Auffüllen dynamischer Routen mit der Injection durch die Umkehrroute

Inhalt

Einführung

Mit Reverse Route Injection (RRI) wird die Routing-Tabelle eines internen Routers gefüllt, auf dem das OSPF-Protokoll (Open Shortest Path First) oder das Routing Information Protocol (RIP) für Remote-VPN-Clients oder LAN-to-LAN-Sitzungen ausgeführt werden. RRI wurde in Version 3.5 und höher der VPN 300 Concentrator-Serie (3005-3080) eingeführt. RRI ist nicht im VPN 3002 Hardware Client enthalten, da es als VPN-Client und nicht als VPN-Concentrator behandelt wird. RRI-Routen können nur von VPN-Concentrators angekündigt werden. Der VPN 3002 Hardware-Client muss die Versionen 3.5 oder höher des Codes ausführen, um Netzwerkerweiterungsrouten zurück in den Haupt-VPN-Konzentrator zu injizieren.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco VPN 3000 Concentrator mit Softwareversion 3.5
- Cisco Router der Serie 2514 mit Cisco IOS® Software, Version 12.2.3
- Cisco VPN 3002 Hardware-Client mit Software-Version 3.5 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Hintergrundinformationen

RRI kann auf vier Arten verwendet werden:

- VPN-Software-Clients geben ihre zugewiesene IP-Adresse als Hostrouten ein.
- Ein VPN 3002 Hardware-Client stellt über den Network Extension Mode (NEM) eine Verbindung her und sendet seine geschützte Netzwerkadresse. (Beachten Sie, dass ein VPN 3002 Hardware-Client im PAT-Modus (Port Address Translation) wie ein VPN-Client behandelt wird.)
- LAN-zu-LAN Remote-Netzwerkdefinitionen sind die injizierten Routen. (Dabei kann es sich um eine einzelne Netzwerk- oder Netzwerkliste handeln.)
- RRI stellt eine Halteroute für VPN-Client-Pools bereit.

Bei Verwendung von RRI können diese Routen entweder über RIP oder OSPF angekündigt werden. Bei früheren Versionen des VPN Concentrator-Codes können LAN-zu-LAN-Sitzungen die automatische Netzwerkerkennung verwenden. Bei diesem Prozess kann RIP jedoch nur als Werberouting-Protokoll verwendet werden.

Hinweis: RRI kann nicht mit Virtual Router Redundancy Protocol (VRRP) verwendet werden, da sowohl der Master- als auch der Backup-Server die RRI-Routen ankündigen. Dies kann Routing-Probleme verursachen. Registrierte Kunden erhalten weitere Informationen zu diesem Problem unter Cisco Bug ID CSCdw30156 (nur registrierte Kunden).

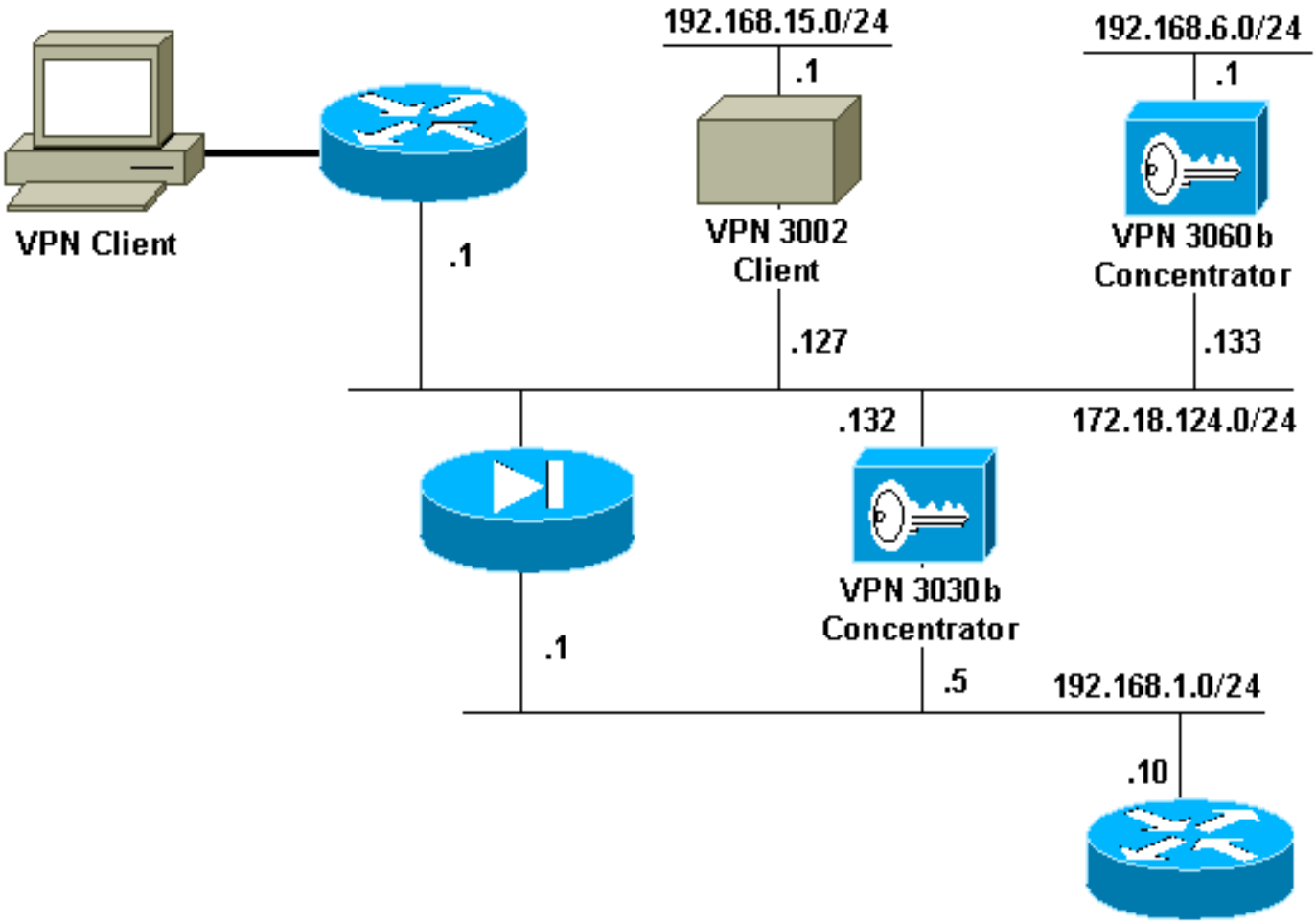
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

