VPN 3000 Concentrator에서 이중화 라우팅 구성

목차

소개

이 문서에서는 원격 사이트에서 VPN 3000 Concentrator 또는 인터넷 연결이 끊길 경우 이중화 VPN 장애 조치를 구성하는 방법에 대해 설명합니다. 이 예에서는 VPN 3030B 뒤에 있는 기업 네트워크가 OSPF(Open Shortest Path First)를 기본 라우팅 프로토콜로 사용한다고 가정합니다.

참고: 라우팅 프로토콜 간에 재배포할 경우 네트워크에서 문제를 일으킬 수 있는 라우팅 루프를 형성할 수 있습니다. 이 예에서는 OSPF가 사용되지만 사용할 수 있는 라우팅 프로토콜만 사용할 수는 없습니다.

이 예제의 목적은 네트워크 다이어그램 섹션에 나와 있는 빨간색 터널(정상 작동 환경에서)을 사용하여 192.168.3.x에 도달하도록 192.168.1.0 네트워크를 설정하는 것입니다. 터널, VPN Concentrator 또는 ISP가 삭제되면 녹색 터널을 통해 동적 라우팅 프로토콜을 통해 192.168.3.0 네트워크가 학습됩니다. 또한 192.168.3.0 사이트로의 연결이 끊기지 않습니다. 문제가 해결되면 트래픽이 자동으로 빨간색 터널로 돌아갑니다.

참고: RIP는 잘못된 경로를 통해 새 경로를 허용하기 전에 3분 에이징 타이머를 갖습니다. 또한 터널이 생성되고 트래픽이 피어 간에 전달될 수 있다고 가정합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 라우터 3620 및 3640
- Cisco VPN 3080 Concentrator - 버전: Cisco Systems, Inc./VPN 3000 Concentrator 버전 4.7
- Cisco VPN 3060 Concentrator - 버전: Cisco Systems, Inc./VPN 3000 Concentrator Series 버전 4.7
- Cisco VPN 3030 Concentrator - 버전: Cisco Systems, Inc./VPN 3000 Concentrator Series 버전 4.7

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

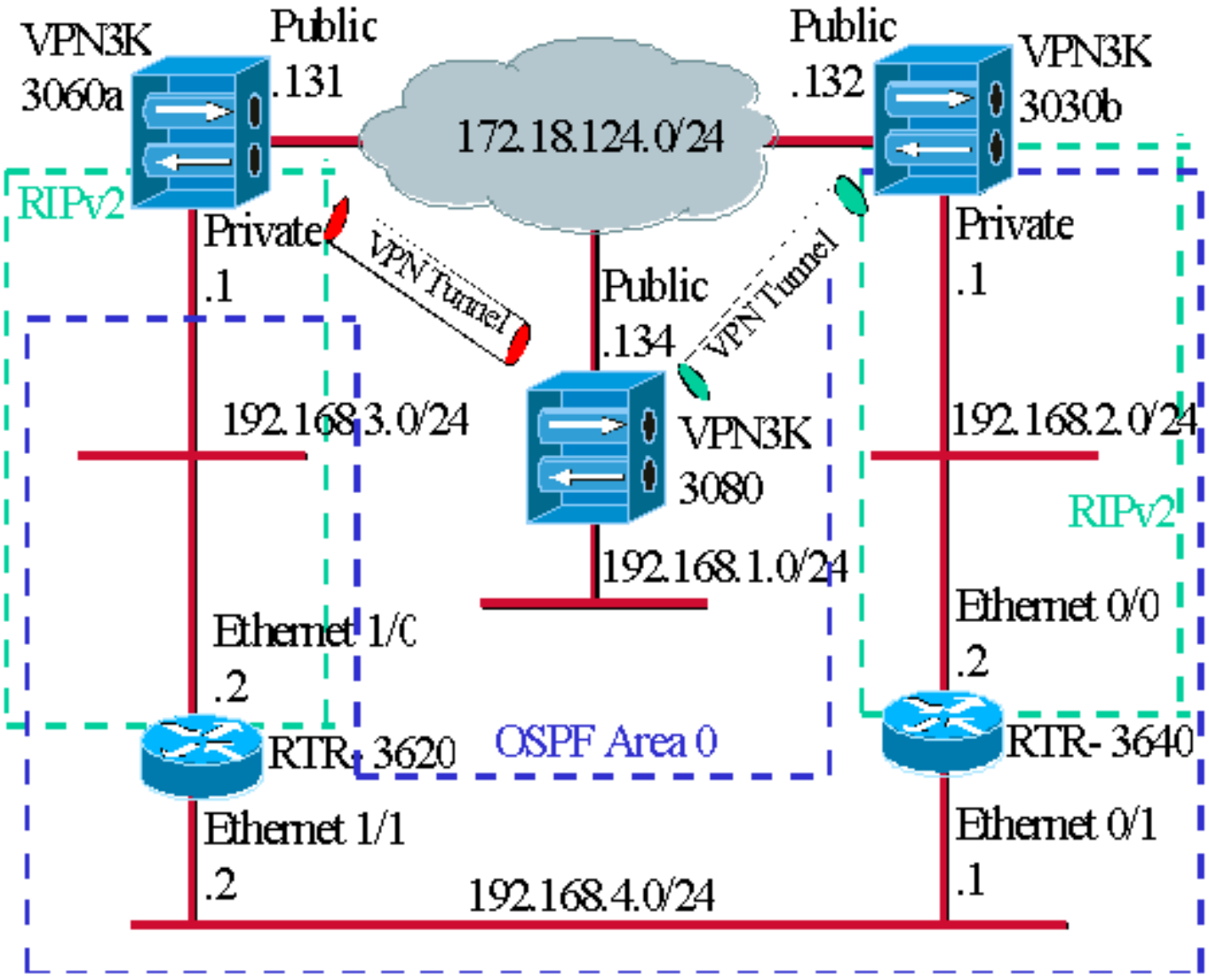
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



파란색 대시는 OSPF가 VPN 3030b에서 RTR-3640 및 RTR-3620으로 활성화되었음을 나타냅니다.

녹색 대시는 RIPv2가 프라이빗 VPN 3060a에서 RTR-3620, RTR-3640 및 프라이빗 VPN 3030b로 활성화되었음을 나타냅니다.

네트워크 검색이 활성화되어 있으므로 RIPv2는 빨간색 및 녹색 VPN 터널에서도 활성화됩니다. VPN 3080 프라이빗 인터페이스에서 RIP를 활성화할 필요는 없습니다. 192.168.4.x 네트워크에는 RIP도 없습니다. 모든 경로는 이 링크를 통해 OSPF에 의해 학습되기 때문입니다.

참고: 192.168.2.x 및 192.168.3.x 네트워크의 PC에는 VPN Concentrator가 아니라 라우터를 가리키는 기본 게이트웨이가 있어야 합니다. 라우터가 패킷을 라우팅할 위치를 결정할 수 있습니다.

라우터 컨피그레이션

이 문서에서는 다음 라우터 컨피그레이션을 사용합니다.

- 라우터 3620
- 라우터 3640

라우터 3620
`rtr-3620#write  terminal`

```
Building configuration...

Current configuration : 873 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtr-3620
!
ip subnet-zero
!
interface Ethernet1/0
 ip address 192.168.3.2 255.255.255.0
 half-duplex
!
interface Ethernet1/1
 ip address 192.168.4.2 255.255.255.0
 half-duplex
!
router ospf 1
 log-adjacency-changes
!--- To pass the routes learned through RIP into the
OSPF process, !--- use the redistribute command. !--- To
prevent a routing loop, block the 192.168.1.0 network !-
-- from entering the OSPF process. It should only be
learned !--- through the RIP process. No two different
routing processes !--- exchange information unless you
implicitly use the !--- redistribute command. !--- The
192.168.1.x network is learned through OSPF from the !--
- 192.168.2.x side. However, since the admin distance is
changed, !--- it is not installed into the table !---
because RIP has an administrative distance of 120, !---
and all of the OSPF distances are 130.

 redistribute rip subnets route-map block192.168.1.0
!--- To enable the OSPF process for the interfaces that
are included !--- in the 192.168.x.x networks: network
192.168.0.0 0.0.255.255 area 0 !--- Since RIP's default
admin distance is 120 and OSPF's is 110, !--- make RIP a
preferable metric for communications !--- over the
"backup" network. !--- Change any learned OSPF routes
from neighbor 192.168.4.1 !--- to an admin distance of
130. distance 130 192.168.4.1 0.0.0.0 ! !--- To enable
RIP on the Ethernet 1/0 interface and set it to !--- use
version 2: router rip version 2 network 192.168.3.0 ! ip
classless ! ! access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any route-map block192.168.1.0
permit 10 match ip address 1 ! line con 0 exec-timeout 0
0 line aux 0 line vty 0 4 ! end
```

