

# 이중화 또는 백업 ISP 링크에 대해 ASA 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[관련 제품](#)

#### [배경 정보](#)

[고정 경로 추적 기능 개요](#)

[중요 권장 사항](#)

#### [구성](#)

[네트워크 다이어그램](#)

[CLI 컨피그레이션](#)

[ASDM 컨피그레이션](#)

#### [다음을 확인합니다.](#)

[구성이 완료되었는지 확인합니다.](#)

[백업 경로가 설치되어 있는지 확인합니다\(CLI 방법\)](#)

[백업 경로가 설치되어 있는지 확인합니다\(ASDM 방법\)](#)

#### [문제 해결](#)

[디버그 명령](#)

[추적된 경로가 불필요하게 제거됨](#)

#### [관련 정보](#)

---

## 소개

이 문서에서는 이중화 또는 백업 인터넷 연결을 사용하도록 Cisco ASA 5500 Series 고정 경로 추적 기능을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소


이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 9.x 이상을 실행하는 Cisco ASA 5555-X Series
- Cisco ASDM 버전 7.x 이상

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

## 관련 제품

Cisco ASA 5500 Series 버전 9.1(5)에서도 이 컨피그레이션을 사용할 수 있습니다.

 참고: ASA 5505 Series에서 네 번째 인터페이스를 구성하려면 backup interface 명령이 필요합니다. 자세한 내용은 Cisco Security Appliance Command Reference, Version 7.2의 [백업 인터페이스](#) 섹션을 참조하십시오.

## 배경 정보

이 섹션에서는 이 문서에 설명된 고정 경로 추적 기능의 개요와 시작하기 전에 몇 가지 중요한 권장 사항을 제공합니다.

### 고정 경로 추적 기능 개요

고정 경로 사용의 한 가지 문제는 경로의 작동 여부를 결정할 수 있는 고유한 메커니즘이 없다는 것입니다.

다음 홉 게이트웨이를 사용할 수 없게 되더라도 경로는 라우팅 테이블에 남아 있습니다.

고정 경로는 보안 어플라이언스의 연결된 인터페이스가 다운된 경우에만 라우팅 테이블에서 제거됩니다.

이러한 문제를 해결하기 위해 고정 경로의 가용성을 추적하기 위해 고정 경로 추적 기능을 사용합니다.

이 기능은 라우팅 테이블에서 고정 경로를 제거하고 실패 시 백업 경로로 대체합니다.

고정 경로 추적을 사용하면 기본 임대 회선을 사용할 수 없게 될 경우 ASA에서 보조 ISP에 대한 저렴한 연결을 사용할 수 있습니다.

이러한 이중화를 달성하기 위해 ASA는 고정 경로를 사용자가 정의하는 모니터링 대상과 연결합니다.

SLA(Service Level Agreement) 작업은 주기적인 ICMP 에코 요청으로 대상을 모니터링합니다.

에코 응답이 수신되지 않으면 객체는 다운된 것으로 간주되며 연결된 경로가 라우팅 테이블에서 제거됩니다.

이전에 구성한 백업 경로가 제거된 경로 대신 사용됩니다.

백업 경로가 사용 중인 동안 SLA 모니터 작업은 모니터링 대상에 도달하기 위한 시도를 계속합니다.


대상을 다시 사용할 수 있게 되면 첫 번째 경로가 라우팅 테이블에서 대체되고 백업 경로가 제거됩니다.

이 문서에서 사용하는 예에서는 ASA가 인터넷에 대한 두 개의 연결을 유지 관리합니다.

첫 번째 연결은 고속 임대 회선으로 기본 ISP에서 제공하는 라우터를 통해 액세스합니다.

두 번째 연결은 보조 ISP에서 제공하는 DSL 모뎀을 통해 액세스하는 저속 DSL(Digital Subscriber Line)입니다.

