRI
ホールドダウンルート
RRIでのOSPFの使用
確認
RIPv2の確認/テスト
LAN-to-LANネットワーク自動検出の確認/テスト
LAN-to-LANネットワークRRIの確認/テスト
ホールドダウンルートの確認およびテスト
RRIのOSPFの確認およびテスト
VPNコンセントレータのルーティングテーブル情報の確認
トラブルシュート
関連情報

概要

Reverse Route Injection(RRI)は、リモートVPNクライアントまたはLAN-to-LANセッション用にOpen Shortest Path First(OSPF)プロトコルまたはRouting Information Protocol(RIP)を実行する内部ルータのルーティングテーブルを設定するために使用されます。RRI は、VPN 3000 コンセントレータ シリーズ (3005 ～ 3080) のバージョン 3.5 以降で導入されました。RRI は VPN コンセントレータとしてではなく VPN Client として取り扱われるため、RRI は VPN 3002 Hardware Client には搭載されていません。VPN コンセントレータだけが RRI ルートをアドバタイズできます。ネットワーク拡張ルートをメインの VPN コンセントレータに注入して戻すには、VPN 3002 Hardware Client でコードのバージョン 3.5 以降を実行する必要があります。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン3.5が稼働するCisco VPN 3000コンセントレータ
- Cisco IOS® ソフトウェア リリース 12.2.3 を実行している Cisco 2514 ルータ
- ソフトウェア バージョン 3.5 以降を実行している Cisco VPN 3002 ハードウェア クライアント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

背景説明

RRI の使用方法には、次の 4 つの方法があります。

- VPN ソフトウェア クライアントは、割り当てられた IP アドレスをホスト ルートとして挿入します。
- VPN 3002 ハードウェア クライアントは、Network Extension Mode（NEM）を使って接続を確立し、保護されているネットワーク アドレスを挿入します（Port Address Translation（PAT; ポート アドレス変換）モードの VPN 3002 ハードウェア クライアントは、単に VPN クライアントとして処理されるという点に注意してください）。
- LAN-to-LANリモートネットワーク定義は、挿入されたルートです。（これは単一のネットワークの場合もあれば、ネットワーク リストの場合もあります）。
- RRI は、VPN クライアントにホールドダウン ルートを提供します。

RRIが使用されている場合、RIPまたはOSPFを使用してこれらのルートをアドバタイズできます。以前のバージョンのVPNコンセントレータコードでは、LAN-to-LANセッションでネットワーク自動検出を使用できます。ただし、このプロセスでは、RIPをアドバタイジングルーティングプロトコルとしてのみ使用できます。

注：RRIは Virtual Router Redundancy Protocol(VRRP)では使用できません。これは、マスターサーバとバックアップサーバの両方がRRIルートをアドバタイズするためです。これにより、ルーティングの問題が発生する可能性があります。登録ユーザは、この問題の詳細をCisco Bug ID CSCdw30156（登録ユーザ専用）に記載しています。

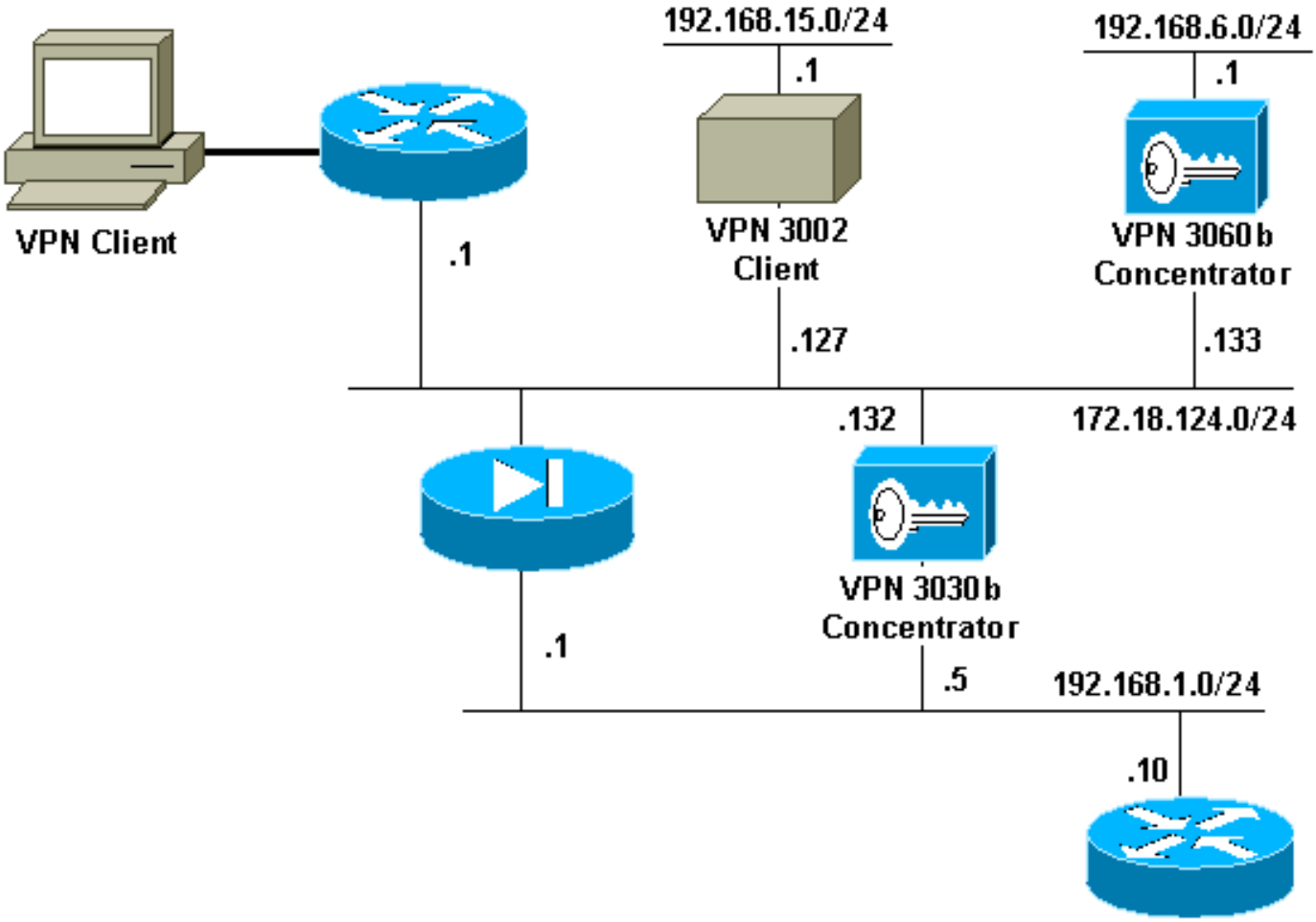
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