라우터 3640

```
rtr-3640#write terminal
Building configuration...

Current configuration : 1129 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

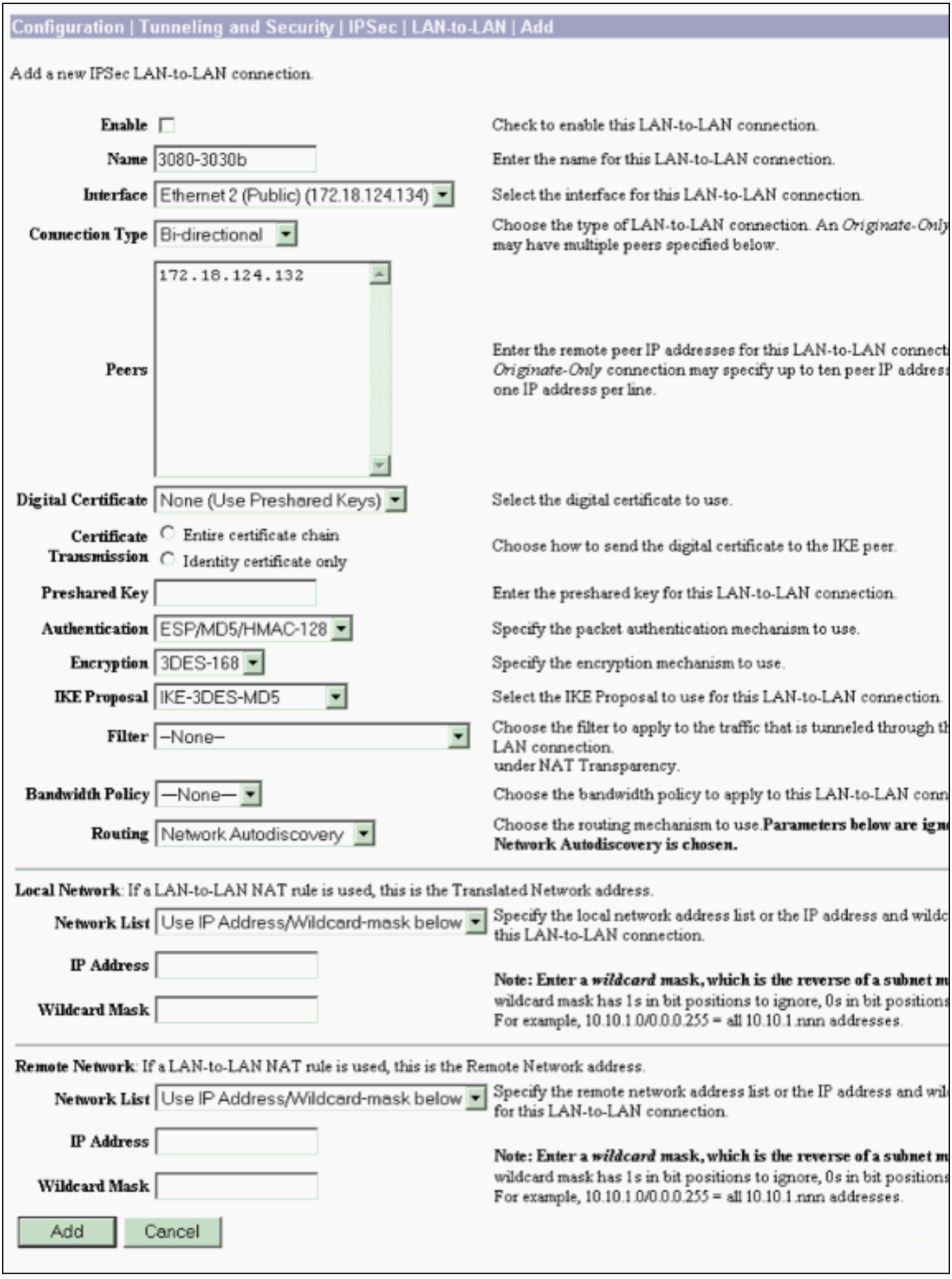
```
!
hostname rtr-3640
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.4.1 255.255.255.0
 half-duplex
!
router ospf 1
 log-adjacency-changes
!--- Use this command to push RIP learned routes into
OSPF. !--- You need this when the VPN 3060a or the
connection drops and !--- the 192.168.3.0 route needs to
be injected into the OSPF backbone. redistribute rip
subnets !--- Place all 192.168.x.x networks into area 0.
network 192.168.0.0 0.0.255.255 area 0 !--- Since RIP's
default admin distance is 120 and OSPF's is 110, !---