---

 참고: 이 문서에서 설명하는 컨피그레이션은 ASA에서 지원되지 않으므로 로드 밸런싱 또는 로드 공유에 사용할 수 없습니다. 이중화 또는 백업용으로만 이 컨피그레이션을 사용합니다. 아웃바운드 트래픽은 기본 ISP를 사용한 다음 기본 ISP에 장애가 발생하면 보조 ISP를 사용합니다. 기본 ISP에 장애가 발생하면 트래픽이 일시적으로 중단됩니다.

---

임대 회선이 활성 상태이고 기본 ISP 게이트웨이에 연결할 수 있는 한 DSL 연결은 유휴 상태입니다.

그러나 기본 ISP에 대한 연결이 다운되면 ASA는 트래픽을 DSL 연결로 전달하기 위해 라우팅 테이블을 변경합니다.

이러한 이중화를 달성하기 위해 고정 경로 추적이 사용됩니다.

ASA는 모든 인터넷 트래픽을 기본 ISP로 보내는 고정 경로로 구성됩니다.

10초마다 SLA 모니터 프로세스는 기본 ISP 게이트웨이에 연결할 수 있는지 확인합니다.

SLA 모니터 프로세스에서 기본 ISP 게이트웨이에 연결할 수 없다고 결정하면 해당 인터페이스로 트래픽을 전달하는 고정 경로가 라우팅 테이블에서 제거됩니다.

고정 경로를 대체하기 위해 보조 ISP로 트래픽을 전달하는 대체 고정 경로가 설치됩니다.

이 대체 고정 경로는 기본 ISP에 연결할 수 있을 때까지 DSL 모뎀을 통해 트래픽을 보조 ISP로 보냅니다.

이 컨피그레이션은 ASA 뒤에 있는 사용자가 아웃바운드 인터넷 액세스를 계속 사용할 수 있도록 비교적 저렴한 방법을 제공합니다.

이 문서에서 설명한 것처럼 이 설정은 ASA 뒤에 있는 리소스에 대한 인바운드 액세스에 항상 적합한 것은 아닙니다. 원활한 인바운드 연결을 위해서는 고급 네트워킹 기술이 필요합니다.

이 문서에서는 이러한 기술에 대해 다루지 않습니다.

## 중요 권장 사항

이 문서에 설명된 컨피그레이션을 시도하기 전에 ICMP(Internet Control Message Protocol) 에코 요청에 응답할 수 있는 모니터링 대상을 선택해야 합니다.

대상은 사용자가 선택하는 모든 네트워크 객체일 수 있지만 ISP(인터넷 서비스 공급자) 연결과 긴


밀하게 연결된 대상이 좋습니다.

다음은 몇 가지 가능한 모니터링 대상입니다.

- ISP 게이트웨이 주소
- 다른 ISP 관리 주소
- ASA가 통신해야 하는 AAA(Authentication, Authorization, and Accounting) 서버와 같은 다른 네트워크의 서버
- 다른 네트워크에 있는 영구 네트워크 개체(밤에 종료할 수 있는 데스크톱 또는 노트북 컴퓨터는 좋은 선택이 아님)

이 문서에서는 Cisco ASDM(Adaptive Security Device Manager)에서 컨피그레이션을 변경할 수 있도록 ASA가 완전히 작동하며 구성되어 있다고 가정합니다.

---


 **팁:** ASDM에서 디바이스를 구성하도록 허용하는 방법에 대한 자세한 내용은 CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1의 [Configuring HTTPS Access for ASDM](#) 섹션을 참조하십시오.

---


## 구성

고정 경로 추적 기능을 사용하도록 ASA를 구성하려면 이 섹션에 설명된 정보를 사용하십시오.