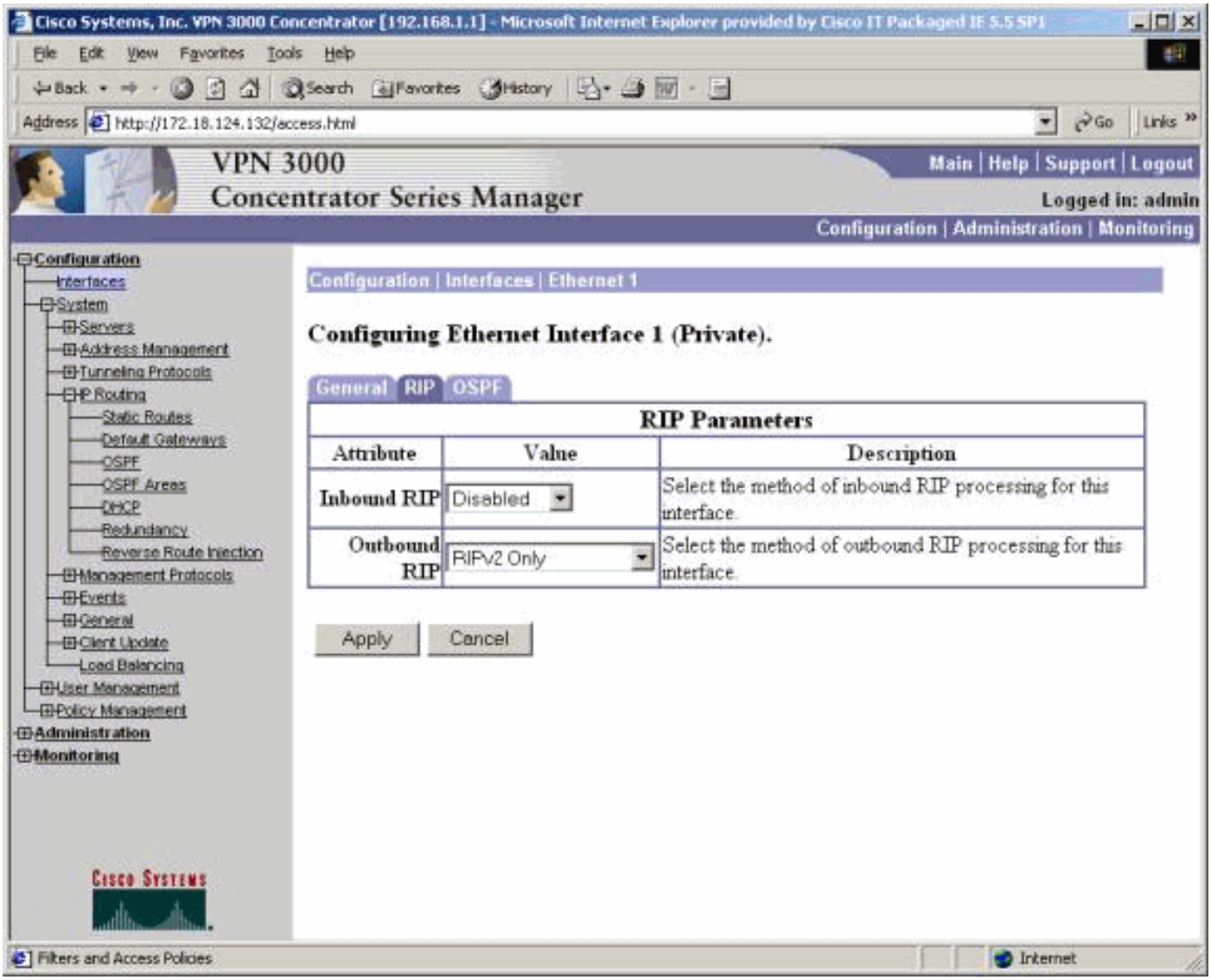
ルータの設定

```
2514-b#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IK8OS-L), Version 12.2(3),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 18-Jul-01 20:14 by pwade
Image text-base: 0x0306B450, data-base: 0x00001000

2514-b#write terminal
```

```
Building configuration...

 Current configuration : 561 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2514-b
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
interface Ethernet0
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.1.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip http server
!
line con 0
line aux 0
line vty 0 4
!
end
```