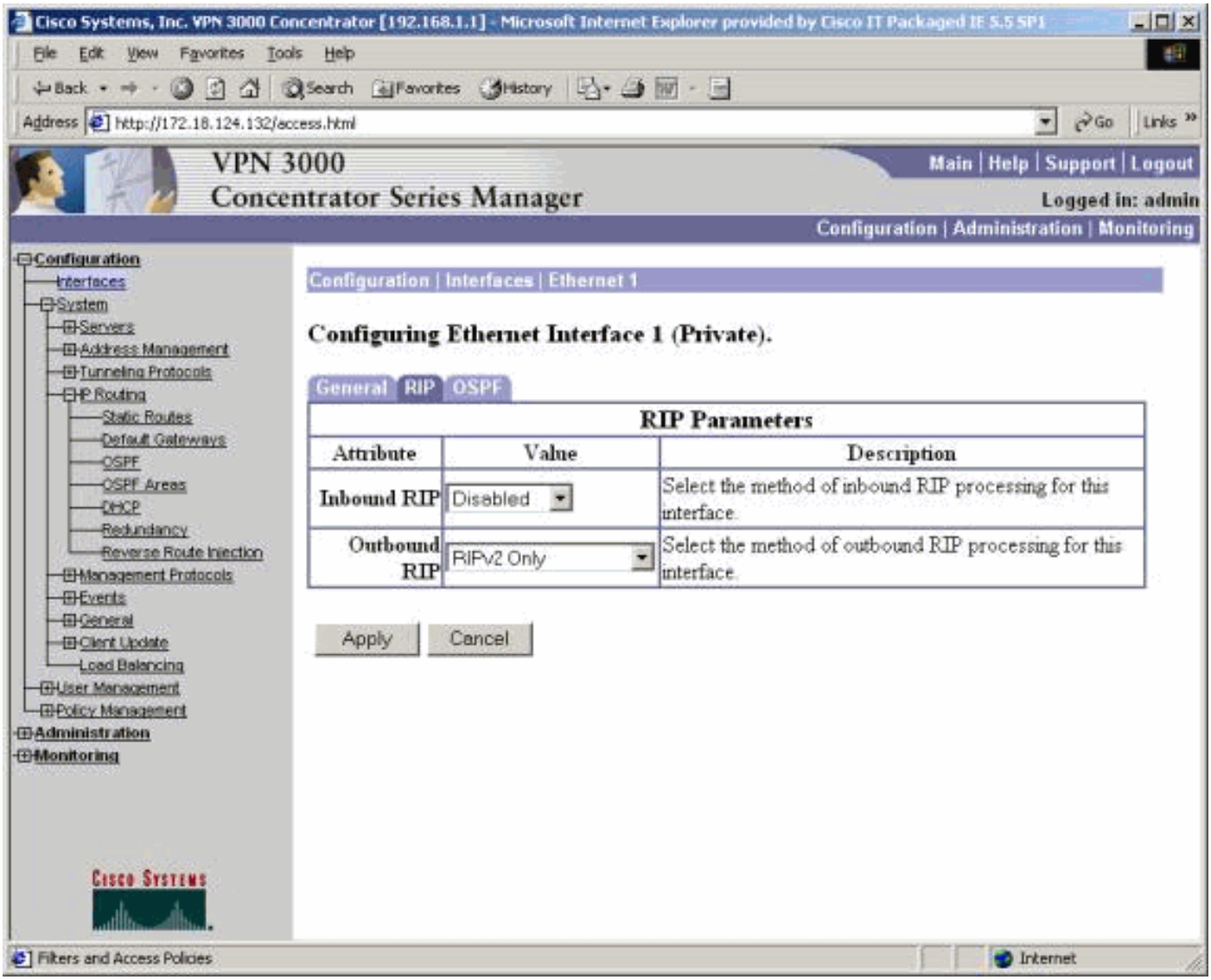
Routerkonfiguration

```
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
```