---

 **참고:** 이 섹션에서 [사용되는 명령어](#)에 대한 자세한 내용을 보려면 [Command Lookup Tool](#)([등록된 고객만 해당](#))을 사용하십시오.

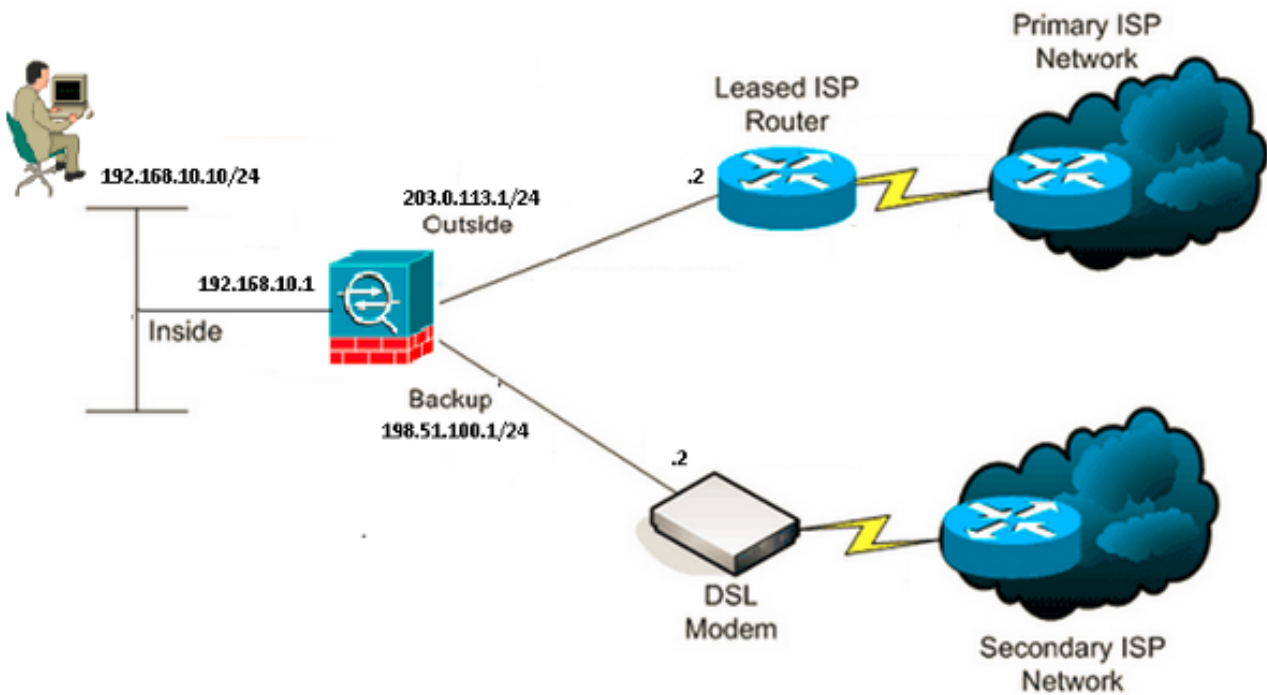
---

 **참고:** 이 컨피그레이션에서 사용되는 IP 주소는 인터넷에서 합법적으로 라우팅할 수 없습니다. 랩 [환경](#)에서 사용되는 RFC 1918 주소입니다.

---

## 네트워크 다이어그램

이 섹션에서 제공하는 예에서는 다음 네트워크 설정을 사용합니다.



## CLI 컨피그레이션

CLI를 통해 ASA를 구성하려면 다음 정보를 사용합니다.

```
<#root>
```

```
ASA#
```

```
show running-config
```

```
ASA Version 9.1(5)
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif backup
 security-level 0
 ip address 198.51.100.1 255.255.255.0
```

```
!--- The interface attached to the Secondary ISP.
```

!--- "backup" was chosen here, but any name can be assigned.

```
!  
interface GigabitEthernet0/3  
shutdown  
no nameif  
no security-level  
no ip address  
!  
interface GigabitEthernet0/4  
no nameif  
no security-level  
no ip address  
!  
interface GigabitEthernet0/5  
no nameif  
no security-level  
no ip address  
!  
interface Management0/0  
management-only  
no nameif  
no security-level  
no ip address  
!  
boot system disk0:/asa915-smp-k8.bin  
ftp mode passive  
clock timezone IND 5 30  
object network Inside_Network  
subnet 192.168.10.0 255.255.255.0  
object network inside_network  
subnet 192.168.10.0 255.255.255.0  
pager lines 24  
logging enable  
mtu inside 1500  
mtu outside 1500  
mtu backup 1500  
icmp unreachable rate-limit 1 burst-size 1  
no asdm history enable  
arp timeout 14400  
no arp permit-nonconnected  
!  
object network Inside_Network  
nat (inside,outside) dynamic interface  
object network inside_network  
nat (inside,backup) dynamic interface
```

!--- NAT Configuration for Outside and Backup

```
route outside 0.0.0.0 0.0.0.0 203.0.113.2 1 track 1
```

!--- Enter this command in order to track a static route.