RIPv2 を使用するVPN 3000 コンセントレータの設定

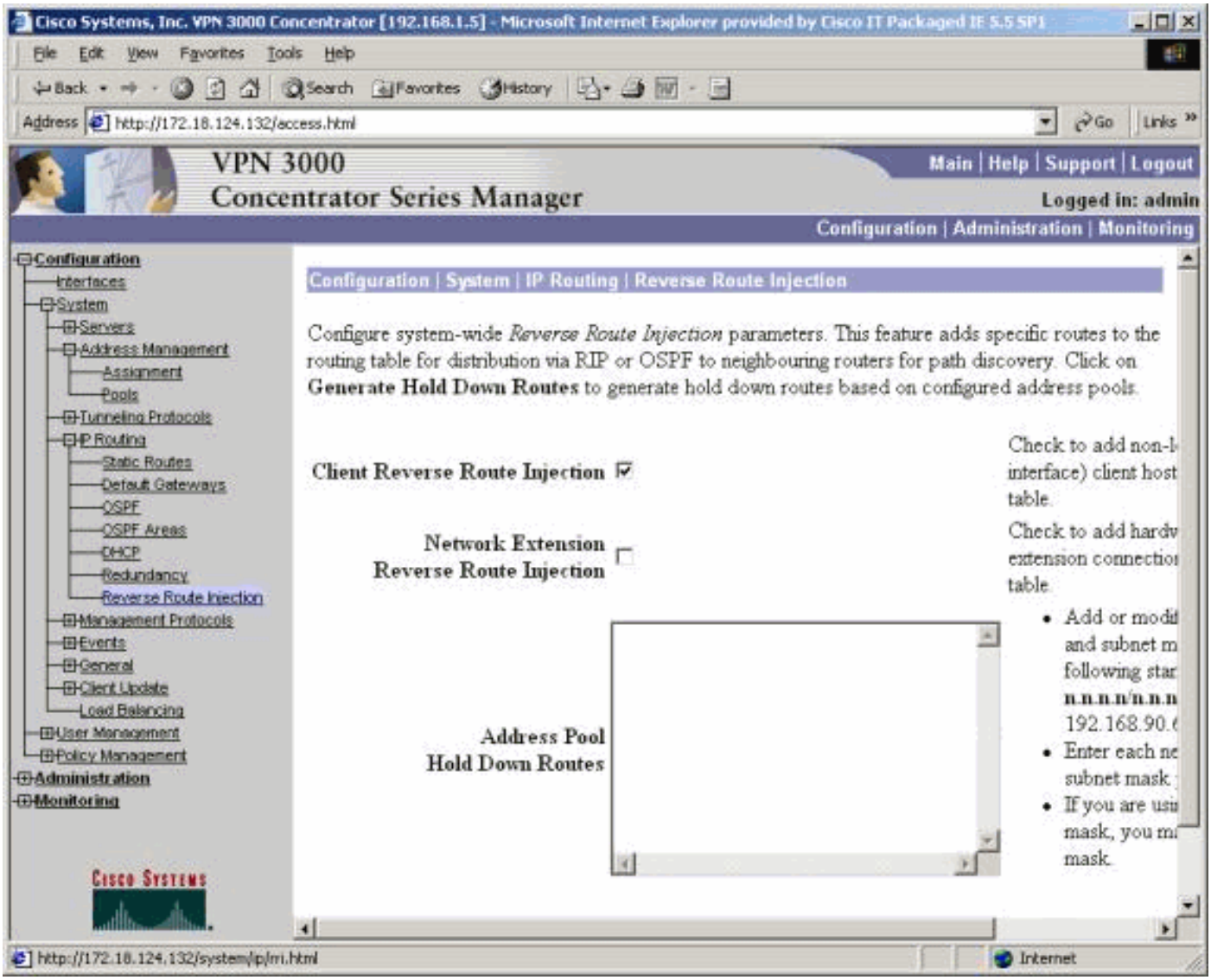
RRI学習ルートをアドバタイズするには、ローカルVPNコンセントレータ（ネットワークダイアグラムではVPN 3030bで表される）のプライベートインターフェイスで（最低でも）アウトバウンドRIPを有効にする必要があります。 ネットワーク自動検出を使用するためには、発信 RIP と着信 RIP の両方をイネーブルにする必要があります。クライアントRRIは、VPNコンセントレータに接続するすべてのVPNクライアント(VPN、レイヤ2トンネルプロトコル(L2TP)、ポイントツーポイントトンネリングプロトコル(PPTP)など)で使用できます。



Client Reverse Route Injection

クライアント RRI は、VPN コンセントレータに接続されているすべての VPN クライアントで使用できます。クライアントRRIを設定するには、**[Configuration] > [System] > [IP Routing] > [Reverse Route Injection]の順に選択**し、**[Client Reverse Route Injection]のオプションを選択します**。

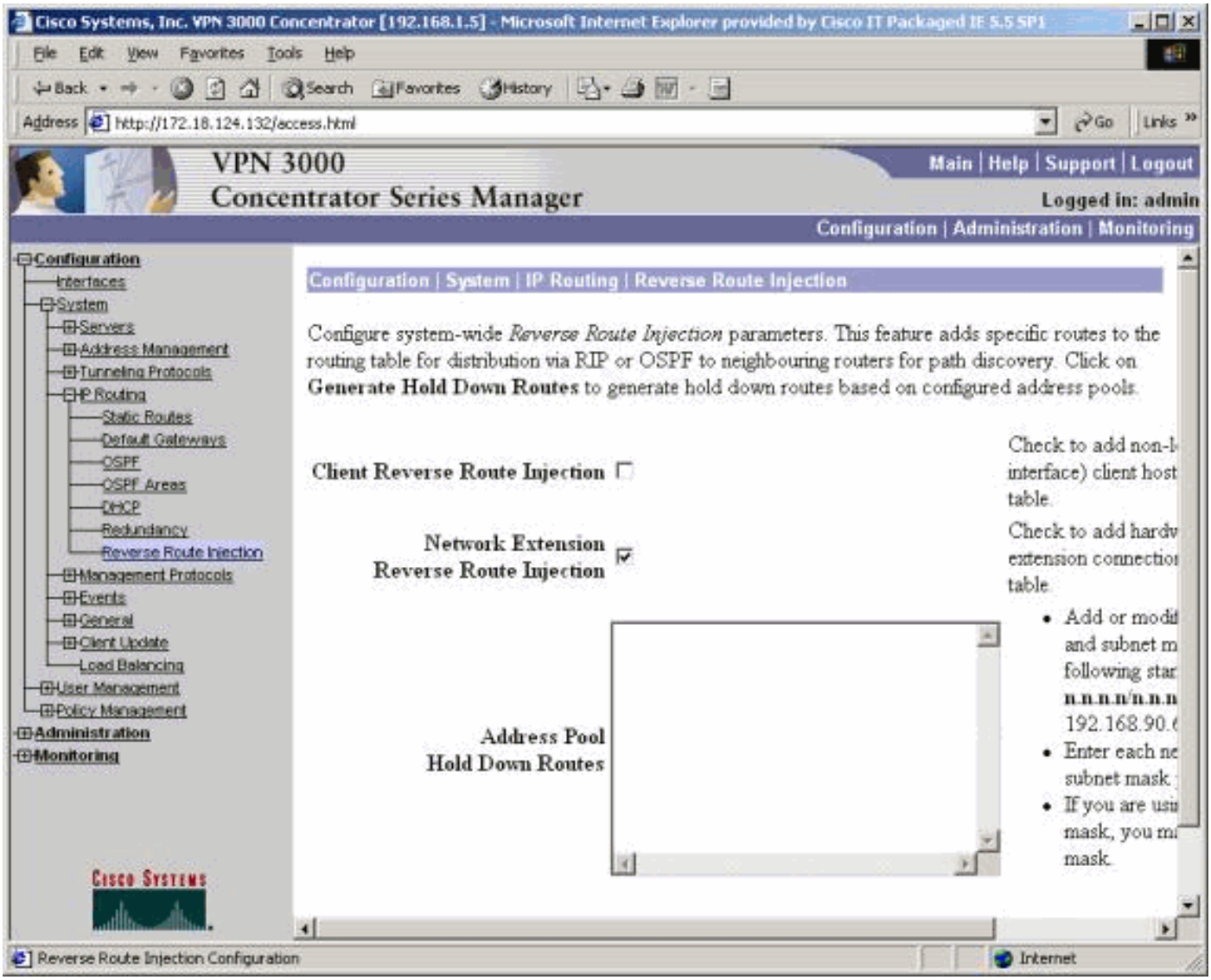
注：VPNコンセントレータには、グループとユーザが定義され、クライアントプールは192.168.3.1 ~ 192.168.3.254です。ルーティングテーブルの詳細については、「RIPv2の確認/テスト」を参照してください。