make RIP a preferable metric for communications !---
over the "backup" network. !--- Change any learned OSPF
routes from neighbor 192.168.4.2 !--- to an admin
distance of 130. distance 130 192.168.4.2 0.0.0.0 ! !---
To enable RIP on the Ethernet 0/0 interface and set it
to !--- use version 2: router rip version 2 network
192.168.2.0 ! ip classless ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 ! end
```

VPN 3080 Concentrator 컨피그레이션

LAN-to-LAN VPN 3080에서 VPN 3030b

Configuration **> Tunneling and Security > IPSec > IPSec LAN-to-LAN을 선택합니다**. 네트워크 자동 검색이 사용되므로 로컬 및 원격 네트워크 목록을 작성할 필요가 없습니다.

참고: 소프트웨어 버전 3.1 이하를 실행하는 VPN Concentrator에는 자동 검색 확인란이 있습니다. 소프트웨어 버전 3.5(VPN 3080에서 사용)는 여기에 표시된 것과 같은 드롭다운 메뉴를 사용합니다
.

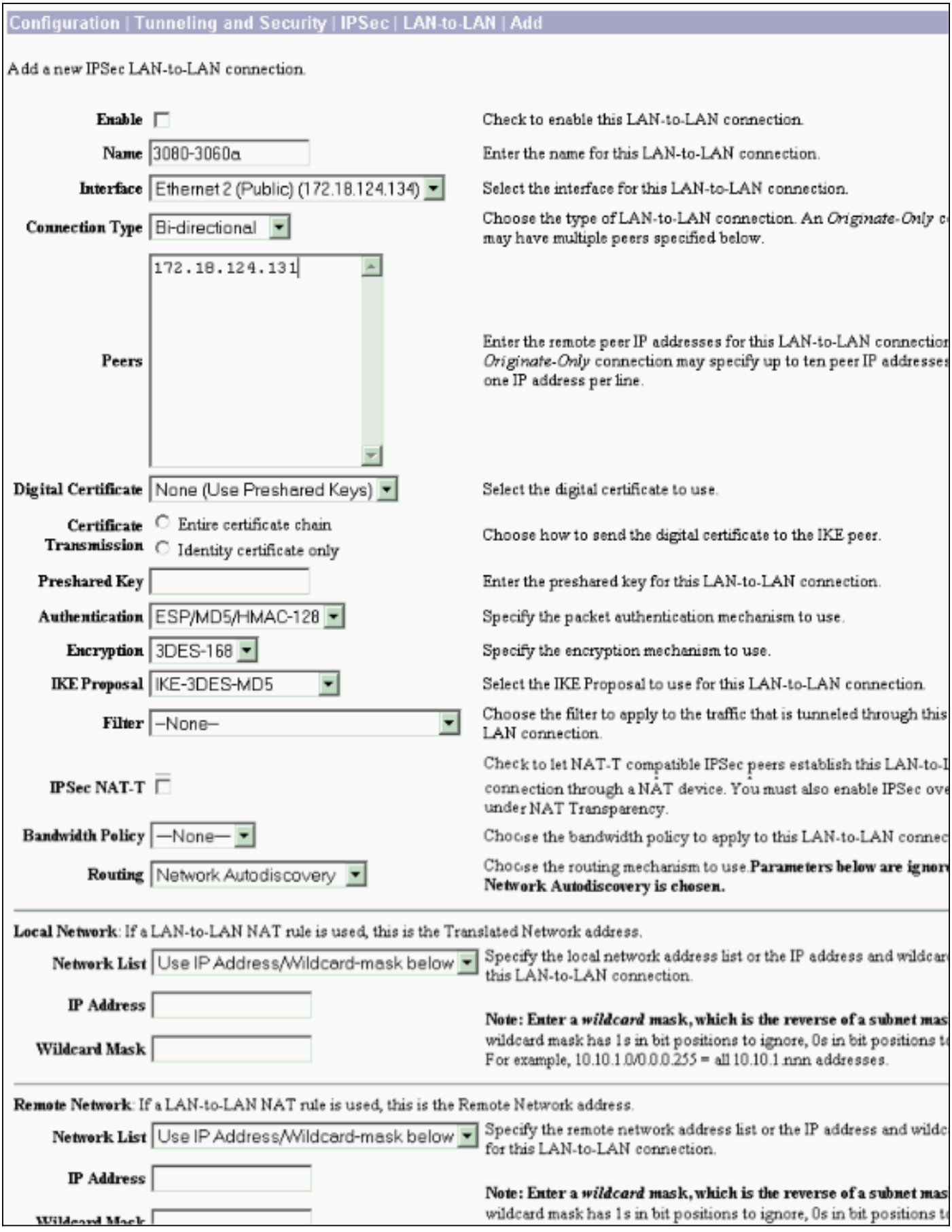


LAN-to-LAN VPN 3080에서 VPN 3060a

Configuration **> Tunneling and Security > IPSec > IPSec LAN-to-LAN을 선택합니다.** 네트워크 자

동 검색이 사용되므로 로컬 및 원격 네트워크 목록을 작성할 필요가 없습니다.

참고: 소프트웨어 버전 3.1 이하를 실행하는 VPN Concentrator에는 자동 검색 확인란이 있습니다. 소프트웨어 버전 3.5(VPN 3080에서 사용)는 여기에 표시된 것과 같은 드롭다운 메뉴를 사용합니다
.

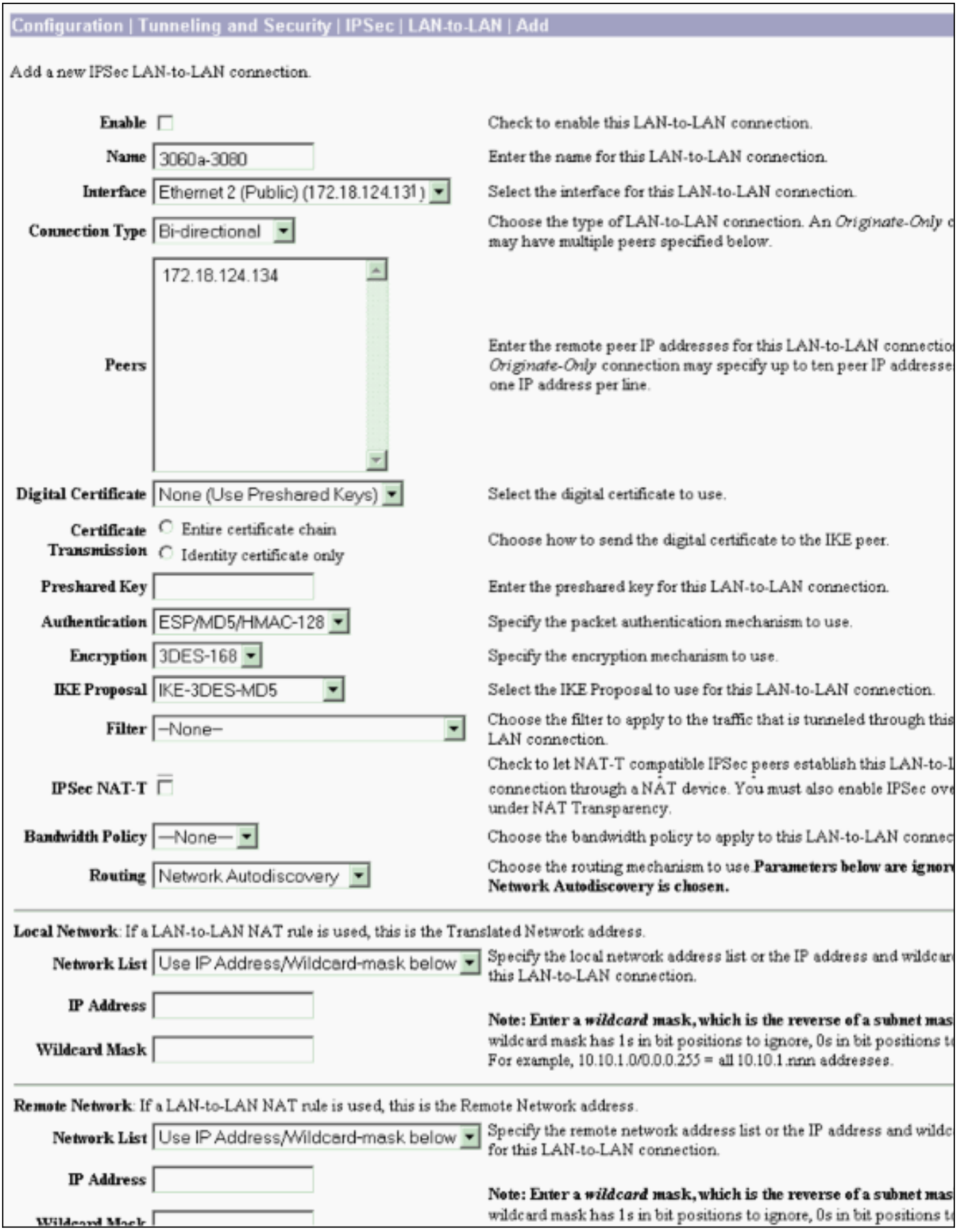


VPN 3060a Concentrator 컨피그레이션

LAN-to-LAN VPN 3060a-VPN 3080

Configuration **> Tunneling and Security > IPSec > IPSec LAN-to-LAN을 선택합니다**.

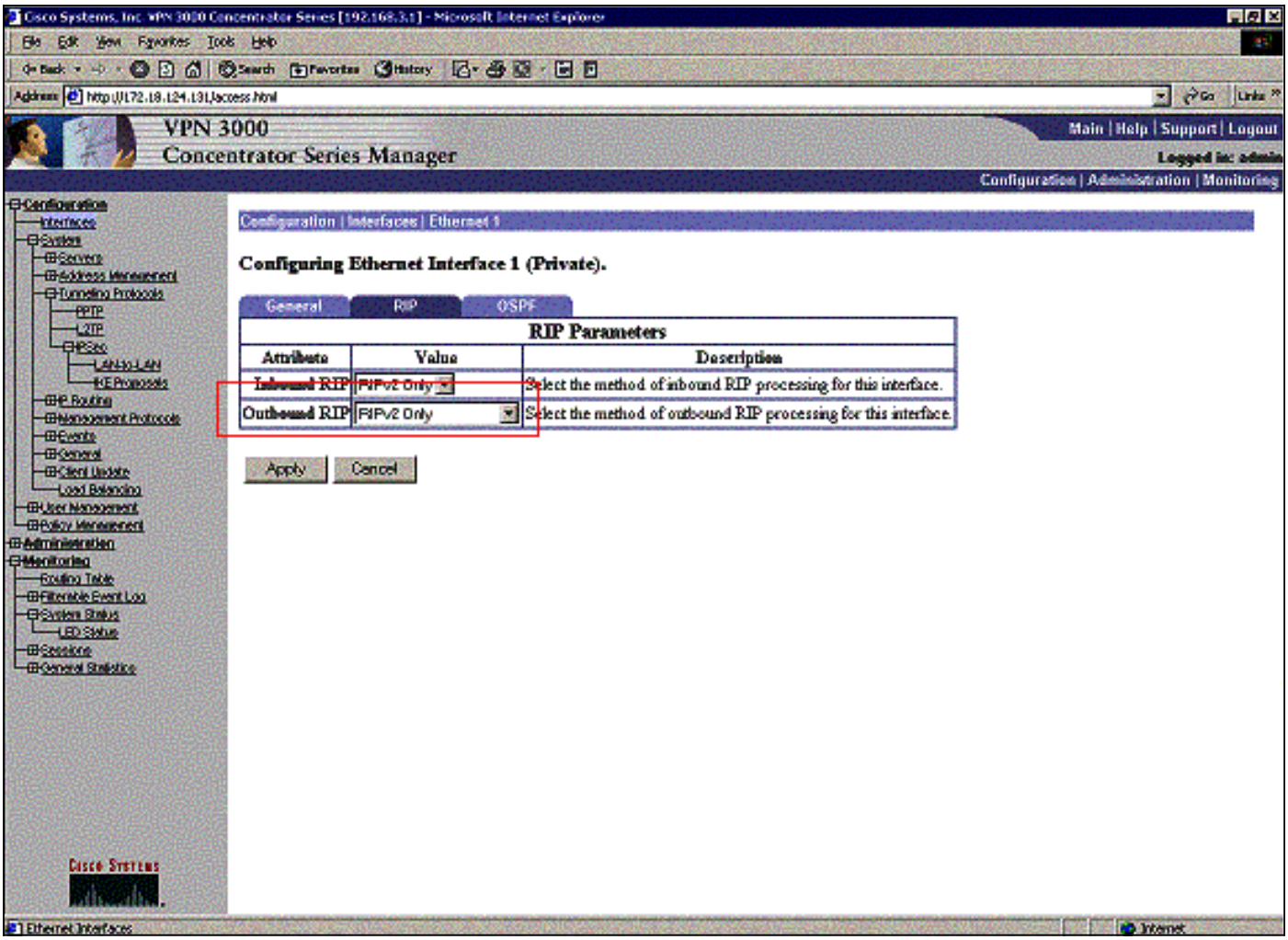
참고: 소프트웨어 버전 3.5 이상에서와 같이 드롭다운 메뉴 대신 네트워크 자동 검색용 VPN 3060에 확인란이 있습니다.



VPN 3620 라우터에 터널 학습 경로를 전달하도록 RIP 활성화