!--- This is the static route to be installed in the routing

!--- table while the tracked object is reachable. The value after

!--- the keyword "track" is a tracking ID you specify.

```
route backup 0.0.0.0 0.0.0.0 198.51.100.2 254
```

!--- Define the backup route to use when the tracked object is unavailable.

!--- The administrative distance of the backup route must be greater than

!--- the administrative distance of the tracked route.

!--- If the primary gateway is unreachable, that route is removed

!--- and the backup route is installed in the routing table

!--- instead of the tracked route.

```
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
```

```
sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10
```

!--- Configure a new monitoring process with the ID 123. Specify the  
!--- monitoring protocol and the target network object whose availability the tracking  
!--- process monitors. Specify the number of packets to be sent with each poll.  
!--- Specify the rate at which the monitor process repeats (in seconds).

```
sla monitor schedule 123 life forever start-time now
```

!--- Schedule the monitoring process. In this case the lifetime  
!--- of the process is specified to be forever. The process is scheduled to begin  
!--- at the time this command is entered. As configured, this command allows the  
!--- monitoring configuration specified above to determine how often the testing  
!--- occurs. However, you can schedule this monitoring process to begin in the

```
!--- future and to only occur at specified times.
```

```
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
!
track 1 rtr 123 reachability
```

```
!--- Associate a tracked static route with the SLA monitoring process.
!--- The track ID corresponds to the track ID given to the static route to monitor:
!--- route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1
!--- "rtr" = Response Time Reporter entry. 123 is the ID of the SLA process
!--- defined above.
```

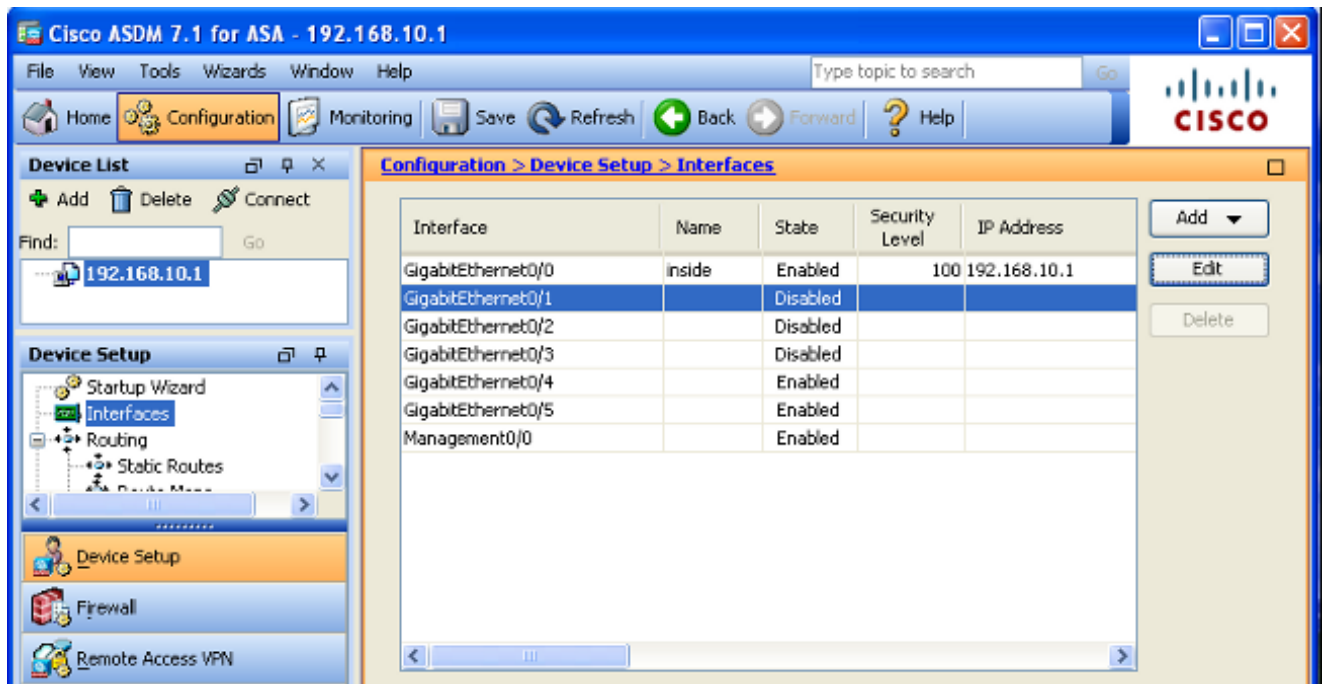
```
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
priority-queue inside
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
!
service-policy global_policy global
```