ネットワーク拡張RRI (NEM だけのVPN 3002 クライアント)

VPN 3002 Clientのネットワーク拡張RRIを設定するには、**[Configuration] > [System] > [IP Routing] > [Reverse Route Injection]の順に進み、[Network Extension Reverse Route Injection]オプションを選択します。**

注：ネットワーク拡張RRIが機能するには、VPN 3002クライアントで3.5以降のコードを実行する必要があります。ルーティングテーブル[の情報については、「NEM RRIの確](#)認/テスト」を参照してください。



LAN-to-LANネットワーク自動検出

これは、ローカルLAN上のネットワーク192.168.6.0/24をカバーするリモートピア172.18.124.133とのLAN-to-LANセッションです。LAN-to-LANの定義内で(**[Configuration] > [System] > [Tunneling Protocols] > [IPSec] > [LAN-to-LAN] > [Routing]を選択**)、ネットワークリストの代わりにネットワーク自動検出が使用されます。

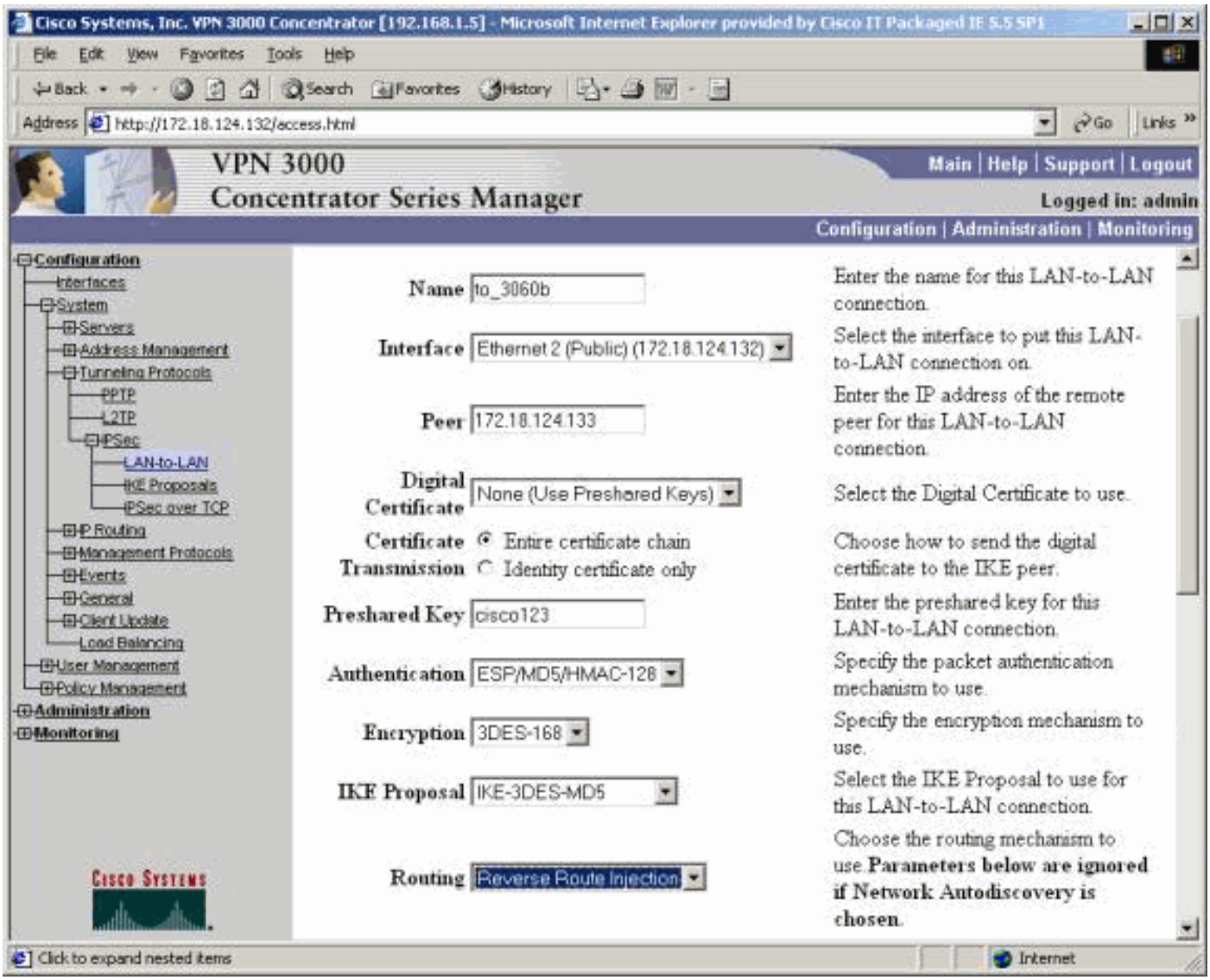
注：ネットワーク自動検出を使用する場合は、リモートネットワークアドレスのアドバタイズにRIPのみを使用できます。この場合、RRIの代わりに通常の自動検出が使用されます。ルーティングテーブルの情報については、「LAN-to-LANネットワークの自動検出の確認/テスト」を参照してください。