Configuration > Interfaces > Private > RIP를 선택합니다. 드롭다운 메뉴를 RIPv2 Only(RIPv2 전용)로 변경하고 Apply(적용)를 클릭합니다. 그런 다음 Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN을 선택합니다.

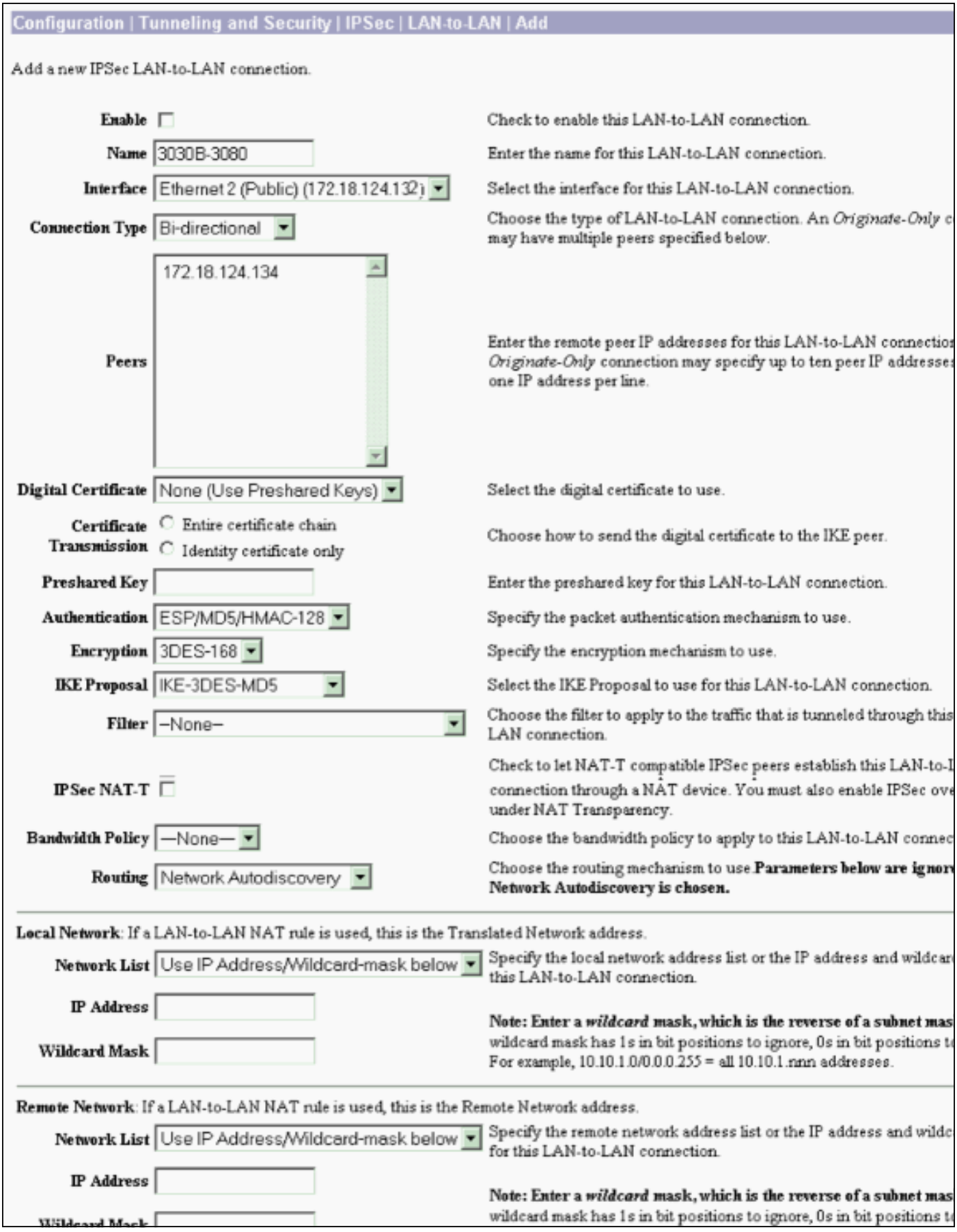
참고: 기본값은 아웃바운드 RIP이며 프라이빗 인터페이스에 대해 비활성화됩니다.



VPN 3030b Concentrator 컨피그레이션

LAN-to-LAN VPN 3030b-VPN 3080

Configuration **> Tunneling and Security > IPSec > LAN-to-LAN**을 선택합니다.

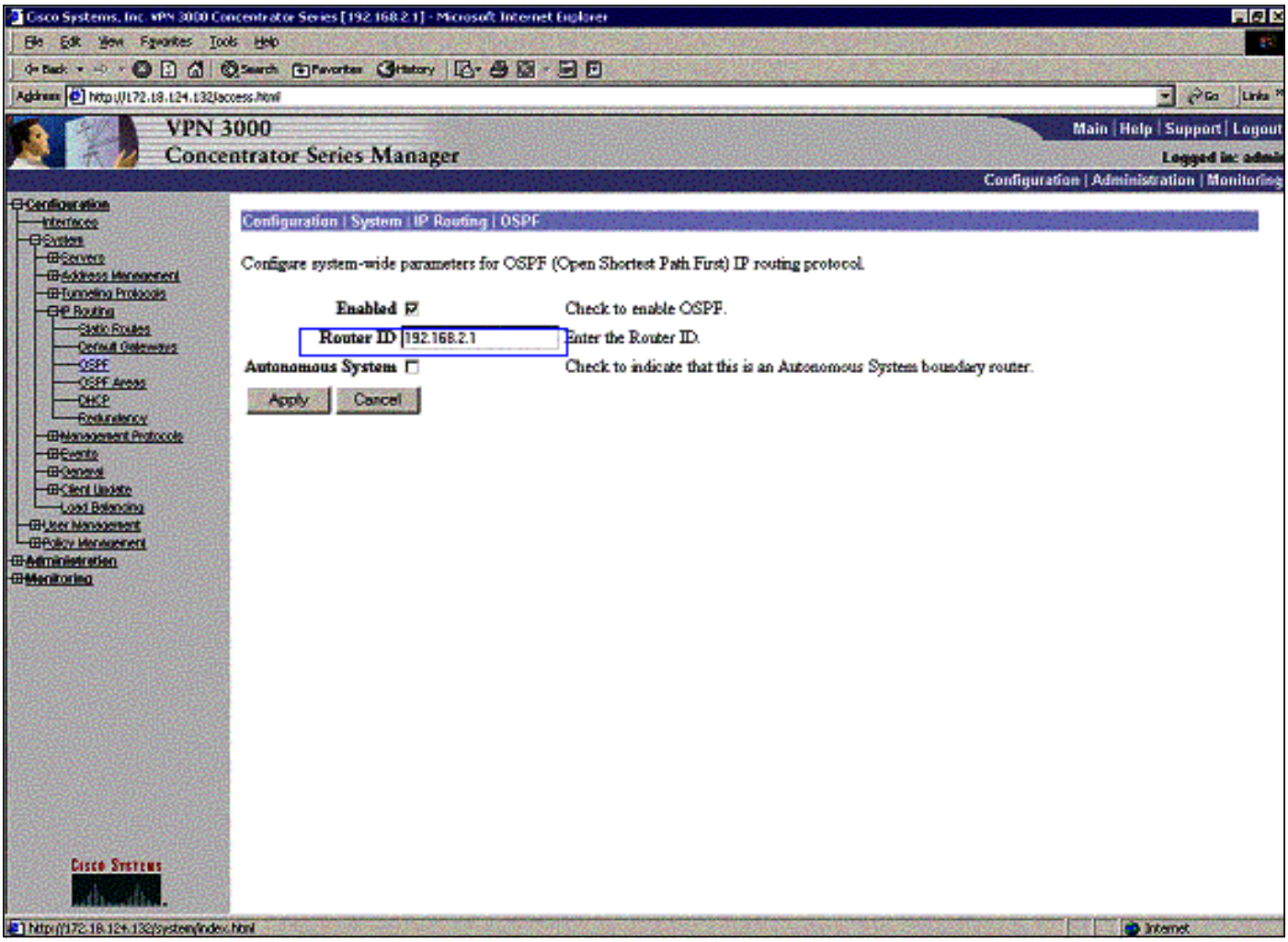


[VPN 3640 라우터에 터널 학습 경로를 전달하도록 RIP 활성화](#)

VPN 3060a Concentrator에 대해 이 문서의 앞부분에 나와 있는 단계를 따릅니다.

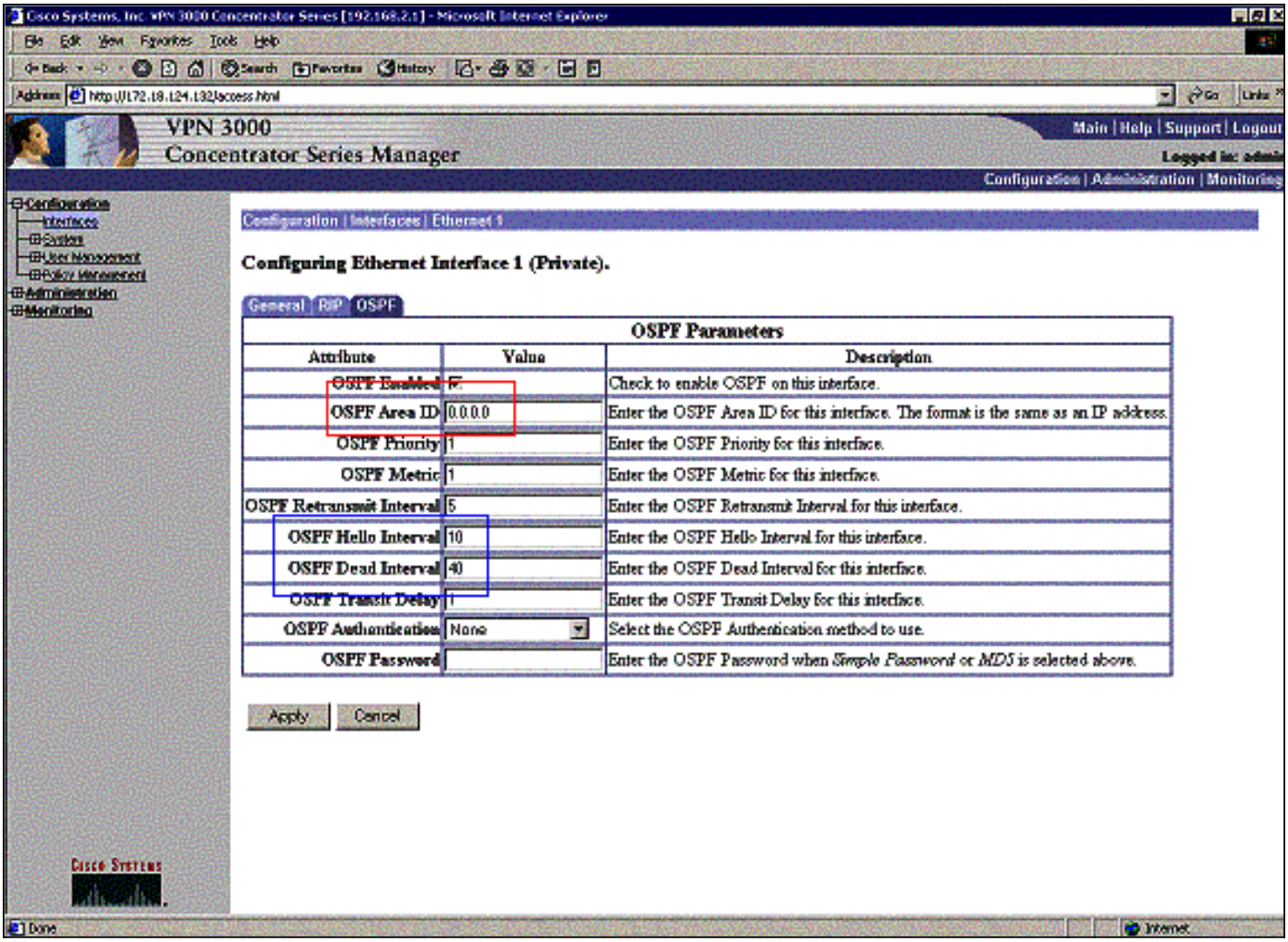
[OSPF가 백본 학습 경로를 VPN 3030b Concentrator로 전달하도록 활성화](#)

Configuration **> System > IP Routing > OSPF를 선택하고** 라우터 ID를 입력합니다.