Konfiguration des VPN 3000-Konzentrators mit RIPv2

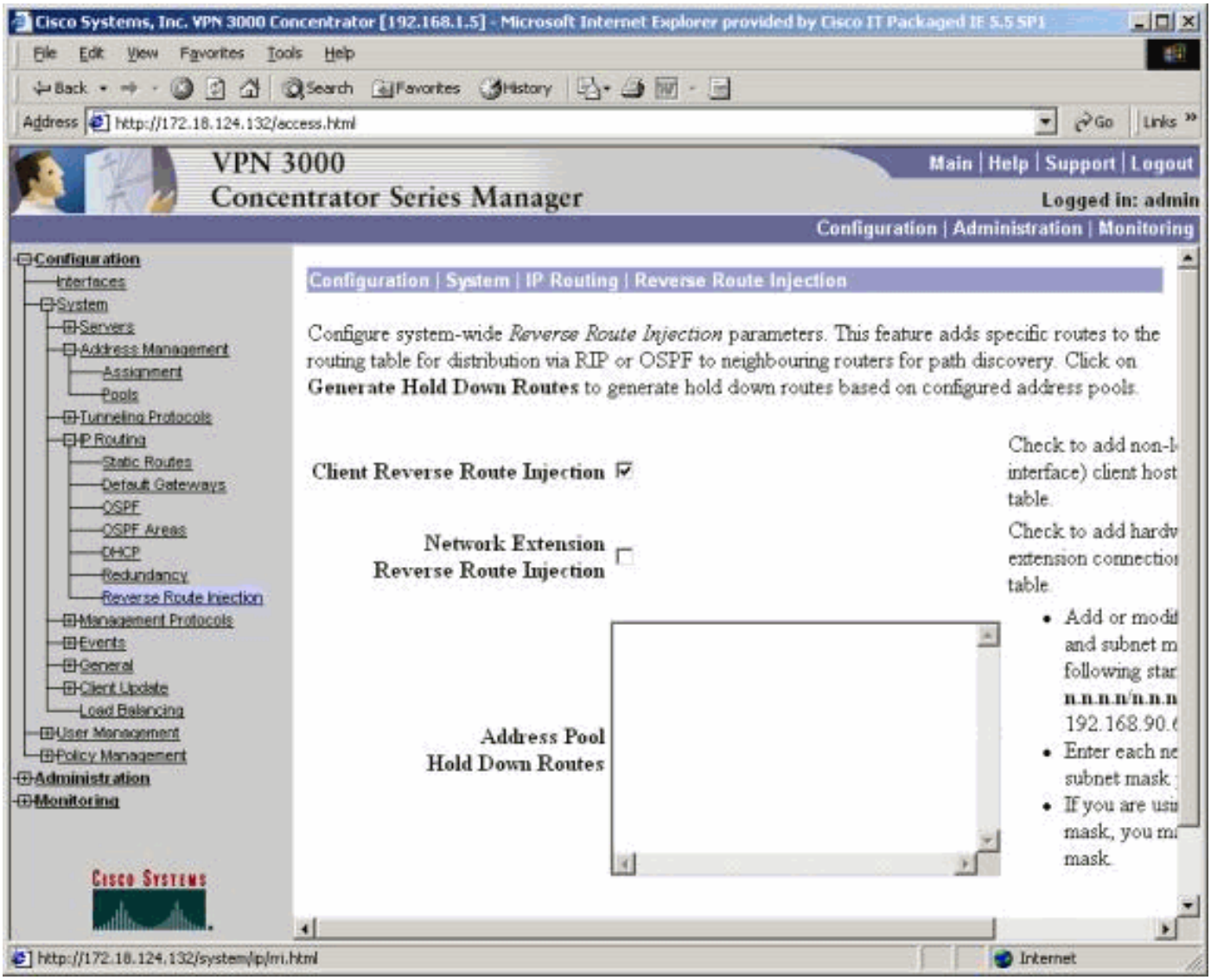
Um die von der RRI ermittelten Routen anzukündigen, muss auf der privaten Schnittstelle des lokalen VPN Concentrator (im Netzwerkdiagramm durch VPN 3030b dargestellt) ausgehender RIP (mindestens) aktiviert sein. Für die automatische Netzwerkerkennung muss sowohl ein- als auch ausgehender RIP aktiviert sein. Client RRI kann auf allen VPN-Clients verwendet werden, die mit dem VPN-Concentrator verbunden sind (z. B. VPN, Layer 2 Tunnel Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP) usw.).



Client Reverse Route Injection

Client RRI kann auf allen VPN-Clients verwendet werden, die mit dem VPN-Concentrator verbunden sind. Um Client RRI zu konfigurieren, gehen Sie zu **Configuration > System > IP Routing > Reverse Route Injection**, und wählen Sie die Option für **Client Reverse Route Injection aus**.

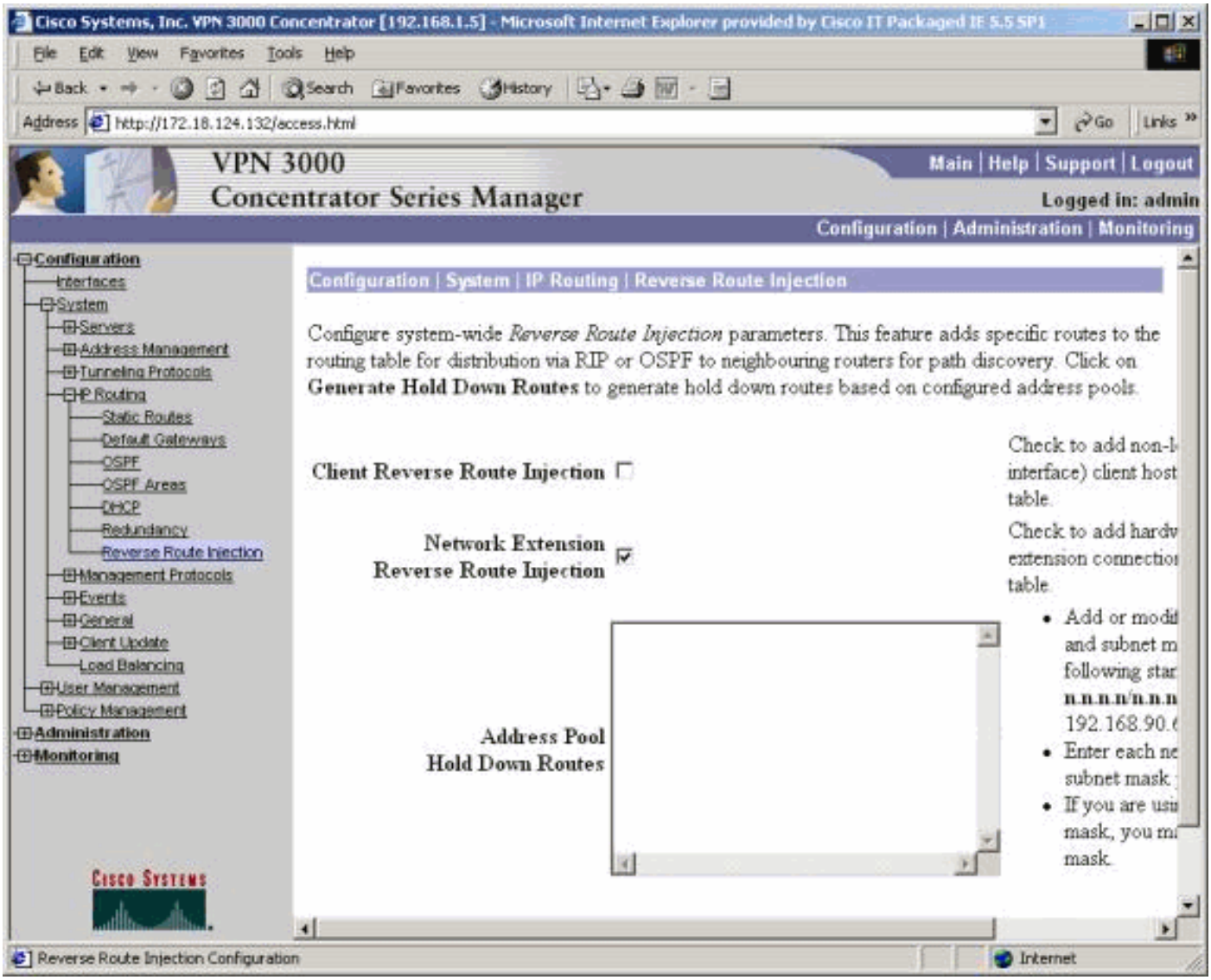
Hinweis: Die Gruppe und der Benutzer des VPN-Konzentrators sind definiert sowie ein Client-Pool von 192.168.3.1 bis 192.168.3.254. Weitere Informationen zur Routing-Tabelle finden Sie unter Prüfen/Testen von RIPv2.