## ASDM 컨피그레이션

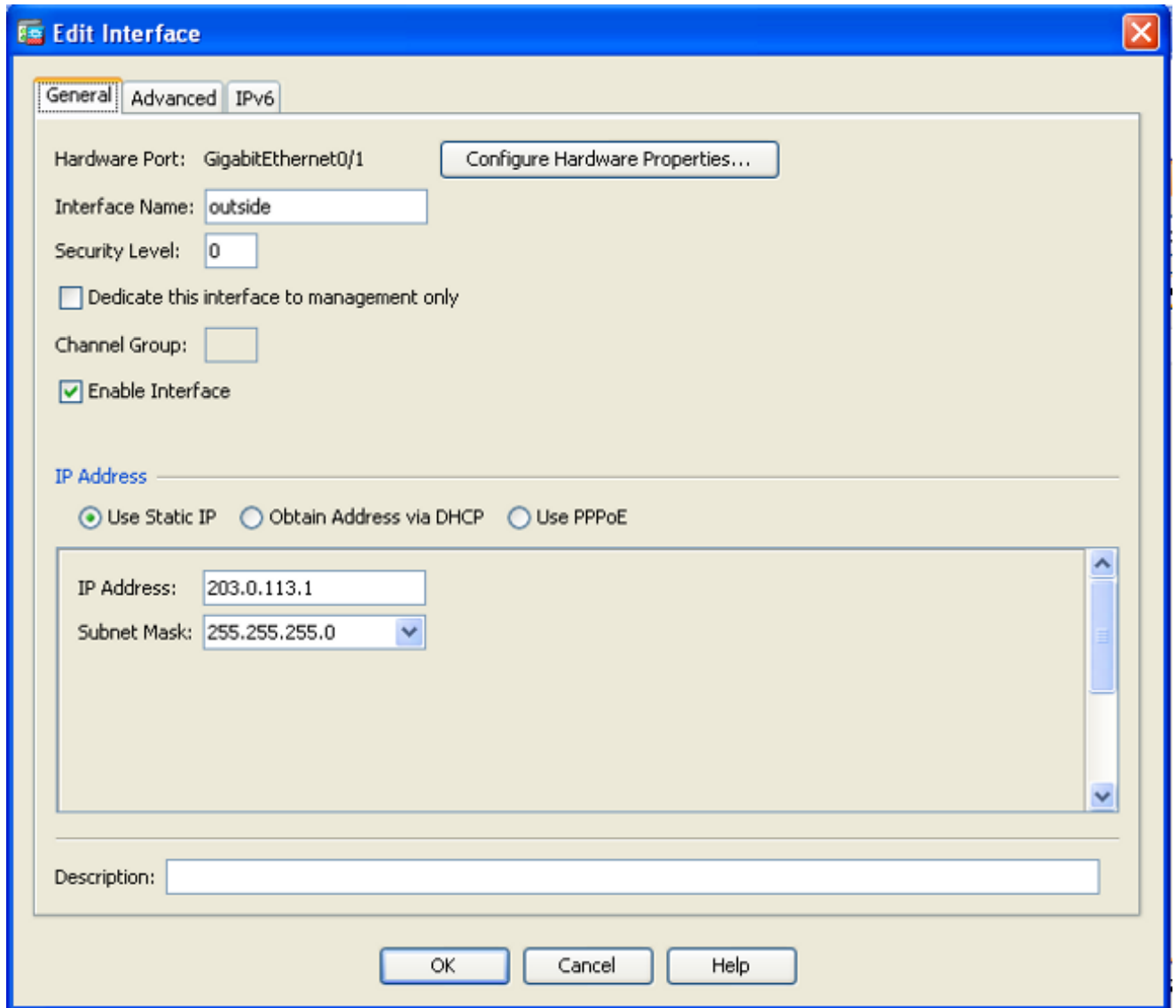
ASDM 애플리케이션을 사용하여 중복 또는 백업 ISP 지원을 구성하려면 다음 단계를 [완료하십시오](#)