LAN-to-LANネットワークRRI

RRIを設定するには、**[Configuration] > [System] > [Tunneling Protocols] > [IPSec]に移動します。**LAN-to-LAN定義では、プルダウンメニューを使用して[Routing]フィールドを**[Reverse Route Injection]に設定**し、LAN-to-LANセッションで定義されたルートがRIPまたはOSPFプロセスに渡されるようにします。設定を保存するには、Apply をクリックします。

注：LAN-to-LAN定義がRRIを使用するように設定されている場合は、VPN 3000コンセントレータは、内部ルータがリモートネットワークから離れるように、リモートネットワーク（単一のネットワークまたはネットワークリスト）をアドバタイズします。ルーティングテーブルの詳細に

ついては、「LAN-to-LANネットワークRRIの確認/テスト」を参照してください。



CLIモードで設定するには、リモートLAN-to-LAN VPNネットワークの情報をOSPF実行ネットワークに注入する方法について、「ルーティングが正しいことを確認する」を参照してください。

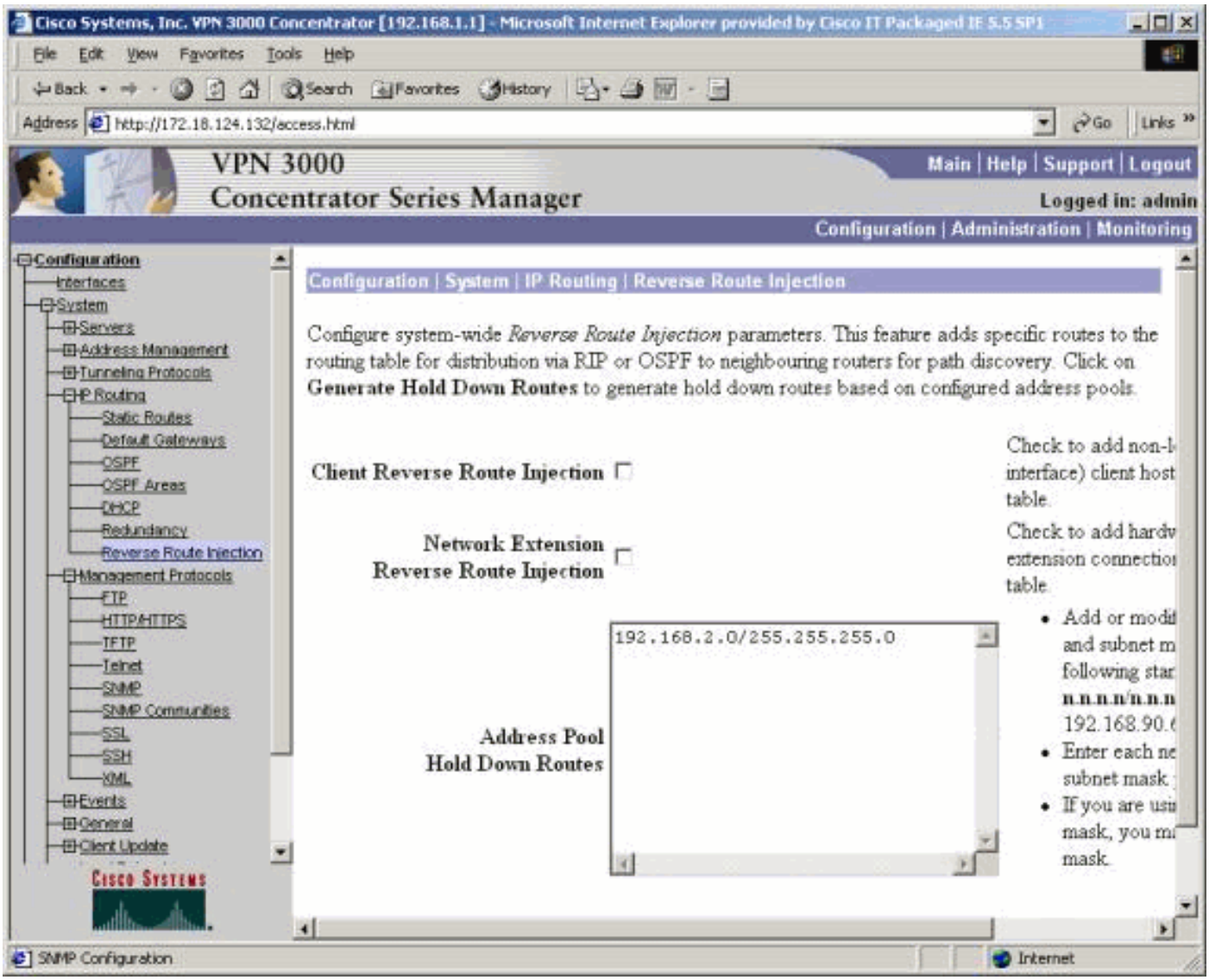
ホールドダウンルート

ホールドダウン ルートは、リモート ネットワークまたは VPN クライアント プールへのルートのプレース ホルダとして使われます。たとえば、リモートVPNピアが192.168.2.0/24ネットワークの前面にある場合、ローカルLANがそのネットワークを認識できる方法はいくつかあります。

- 内部ルータ（サンプルルータ設定の2514-bなど）には、VPNコンセントレータのプライベートアドレスを指す192.168.2.0/24のスタティックルートがあります。RRI の実行を望まない場合や、VPN コンセントレータがこの機能をサポートしていない場合、これは十分に受け入れられるソリューションです。
- ネットワーク自動検出を使用できます。ただし、これにより、VPNトンネルがアップ状態のときだけ、192.168.2.0/24ネットワークがローカルネットワークにプッシュされます。つまり、ローカル ネットワークではリモート ネットワークのルーティングに関する情報をまったく持たないため、ローカル ネットワークはトンネルを確立できないということです。192.168.2.0 リモート ネットワークによってトンネルが確立された場合、自動検出により、このトンネルによってネットワークが受け渡され、ルーティング プロセスに挿入されます。

これはRIPだけに適用されることに注意してください。この場合、OSPFは使用できません。
- Address Pool Hold Down Routes を使うと、トンネルが存在していない場合、ローカル ネットワークとリモート ネットワークの両方でトンネルを確立できるように、常に定義済みのネットワークがアドバタイズされます。