RRI-Netzwerkerweiterung (nur VPN 3002-Client in NEM)

Um die RRI der Netzwerkerweiterung für den VPN 3002-Client zu konfigurieren, gehen Sie zu **Configuration > System > IP Routing > Reverse Route Injection**, und wählen Sie die Option für **Network Extension Reverse Route Injection aus**.

Hinweis: Der VPN 3002-Client muss Code 3.5 oder höher ausführen, damit der RRI für die Netzwerkerweiterung funktioniert. Informationen zur Routing-Tabelle finden Sie unter Verifizieren/Testen des NEM-RRI.



Automatische Erkennung von LAN-zu-LAN-Netzwerken

Dies ist eine LAN-zu-LAN-Sitzung mit einem Remote-Peer von 172.18.124.133, der das Netzwerk 192.168.6.0/24 im lokalen LAN abdeckt. Innerhalb der LAN-to-LAN-Definition (wählen Sie **Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN > Routing**) wird die automatische Netzwerkerkennung anstelle von Netzwerklisten verwendet.

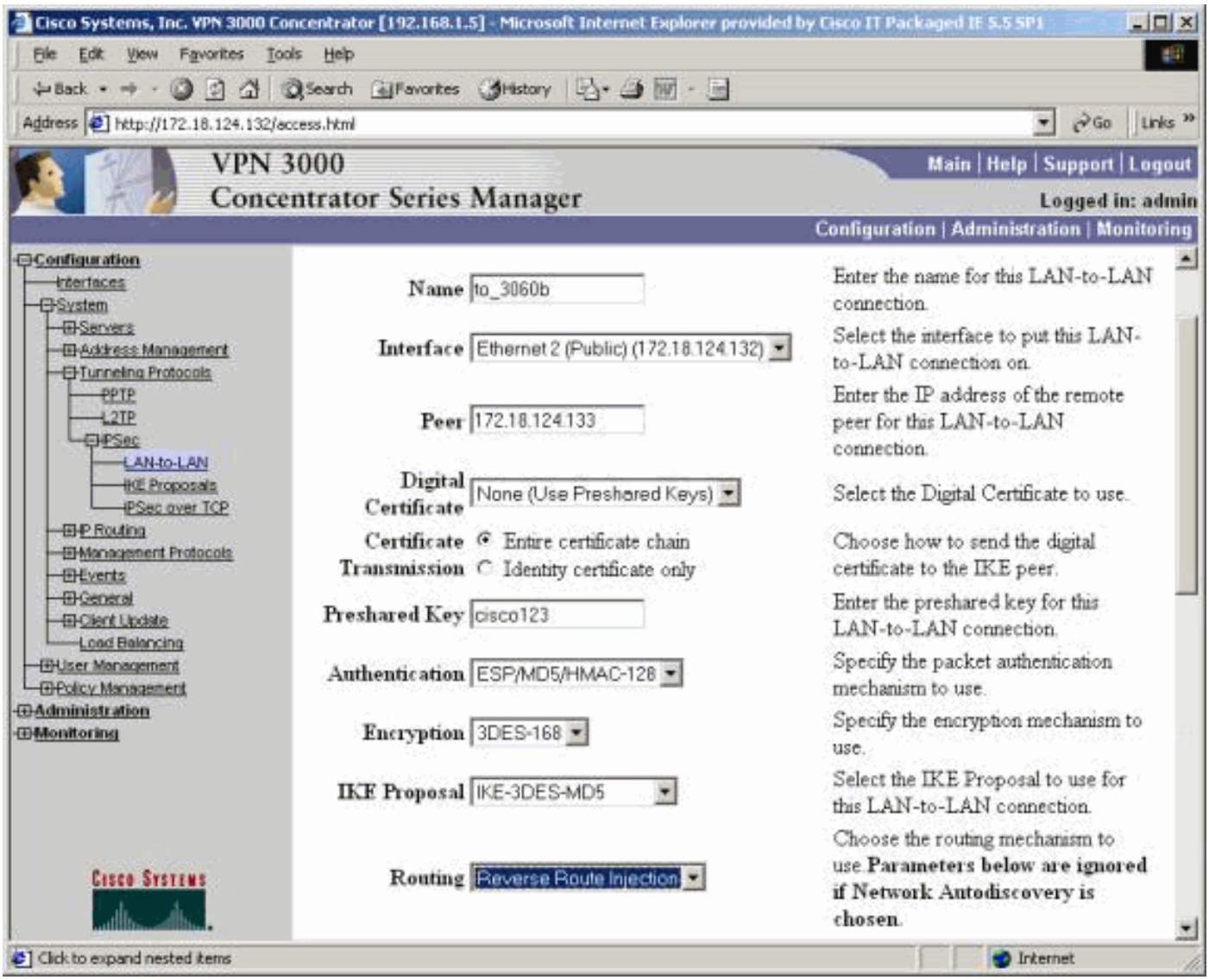
Hinweis: Denken Sie daran, dass nur RIP verwendet werden kann, um die Adresse des Remote-Netzwerks anzuzeigen, wenn die automatische Netzwerkerkennung verwendet wird. In diesem Fall wird statt RRI die normale automatische Erkennung verwendet. Informationen zur Routing-Tabelle finden Sie unter Verifizieren/Testen der Autodiscovery-Funktion für das LAN-zu-LAN-Netzwerk.