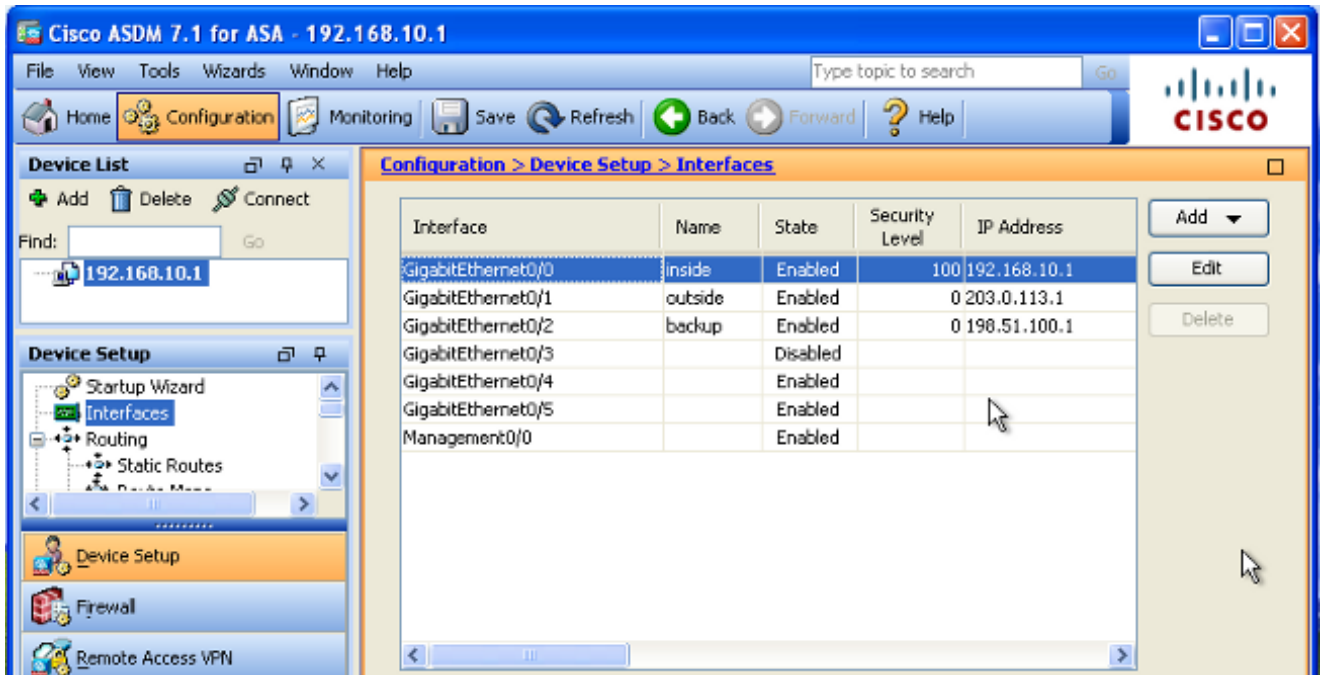
1. ASDM 애플리케이션 내에서 Configuration(컨피그레이션)을 클릭한 다음 Interfaces(인터페이스)를 클릭합니다.