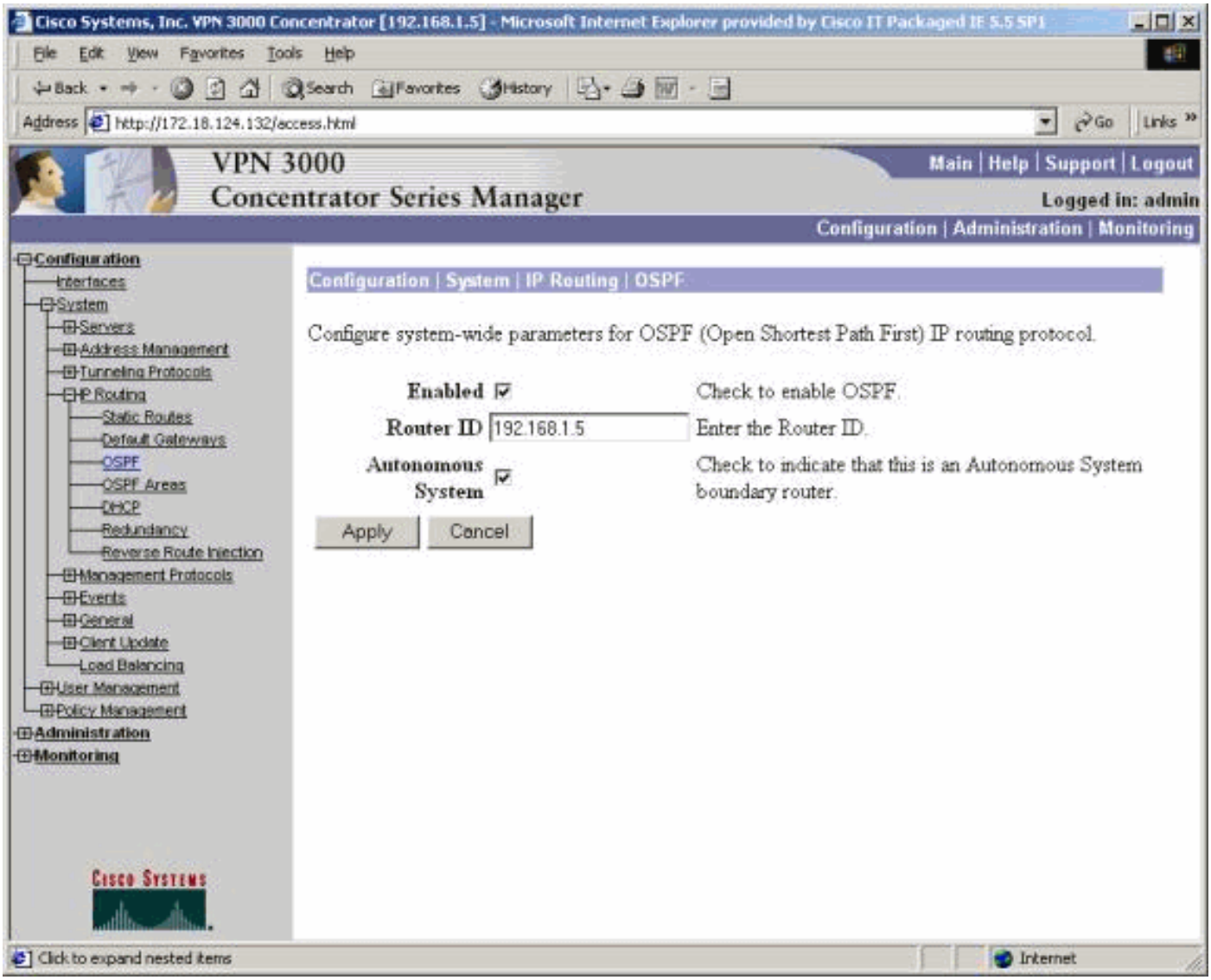
アドレスプールのホールドダウンルートを設定するには、次に示すように[Configuration] > [System] > [IP Routing] > [Reverse Route Injection]に移動し、アドレスプールを入力します。ルーティングテーブルの情報については、「ホールドダウンルートの確認/テスト」を参照してください。