LAN-zu-LAN-Netzwerk-RRI

Um RRI zu konfigurieren, gehen Sie zu **Configuration > System > Tunneling Protocols > IPSec**. Verwenden Sie in der LAN-zu-LAN-Definition das Pulldown-Menü, um das Feld Routing auf **Reverse Route Injection** festzulegen, sodass die in der LAN-zu-LAN-Sitzung definierten Routen an den RIP- oder OSPF-Prozess weitergeleitet werden. Klicken Sie auf **Apply**, um die Einstellung zu speichern.

Hinweis: Wenn die LAN-zu-LAN-Definition auf die Verwendung von RRI festgelegt ist, informiert

der VPN 3000 Concentrator die Remote-Netzwerke (ein Netzwerk oder eine Netzwerkliste), sodass sich der interne Router nicht im Remote-Netzwerk befindet. Informationen zur Routing-Tabelle finden Sie unter RRI für das Verifizieren/Testen des LAN-zu-LAN-Netzwerks.



Informationen zur Konfiguration im CLI-Modus finden Sie unter Überprüfen der Richtigkeit des Routings, um die Informationen der VPN-Remote-LAN-zu-LAN-VPN-Netzwerke in das OSPF-laufende Netzwerk einzufügen.

Halten-Routen

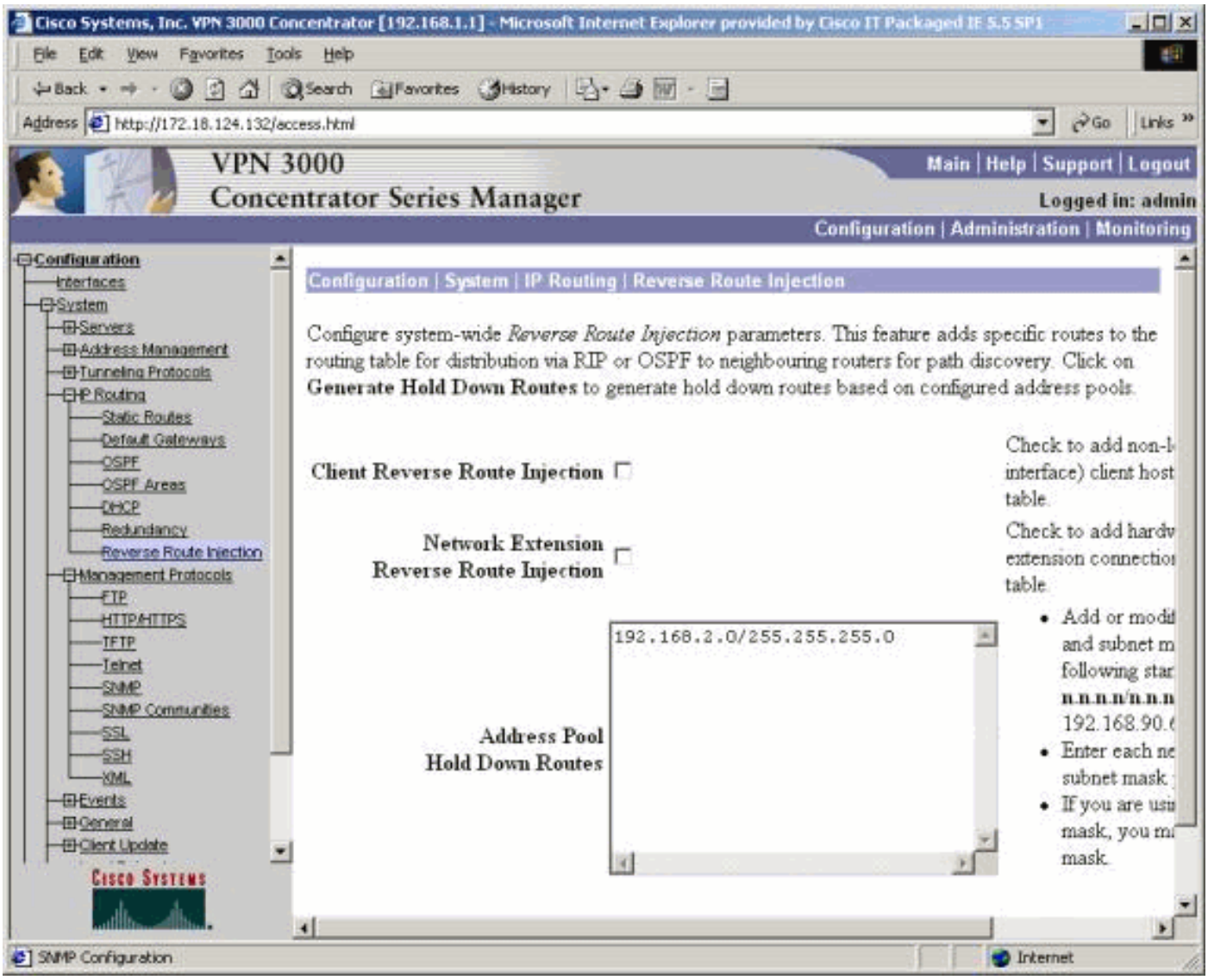
Hold-Down-Routen werden als Platzhalter für Routen zu Remote-Netzwerken oder VPN-Client-Pools verwendet. Wenn beispielsweise ein Remote-VPN-Peer das Netzwerk 192.168.2.0/24 frontiert, gibt es nur wenige Möglichkeiten, wie das lokale LAN dieses Netzwerk sehen kann:

- Der interne Router (z. B. 2514-b in der Beispiel-Routerkonfiguration) verfügt über eine statische Route für 192.168.2.0/24, die auf die private Adresse des VPN-Konzentrators verweist. Dies ist eine akzeptable Lösung, wenn Sie kein RRI ausführen möchten oder wenn der VPN Concentrator diese Funktion nicht unterstützt.
- Sie können die automatische Netzwerkerkennung verwenden. Dadurch wird das Netzwerk 192.168.2.0/24 jedoch nur dann in das lokale Netzwerk geleitet, wenn der VPN-Tunnel aktiv ist. Kurz gesagt: Das lokale Netzwerk kann den Tunnel nicht starten, da es keine Routing-

Kenntnisse über das Remote-Netzwerk hat. Sobald das Remote-Netzwerk 192.168.2.0 den Tunnel öffnet, durchläuft es das Netzwerk über die automatische Erkennung und injiziert es dann in den Routing-Prozess. Beachten Sie, dass dies nur für RIP gilt. In diesem Fall kann OSPF nicht verwendet werden.