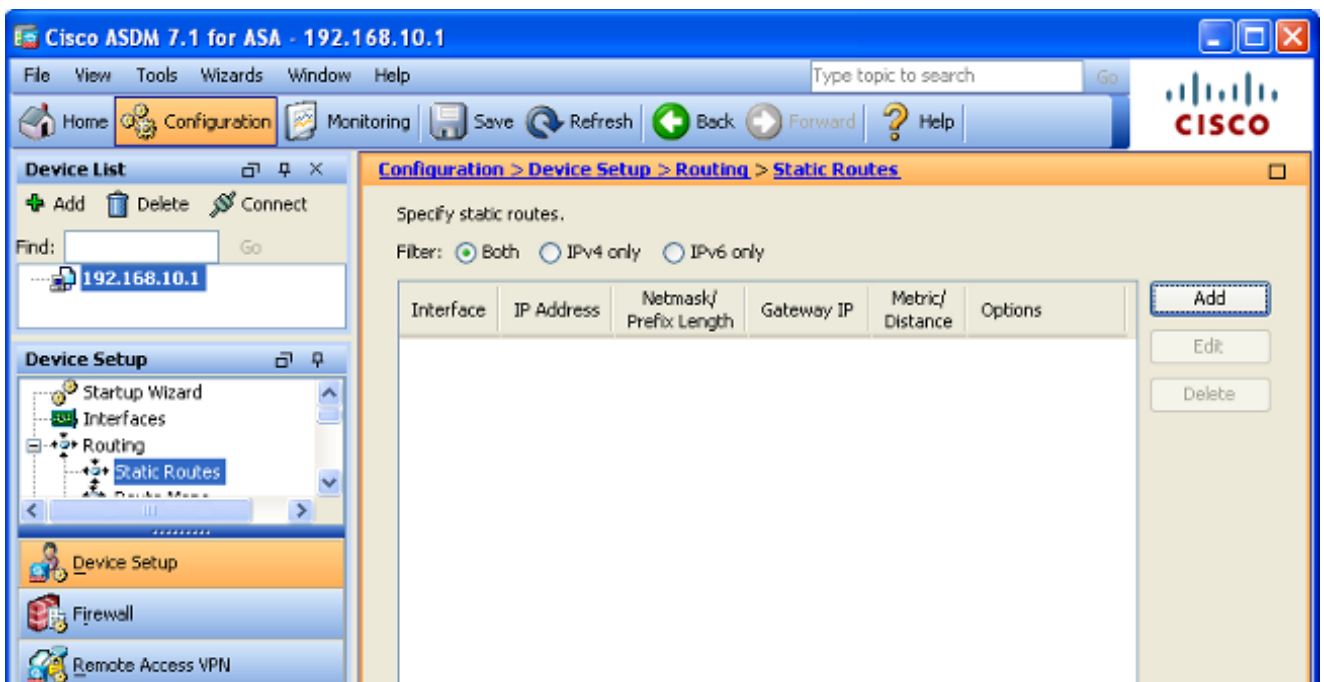
2. Interfaces 목록에서 GigabitEthernet0/1을 선택한 다음 Edit를 클릭합니다. 이 대화 상자가 나타납니다.



3. Enable Interface(인터페이스 활성화) 확인란을 선택하고 Interface Name(인터페이스 이름), Security Level(보안 레벨), IP Address(IP 주소) 및 Subnet Mask(서브넷 마스크) 필드에 적절한 값을 입력합니다.
4. 대화 상자를 닫으려면 OK를 클릭합니다.
5. 필요에 따라 다른 인터페이스를 구성한 다음 Apply를 클릭하여 ASA 컨피그레이션을 업데이트합니다.



6. Routing을 선택하고 ASDM 애플리케이션의 왼쪽에 있는 Static Routes를 클릭합니다.



7. 새 고정 경로를 추가하려면 Add를 클릭합니다. 이 대화 상자가 나타납니다.