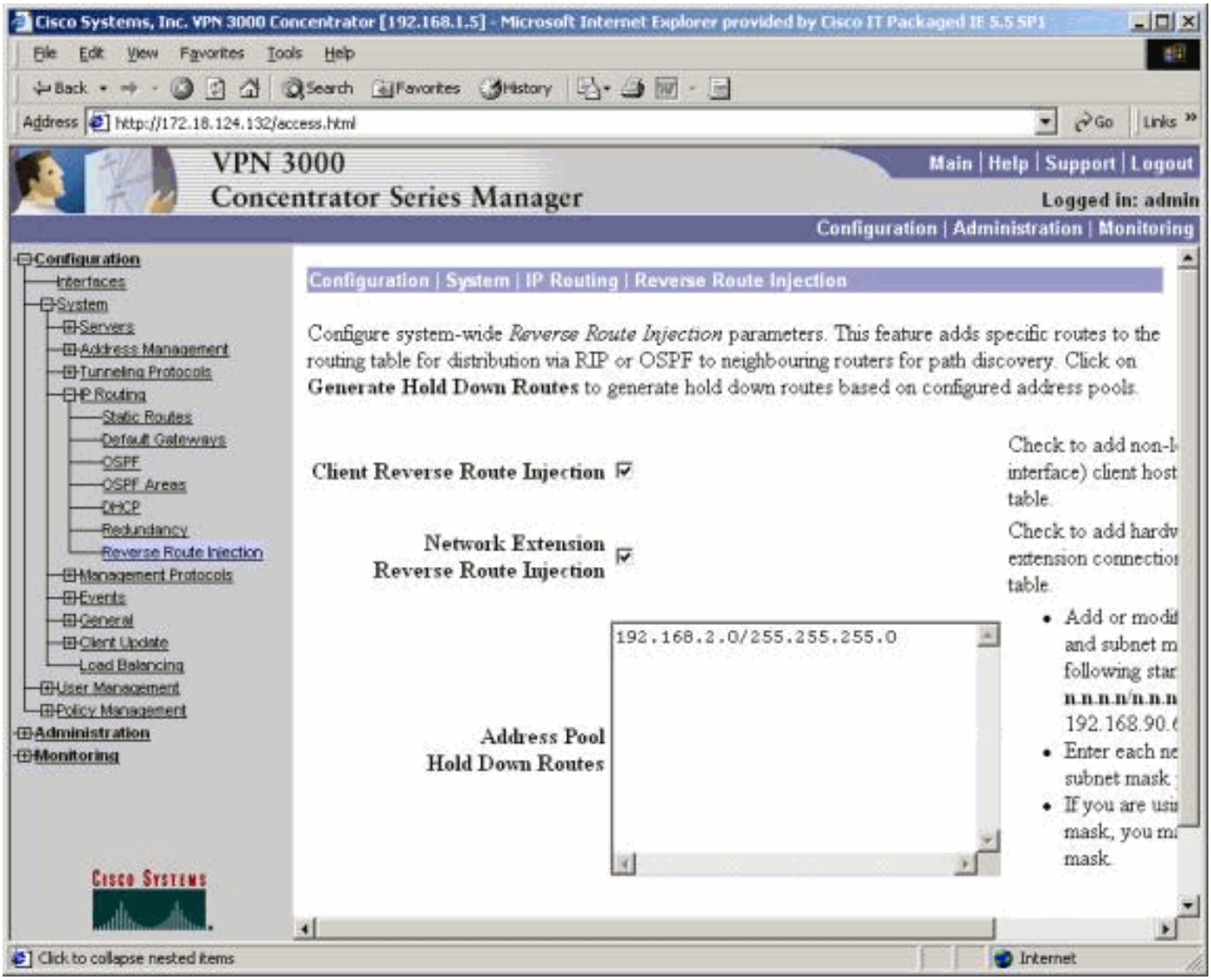


RRIでのOSPFの使用

OSPFを使用するには、[Configuration] > [System] > [IP Routing] > [OSPF]の順に選択し、ルータ ID（IPアドレス）を入力します。 Autonomous System と Enabled の各オプションを選択します。RRI ルートを OSPF テーブルに挿入するには、VPN 3000 コンセントレータ上の OSPF プロセスを自律システムにする必要があります。

ルーティングテーブルの情報については、「RRIによるOSPFの確認/テスト」を参照してください。


Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.5] - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.18.124.132/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
IP Routing
Static Routes
Default Gateways
OSPF
OSPF Areas
DHCP
Redundancy
Reverse Route Injection
Management Protocols
Events
General
Client Update
Load Balancing
User Management
Policy Management
Administration
Monitoring
Configuration | System | IP Routing | OSPF
Configure system-wide parameters for OSPF (Open Shortest Path First) IP routing protocol.
Enabled
Check to enable OSPF.
Router ID
192.168.1.5
Enter the Router ID.
Autonomous System
Check to indicate that this is an Autonomous System boundary router.
Apply
Cancel
Cisco Systems
Click to expand nested items
Internet



確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

RIPv2の確認/テスト

VPN クライアントを接続する前のルーティング テーブル

VPN コンセントレータは、定義済みのグループおよびユーザ、そして 192.168.3.1 - 192.168.3.254 のクライアント プールを保持しています。

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
```

```
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

VPN クライアント接続中のルーティング テーブル

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:21, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
     192.168.3.0/32 is subnetted, 1 subnets
R       192.168.3.1 [120/1] via 192.168.1.5, 00:00:21, Ethernet0
     !--- 192.168.3.1 is the client-assigned IP address !--- for the newly connected VPN Client.
S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

2 台のクライアントが接続されている場合のルーティング テーブル

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
     192.168.3.0/32 is subnetted, 2 subnets
R       192.168.3.2 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
R       192.168.3.1 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

各VPN Clientにホストルートを追加すると、ルーティングテーブルで192.168.3.0/24のホールドダウンルートを使用する方が簡単になる場合があります。つまり、クライアントRRIを使用する250ホストルートと1つのネットワークホールドダウンルートの間で選択されます。

次に、ホールドダウンルートの使用例を示します。

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:13, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
```

```
     192.168.3.0/24 is subnetted, 1 subnets
R       192.168.3.0 [120/1] via 192.168.1.5, 00:00:14, Ethernet0
     !--- There is one entry for the 192.168.3.x network, !--- rather than 1 for each host for
the VPN pool. S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

NEM RRIの確認/テスト

ルータのルーティングテーブルを次に示します。

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

R    192.168.15.0/24 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
!--- This is the network behind the VPN 3002 Client. 172.18.0.0/24 is subnetted, 1 subnets R
172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0 C 192.168.1.0/24 is directly
connected, Ethernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

LAN-to-LANネットワーク自動検出の確認/テスト

LAN-to-LAN接続前のルーティングテーブル（ネットワーク自動検出）

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:07, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

LAN-to-LAN（ネットワーク自動検出）中のルーティングテーブル（内部ルータ）

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 1 subnets
```

```
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:04, Ethernet0
R    192.168.6.0/24 [120/2] via 192.168.1.5, 00:00:04, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

注：RIPには3分間のホールドダウンタイマーがあります。LAN-to-LANセッションがドロップされても、ルートが実際にタイムアウトするまで約3分かかります。

LAN-to-LANネットワークRRIの確認/テスト

ルータのルーティングテーブルを次に示します。

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:11, Ethernet0
R    192.168.6.0/24 [120/1] via 192.168.1.5, 00:00:11, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

192.168.6.0/24はLAN-to-LANリモートネットワークリストで使用されているため、この情報はルーティングプロセスに渡されます。192.168.6.x、.7.xおよび.8.x (すべての/24)のネットワークリストがあったら、ルータのルーティング テーブルは以下のようになります：

```
R    192.168.8.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
R    192.168.6.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
R    192.168.7.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
...
```

ホールドダウンルートの確認およびテスト

この例では、192.168.2.0 はプレース ホルダとして使用するリモート ネットワークです。デフォルトでは、ホールドダウンプールを有効にした後の内部ルータのルーティングテーブルには次のように表示されます。

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
R    192.168.2.0/24 [120/1] via 192.168.1.5, 00:00:06, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

172.18.124.0 ルートは実際は、VPN 3000 コンセントレータの外部のパブリック インターフェイス ネットワークであるという点に注意してください。このルートをVPNコンセントレータのプラ