- Bei Verwendung von **Adress Pool Hold-Routen** werden immer die definierten Netzwerke angekündigt, sodass sowohl das lokale als auch das Remote-Netzwerk den Tunnel öffnen können, wenn der Tunnel nicht vorhanden ist.

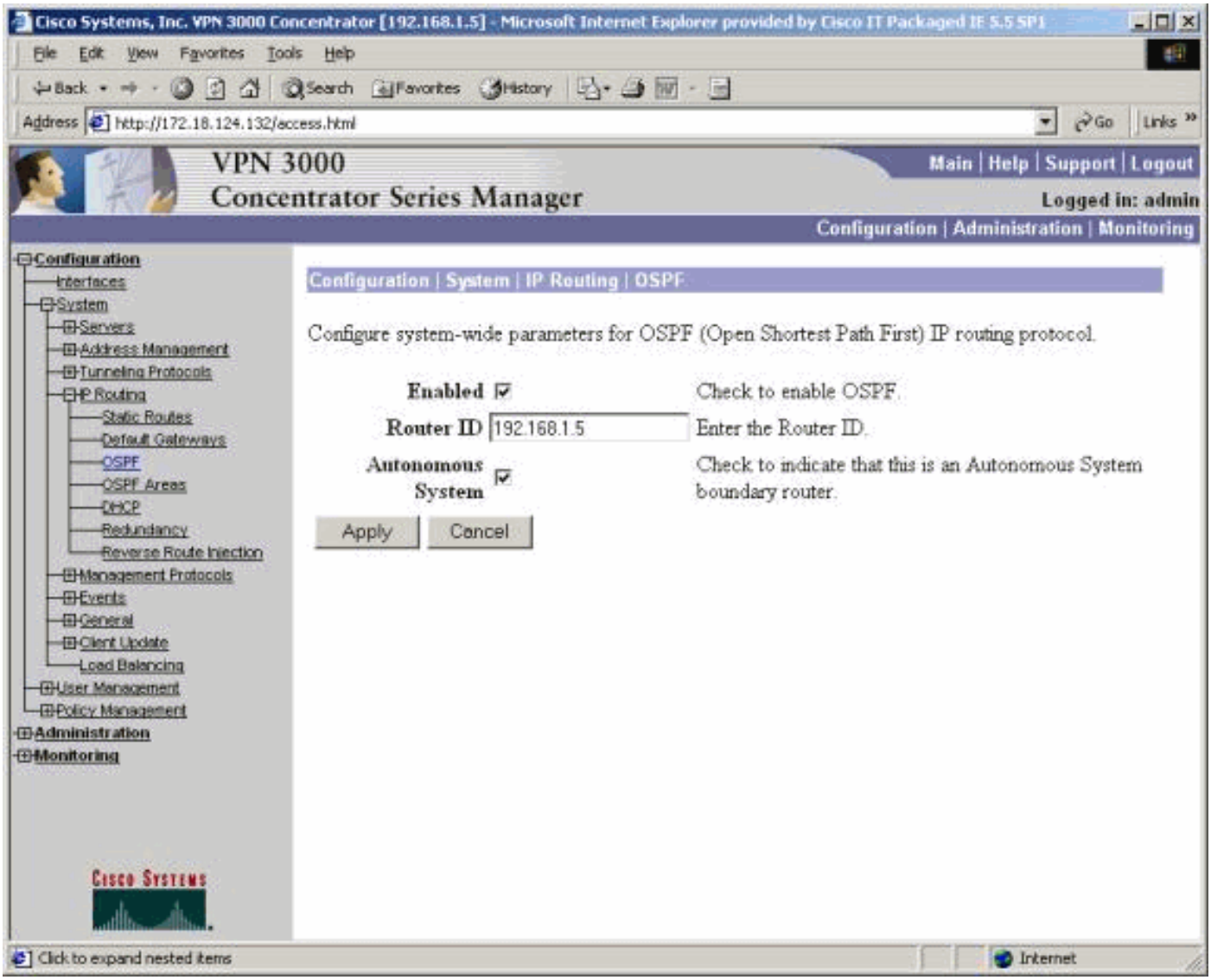
Um die **Routen** für die **Adress-Pool-Zurückstellung** zu konfigurieren, gehen Sie zu **Configuration > System > IP Routing > Reverse Route Injection**, und geben Sie den Adresspool ein, wie hier gezeigt. Informationen zur Routing-Tabelle finden Sie unter Routen zur Überprüfung/Teststellung.