```
rtr-3640#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

192.168.4.2       1   FULL/DR         00:00:39    192.168.4.2     Ethernet0/1
!--- For troubleshooting purposes, it helps to make the router ID the !--- IP address of the
private interface. 192.168.2.1       1   FULL/BDR        00:00:36    192.168.2.1     Ethernet0/0
```

영역 ID는 전선의 ID와 일치해야 합니다. 이 예제의 영역은 0이므로 0.0.0.0으로 표시됩니다. 또한 **Enable OSPF** 상자를 선택하고 Apply를 **클릭합니다**.



OSPF 타이머가 라우터의 타이머와 일치하는지 확인합니다. 라우터 타이머를 확인하려면 show ip ospf **interface *<interface name>* 명령을** 사용합니다.

```
rtr-3640#show ip ospf interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.2.2/24, Area 0
  Process ID 1, Router ID 192.168.4.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.4.1, Interface address 192.168.2.2
  Backup Designated router (ID) 192.168.2.1, Interface address 192.168.2.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.2.1  (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

OSPF에 대한 자세한 내용은 RFC 1247을 참조하십시오 .

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

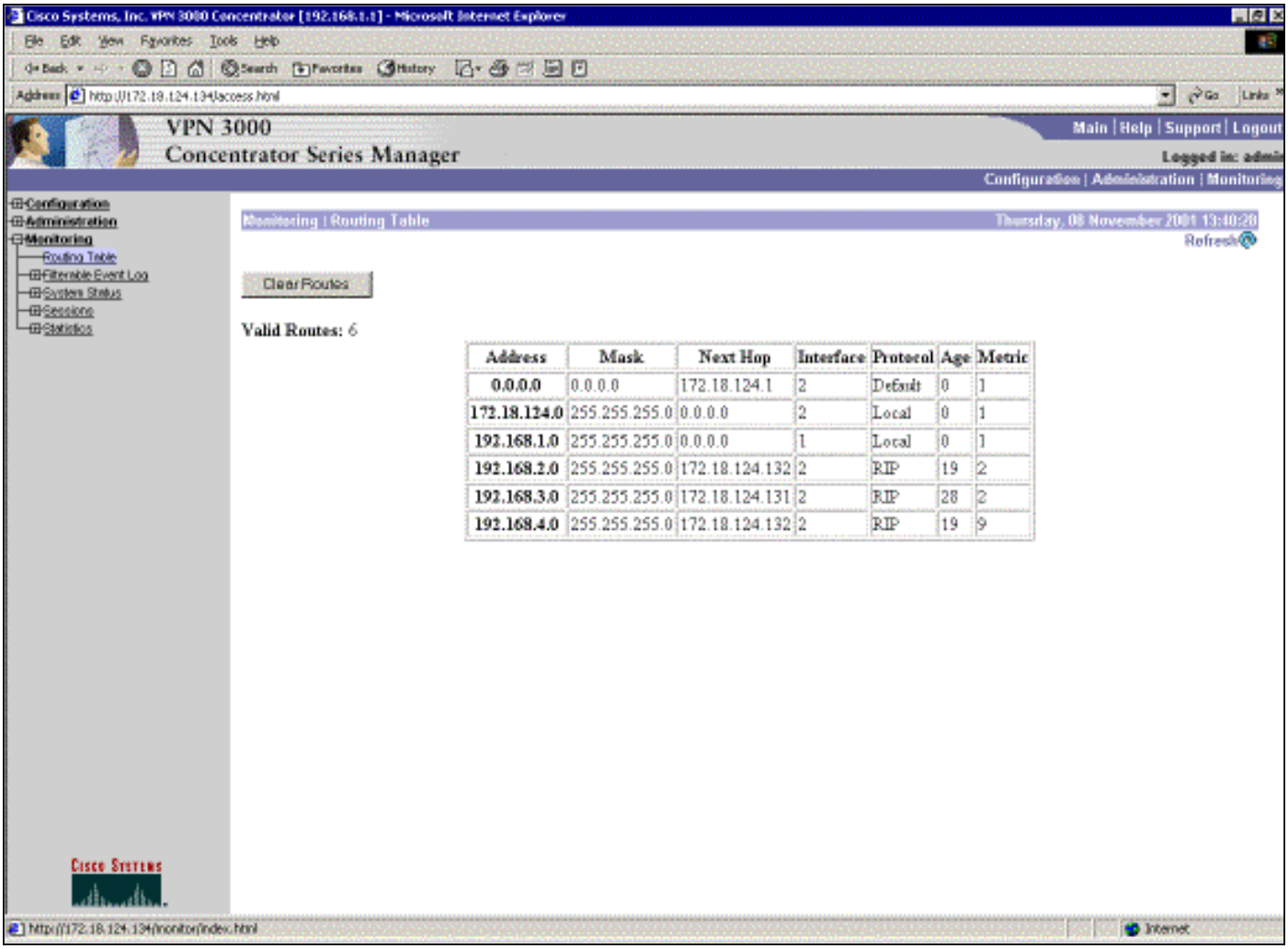
일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명**

령 출력의 분석 결과를 볼 수 있습니다.

이 명령 출력은 정확한 라우팅 테이블을 보여줍니다.

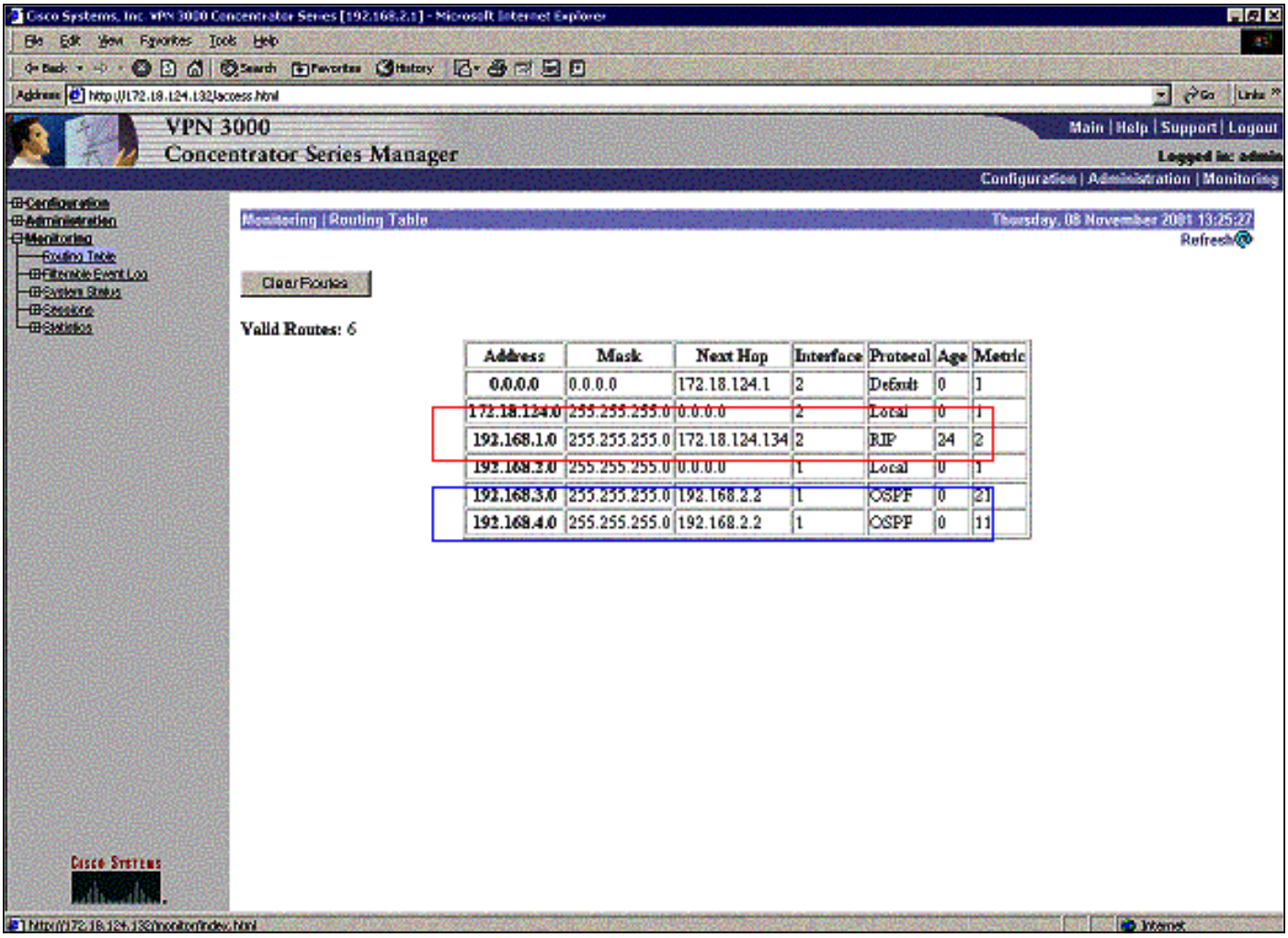
```
rtr-3620#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.3.1, 00:00:11, Ethernet1/0
C    192.168.4.0/24 is directly connected, Ethernet1/1
!--- The 192.168.1.x network is learned from the !--- VPN 3060a Concentrator. R
192.168.1.0/24 [120/2] via 192.168.3.1, 00:00:11, Ethernet1/0
!--- The 192.168.3.x network traverses the 192.168.4.x network !--- to get to the 192.168.2.x
network. O    192.168.2.0/24 [130/20] via 192.168.4.1, 00:01:07, Ethernet1/1
C    192.168.3.0/24 is directly connected, Ethernet1/0

rtr-3640#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

Gateway of last resort is not set

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.2.1, 00:00:23, Ethernet0/0
C    192.168.4.0/24 is directly connected, Ethernet0/1
!--- The 192.168.1.x network is learned from the !--- VPN 3030b Concentrator. R
192.168.1.0/24 [120/2] via 192.168.2.1, 00:00:23, Ethernet0/0
C    192.168.2.0/24 is directly connected, Ethernet0/0
!--- The 192.168.2.x network traverses the 192.168.4.x network !--- to get to the 192.168.3.x
network. !--- This is an example of perfect symmetrical routing. O    192.168.3.0/24 [130/20]
via 192.168.4.2, 00:00:58, Ethernet0/1
```

정상적인 환경에서 VPN 3080 Concentrator 라우팅 테이블입니다.