イベートインターフェイス経由で学習したくない場合は、スタティックルートまたはルートフィルタを追加して、この学習ルートを書き換えたりブロックしたりします。

192.168.1.1の企業ファイアウォールを指すスタティックルートを使用すると、次に示すように、ルーティングテーブルがip route 172.18.124.0 255.255.255.0 192.168.1.1を使用していると示されます。

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 1 subnets
S       172.18.124.0 [1/0] via 192.168.1.1
C    192.168.1.0/24 is directly connected, Ethernet0
R    192.168.2.0/24 [120/1] via 192.168.1.5, 00:00:28, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

RRIのOSPFの確認およびテスト

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

O E2 192.168.15.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
O E2 192.168.6.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
O E2 192.168.2.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
     192.168.3.0/32 is subnetted, 1 subnets
O E2    192.168.3.1 [110/20] via 192.168.1.5, 00:00:08, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

この例の値を次に示します。

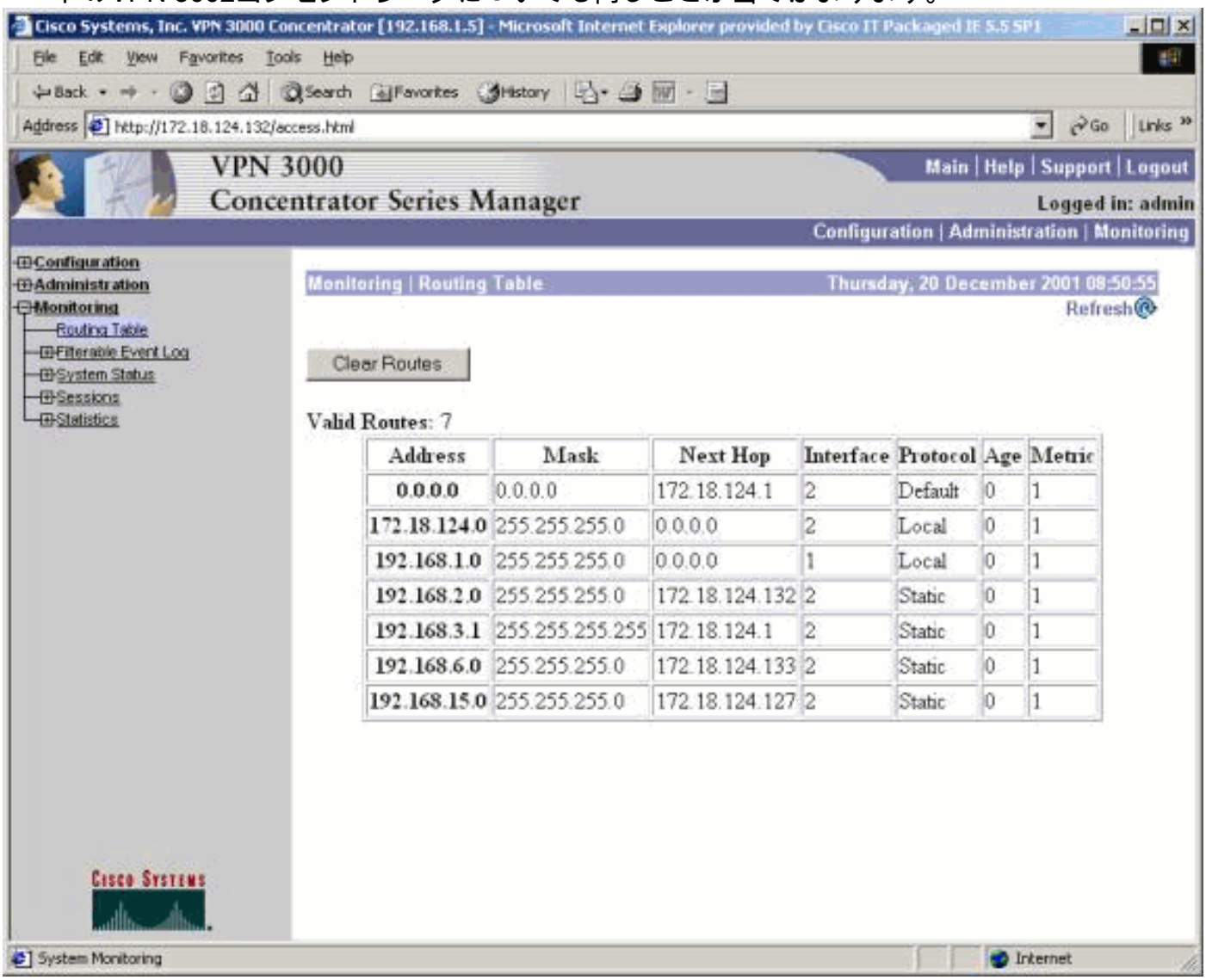
- *192.168.15.0 は、VPN 3002 コンセントレータのネットワーク拡張モードです。*
- *192.168.6.0*は、LAN-to-LANセッションのネットワークです。
- *192.168.2.0 は、ホールドダウン ルートです。*
- *192.168.3.1 は、クライアント挿入ルートです。*

VPNコンセントレータのルーティングテーブル情報の確認

ローカル VPN コンセントレータのルーティング テーブルに、ルートが表示されることを確認します。これを確認するには、[Monitoring] > [Routing Table]に移動します。

RRI によって認識されたルートが、パブリック インターフェイス (インターフェイス #2) からのスタティック ルートであることが確認できます。 この例では、ルートは次のとおりです。

- ホールドダウン ルート (192.168.2.0) は、ネクストホップがパブリック インターフェイス (172.18.124.132.) の IP アドレスのネクストホップであることを示しています。
- 192.168.3.1 アドレスが割り当てられた VPN クライアントのネクストホップは、パブリック インターフェイス (172.18.124.1) 上の VPN コンセントレータのデフォルト ゲートウェイです。
- 192.168.6.0のLAN-to-LAN接続はピアアドレス172.18.124.133を示し、ネットワーク拡張モードのVPN 3002コンセントレータについても同じことが当てはまります。



トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- Cisco VPN 3000シリーズコンセントレータサポート
- Cisco VPN 3000シリーズクライアントサポート

- IPSec ネゴシエーション/IKE プロトコルのサポート
- OSPFサポート
- RIPサポート
- テクニカルサポート - Cisco Systems