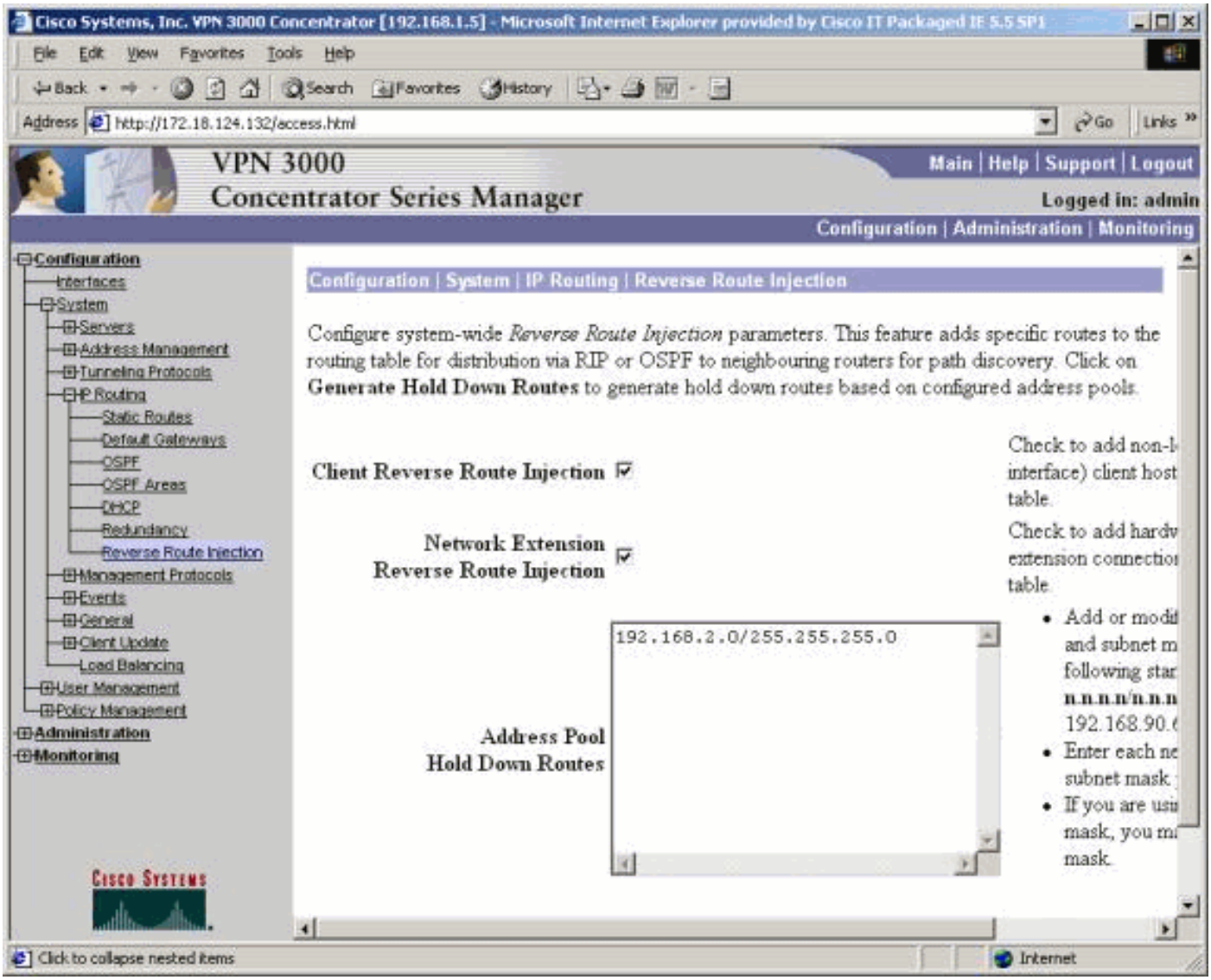


OSPF mit RRI verwenden

Um OSPF zu verwenden, gehen Sie zu **Configuration > System > IP Routing > OSPF**, und geben Sie dann die **Router-ID** (IP-Adresse) ein. Wählen Sie die Optionen für **Autonomous System** und **Enabled aus**. Beachten Sie, dass Sie zum Übertragen der RRI-Routen in die OSPF-Tabelle den OSPF-Prozess auf dem VPN 3000-Konzentrator als autonomes System festlegen müssen.

Informationen zur Routing-Tabelle finden Sie unter Verifizieren/Testen von OSPF mit RRI.


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



Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Überprüfen/Testen von RIPv2

Routing-Tabelle vor der VPN-Client-Verbindung

Für den VPN Concentrator ist eine Gruppe und ein benutzerdefinierter Client-Pool von 192.168.3.1 bis 192.168.3.254 definiert.

```
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
```

Routing-Tabelle während der VPN-Client-Verbindung

```
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
```

Routing-Tabelle, wenn zwei Clients verbunden sind

```
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
```

Wenn für jeden VPN-Client Hostrouten hinzugefügt werden, kann es für die Routing-Tabelle einfacher sein, eine Hold-Down-Route für 192.168.3.0/24 zu verwenden. Mit anderen Worten, es wird eine Wahl zwischen 250 Host-Routen, die Client RRI verwenden, und einer Netzwerk-Hold-Down-Route getroffen.

Im folgenden Beispiel wird die Verwendung einer Hold-Down-Route veranschaulicht:

```
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
```

Überprüfung/Test von NEM RRI

Die Routing-Tabelle des Routers ist wie folgt:

```
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
```

Automatische Erkennung von LAN-zu-LAN-Netzwerken überprüfen/testen

Routing-Tabelle vor LAN-zu-LAN-Verbindung (Automatische Erkennung des Netzwerks)

```
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
```

Routing-Tabelle (interner Router) während der LAN-zu-LAN-Erkennung (automatische Netzwerkerkennung)

```
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
```

Hinweis: RIP verfügt über einen Haltezeitgeber von drei Minuten. Obwohl die LAN-zu-LAN-Sitzung abgebrochen wurde, dauert es ungefähr drei Minuten, bis die Route tatsächlich eine Zeitüberschreitung durchläuft.

RRI für LAN-to-LAN-Netzwerk überprüfen/testen

Die Routing-Tabelle des Routers ist wie folgt:

```
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
```

Da 192.168.6.0/24 in der Liste der LAN-to-LAN-Remote-Netzwerke verwendet wurde, werden diese Informationen an den Routing-Prozess weitergeleitet. Wenn eine Netzwerkliste von 192.168.6.x, .7.x und .8.x vorhanden ist (alle /24), würde die Routing-Tabelle des Routers wie folgt aussehen:

```
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
...
```

Halten von Routen überprüfen/testen

In diesem Beispiel ist 192.168.2.0 das Remote-Netzwerk, das Sie als Platzhalter wünschen. Standardmäßig zeigt die Routing-Tabelle auf dem internen Router nach Aktivierung des Hold-Down-Pools Folgendes an:

```
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
```

Beachten Sie, dass die Route 172.18.124.0 das externe öffentliche Schnittstellennetzwerk des VPN 3000 Concentrator ist. Wenn Sie nicht möchten, dass diese Route über die private Schnittstelle des VPN Concentrator abgerufen wird, fügen Sie eine statische Route oder einen Routenfilter hinzu, um diese erfasste Route neu zu schreiben/zu blockieren.