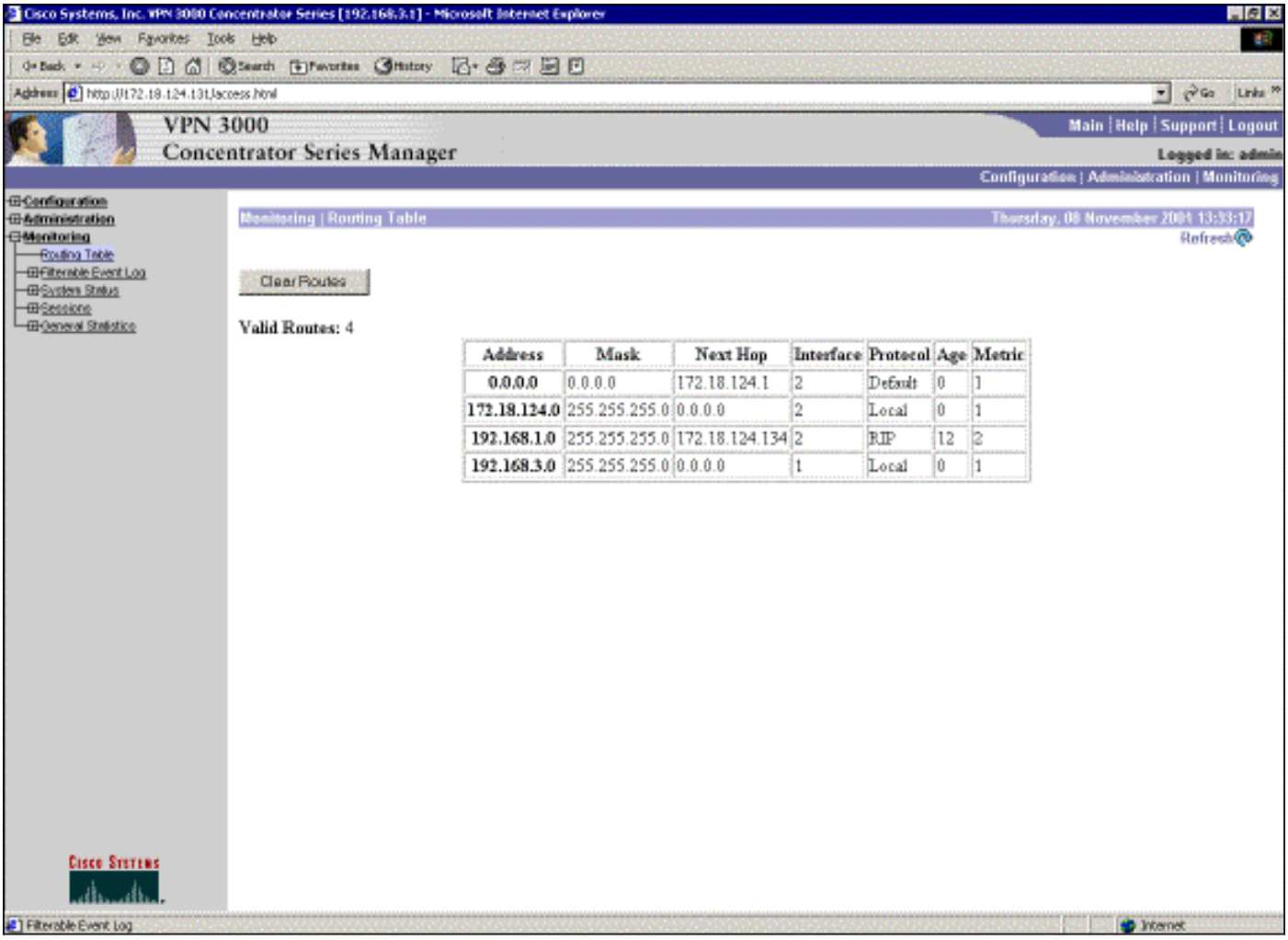
네트워크 192.168.2.x 및 192.168.3.x는 각각 VPN 터널 172.18.124.132 및 172.18.124.131을 통해 학습됩니다. 192.168.4.x 네트워크는 172.18.124.132 터널을 통해 학습됩니다. 라우터의 OSPF 알림이 VPN 3030b Concentrator 라우팅 테이블에 배치되기 때문입니다. 그런 다음 라우팅 테이블에서 원격 VPN 피어에 네트워크를 알립니다.

일반적인 상황에서는 VPN 3030b Concentrator 라우팅 테이블입니다.



빨간색 상자는 192.168.1.x 네트워크가 VPN 터널에서 학습된다는 것을 강조 표시합니다. 파란색 상자는 코어 OSPF 프로세스를 통해 네트워크 192.168.3.x 및 192.168.4.x를 학습한다는 것을 강조 표시합니다.

일반적인 상황에서는 VPN 3060a Concentrator 라우팅 테이블입니다.

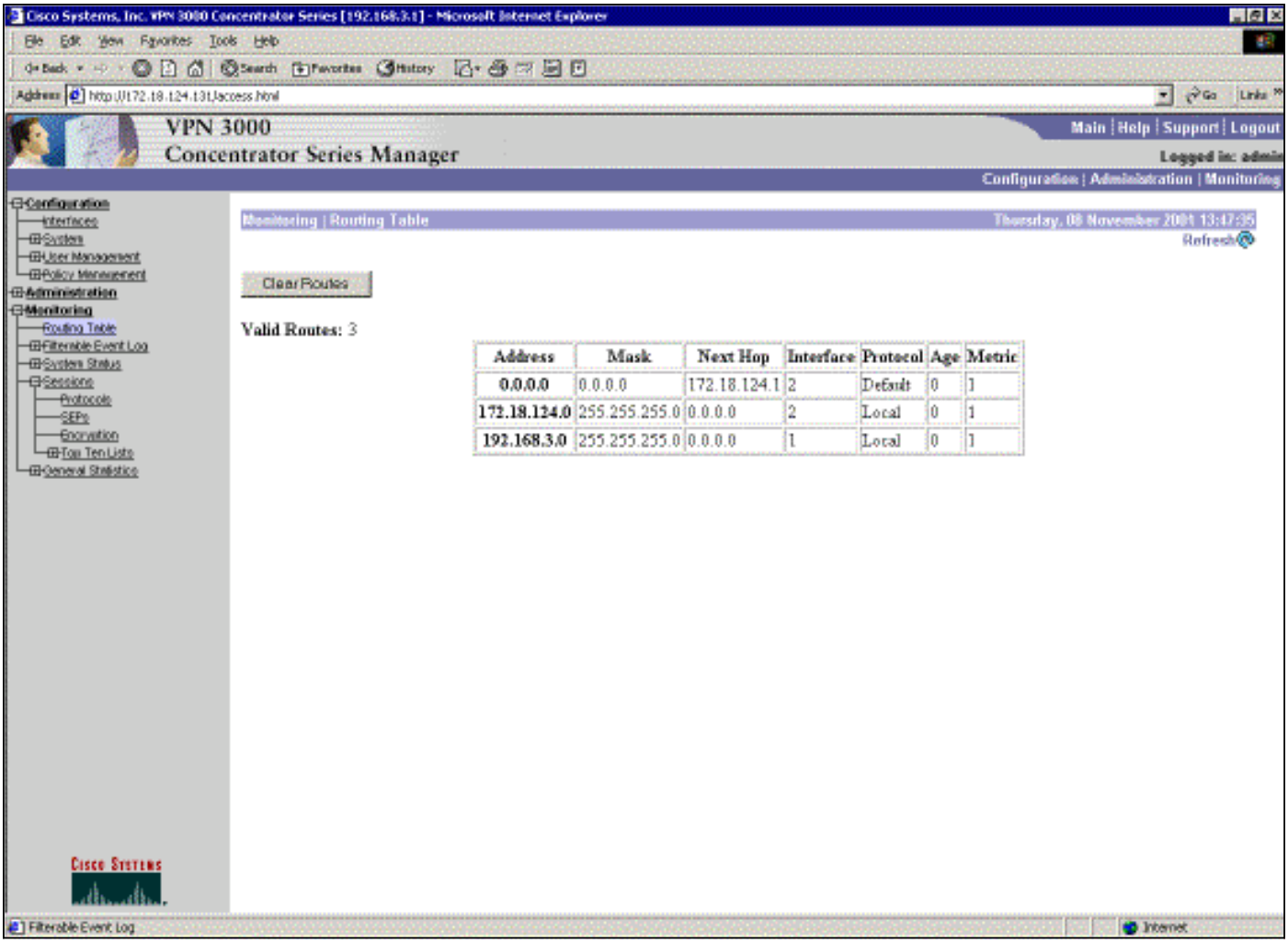


여기서 네트워크 192.168.1.x는 유일한 네트워크이며 VPN 터널을 통해 연결할 수 있습니다. 해당 경로를 따라 프로세스(예: RIP)가 전달되지 않으므로 192.168.2.0 네트워크가 없습니다. 192.168.3.x 네트워크의 PC가 기본 게이트웨이를 VPN Concentrator로 가리키지 않는 한 손실된 것은 없습니다. 선택한 경우 항상 고정 경로를 추가할 수 있습니다. 그러나 이 예에서 VPN Concentrator 자체는 192.168.2.0 네트워크에 연결할 필요가 없습니다.