Die Verwendung einer statischen Route, die auf die Corporate Firewall unter 192.168.1.1 zeigt, dass die Routing-Tabelle jetzt die **IP-Route 172.18.124.0 255.255.255.0 192.168.1.1** verwendet, wie folgt:

```
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
```

Verifizieren/Testen von OSPF mit RRI

```
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
```

Die Werte für dieses Beispiel sind wie folgt:

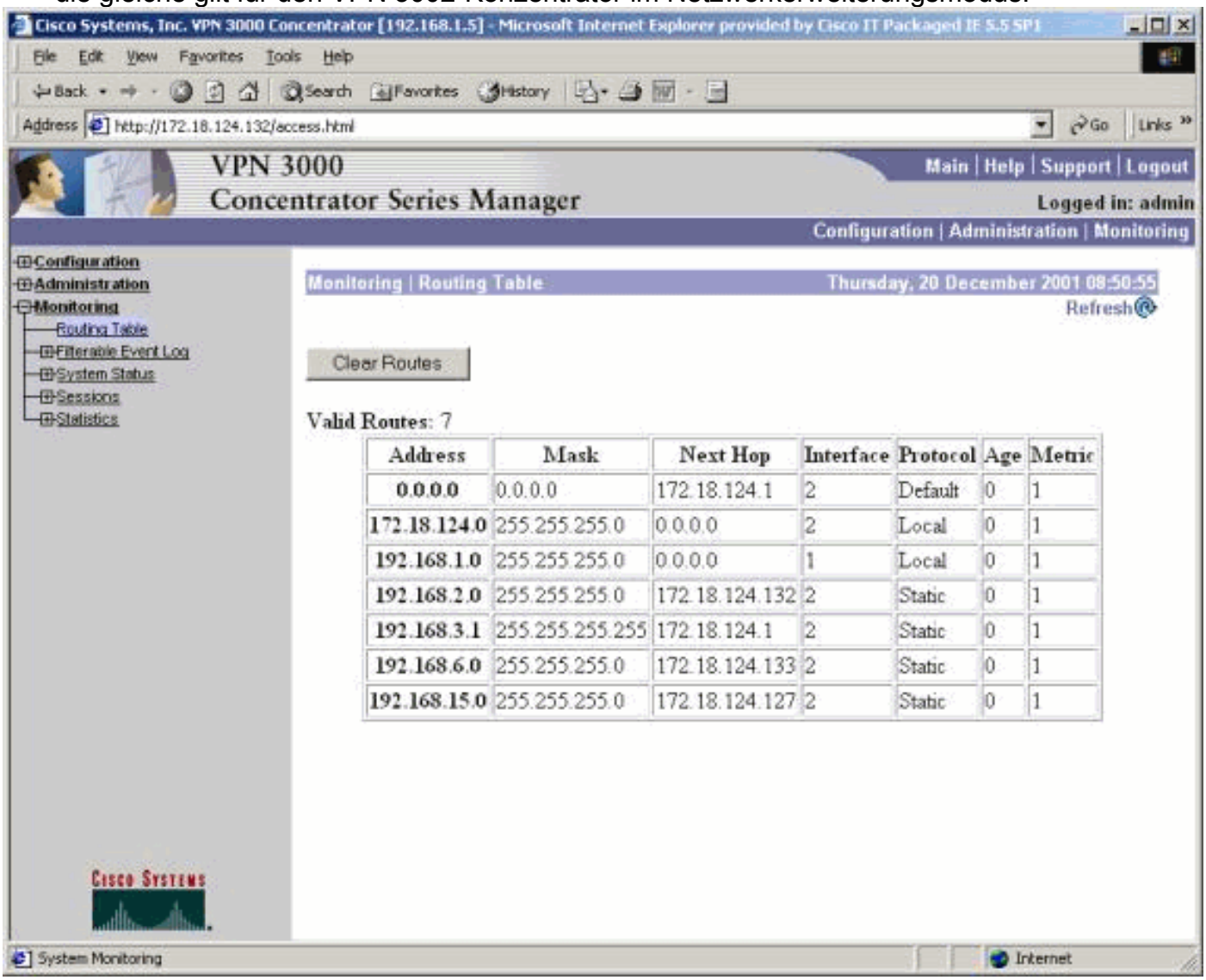
- *192.168.15.0* ist der Netzwerkerweiterungsmodus für den VPN 3002-Konzentrator.
- *192.168.6.0* ist das Netzwerk für die LAN-zu-LAN-Sitzung.
- *192.168.2.0* ist eine Halten-Down-Route.
- *192.168.3.1* ist eine vom Client injizierte Route.

Überprüfen der Informationen zur Routing-Tabelle im VPN Concentrator

Stellen Sie sicher, dass die Routen in der Routing-Tabelle im lokalen VPN Concentrator angezeigt werden. Um dies zu überprüfen, gehen Sie zu **Monitoring > Routing Table**.

Sie können die über RRI gelernten Routen als statische Routen von der öffentlichen Schnittstelle (Schnittstelle Nr. 2) sehen. In diesem Beispiel sind die Routen:

- Die Hold-Down-Route 192.168.2.0 zeigt, dass der nächste Hop der IP-Adresse der öffentlichen Schnittstelle 172.18.124.132 entspricht.
- Der VPN-Client, dem die Adresse 192.168.3.1 zugewiesen wurde, hat seinen nächsten Hop auf das Standard-Gateway für den VPN-Konzentrator im öffentlichen Netzwerk (172.18.124.1).
- Die LAN-zu-LAN-Verbindung unter 192.168.6.0 zeigt die Peer-Adresse 172.18.124.133 und die gleiche gilt für den VPN 3002-Konzentrator im Netzwerkerweiterungsmodus.



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- Cisco VPN Concentrator der Serie 3000 - Unterstützung
- Cisco VPN Client-Unterstützung der Serie 3000
- Unterstützung für IPSec-Aushandlung/IKE-Protokolle
- OSPF-Unterstützung
- RIP-Unterstützung
- Technischer Support - Cisco Systems