문제 해결

시뮬레이션된 결함

이는 컨피그레이션에서 시뮬레이션된 fault입니다. 공용 인터페이스에 대한 필터를 제거하면 VPN 터널이 삭제됩니다. 이렇게 하면 터널을 통해 학습된 192.168.1.0에 대한 경로도 삭제됩니다. RIP 프로세스에서 경로를 제거하는 데 약 3분이 걸립니다. 따라서 라우트가 시간 초과될 때까지 잠재적으로 3분 동안 중단이 발생할 수 있습니다.



RIP 경로가 만료되면 라우터의 새 라우팅 테이블이 다음과 같이 나타납니다.

```
rtr-3620#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 not set

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.3.1, 00:00:05, Ethernet1/0
C    192.168.4.0/24 is directly connected, Ethernet1/1
!--- Now the 192.168.1.0 route is learned properly !--- through the OSPF backbone. O E2
192.168.1.0/24 [130/20] via 192.168.4.1, 00:00:05, Ethernet1/1
O    192.168.2.0/24 [130/20] via 192.168.4.1, 19:55:48, Ethernet1/1
C    192.168.3.0/24 is directly connected, Ethernet1/0
```

무엇이 잘못될 수 있습니까?

관리자 거리에 추가하는 것을 잊어버린 경우 이 출력을 볼 수 있습니다. 두 VPN 터널이 모두 작동 중입니다.

VPN 3080 Concentrator

참고: 라우팅 테이블의 비 그래픽 사용자 인터페이스(GUI) 버전입니다.

```
Monitor -> 1

Routing Table
-------------

Number of Routes: 6

   IP Address         Mask          Next Hop     Intf Protocol Age Metric
-------------------------------------------------------------------------
0.0.0.0         0.0.0.0         172.18.124.1       2 Default    0      1
172.18.124.0    255.255.255.0   0.0.0.0            2 Local      0      1
192.168.1.0     255.255.255.0   0.0.0.0            1 Local      0      1
192.168.2.0     255.255.255.0   172.18.124.132     2 RIP       10      2
192.168.3.0     255.255.255.0   172.18.124.131     2 RIP        2      2
192.168.4.0     255.255.255.0   172.18.124.132     2 RIP       10      9
```

192.168.3.0 네트워크에 연결하려면 경로가 172.18.124.131을 통과해야 합니다. 그러나 RTR-3620의 라우팅 테이블에는 다음이 표시됩니다.

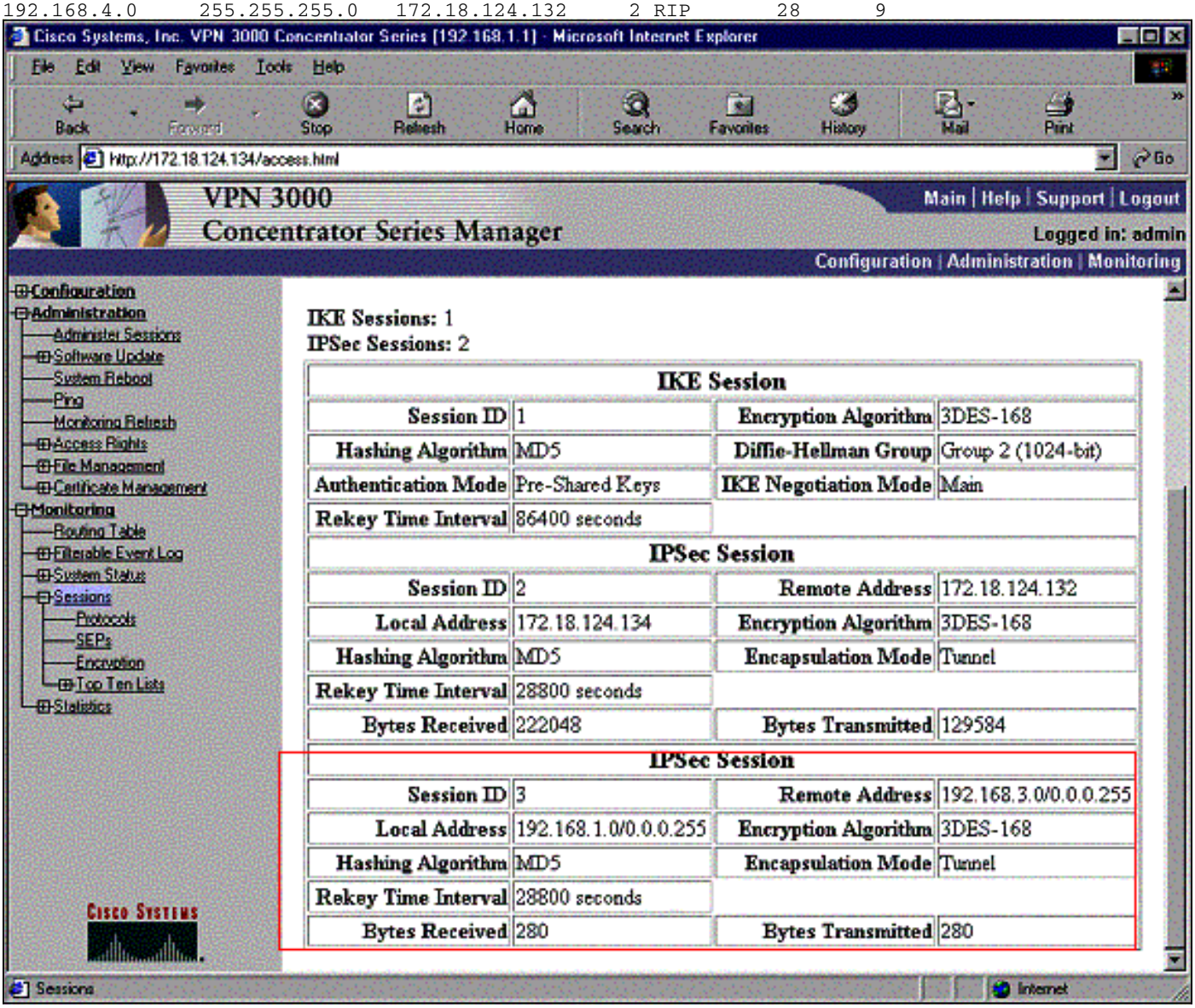
```
rtr-3620#show ip route

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 not set

     172.18.0.0/24 is subnetted, 1 subnets
O E2    172.18.124.0 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1
C    192.168.4.0/24 is directly connected, Ethernet1/1
!--- This is an example of asymmetric routing. O E2 192.168.1.0/24 [110/20] via 192.168.4.1,
00:03:16, Ethernet1/1
O    192.168.2.0/24 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1
C    192.168.3.0/24 is directly connected, Ethernet1/0
```

192.168.1.0 네트워크로 돌아가려면 백본 192.168.4.x 네트워크를 통해 경로를 이동해야 합니다.

자동 검색이 VPN 3030b Concentrator에 적절한 SA(보안 연결) 정보를 생성하므로 트래픽은 계속 작동합니다. 예를 들면 다음과 같습니다.

```
Routing -> 1

Routing Table

-------------
Number of Routes: 6
   IP Address         Mask          Next Hop     Intf Protocol Age Metric

-------------------------------------------------------------------------
0.0.0.0         0.0.0.0         172.18.124.1       2 Default    0      1
172.18.124.0    255.255.255.0   0.0.0.0            2 Local      0      1
192.168.1.0     255.255.255.0   0.0.0.0            1 Local      0      1
192.168.2.0     255.255.255.0   172.18.124.132     2 RIP       28      2
192.168.3.0     255.255.255.0   172.18.124.131     2 RIP       20      2
```

```
192.168.4.0     255.255.255.0   172.18.124.132     2 RIP       28      9
```



라우팅 테이블에서 피어가 172.18.124.131이어야 한다고 했지만 실제 SA(트래픽 흐름)는 172.18.124.132의 VPN 3030b Concentrator를 통해 수행됩니다. SA 테이블은 경로 테이블보다 우선합니다. VPN 3060a Concentrator의 경로 테이블 및 SA 테이블에 대한 정밀 조사만 트래픽이 올바른 방향으로 흐르지 않음을 보여줍니다.

관련 정보

- Cisco VPN 3000 Series Concentrator 지원 페이지
- IPSec 지원 페이지
- Technical Support - Cisco Systems