**Edit Static Route**

IP Address Type:  IPv4  IPv6

Interface:

Network:

Gateway IP:  Metric:

**Options**

None

Tunneled (Default tunnel gateway for VPN traffic)

Tracked

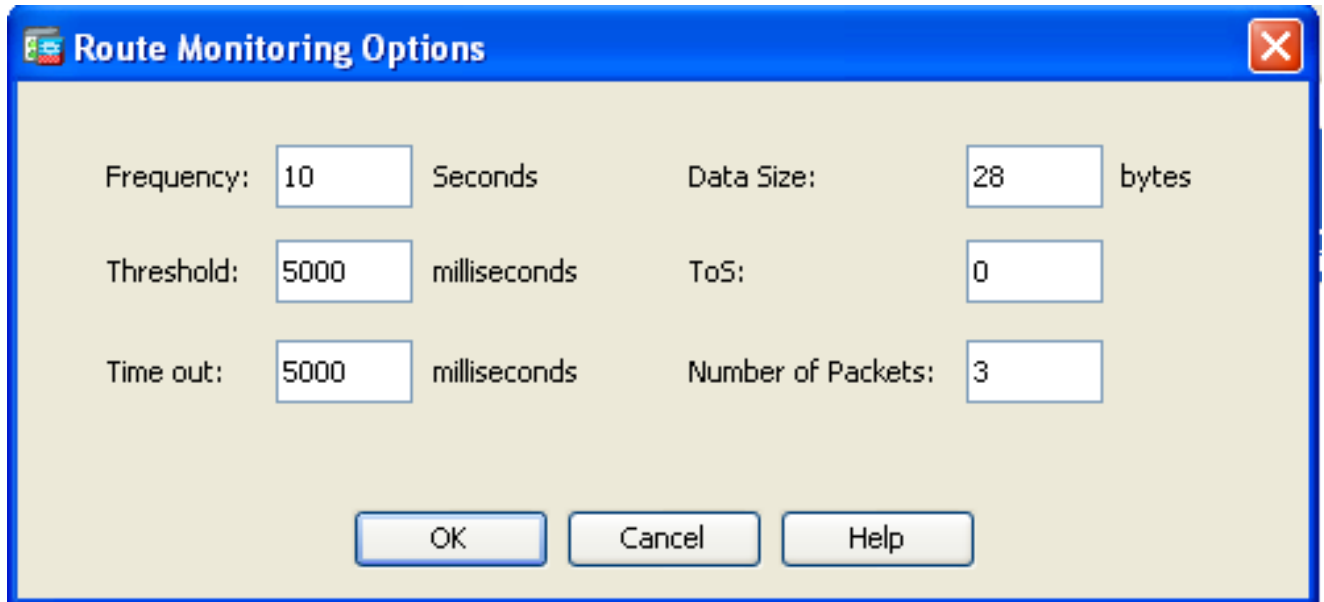
Track ID:  Track IP Address:

SLA ID:  Target Interface:

**Monitoring Options**

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

8. Interface Name 드롭다운 목록에서 경로가 상주하는 인터페이스를 선택하고 게이트웨이에 도달하도록 기본 경로를 구성합니다. 이 예에서 203.0.113.2는 기본 ISP 게이트웨이이고 4.2.2.2는 ICMP 에코로 모니터링할 객체입니다.
9. Options(옵션) 영역에서 Tracked(추적됨) 라디오 버튼을 클릭하고 Track ID(추적 ID), SLA ID(SLA ID) 및 Track IP Address(추적 IP 주소) 필드에 적절한 값을 입력합니다.
10. Monitoring Options(모니터링 옵션)를 클릭합니다. 이 대화 상자가 나타납니다.



11. 빈도 및 기타 모니터링 옵션에 대한 적절한 값을 입력한 다음 확인을 클릭합니다.
12. 인터넷에 연결할 경로를 제공하려면 보조 ISP에 다른 고정 경로를 추가합니다. 보조 경로로 만들려면 254와 같이 더 높은 메트릭으로 이 경로를 구성합니다. 기본 경로(기본 ISP)에 장애가 발생하면 해당 경로가 라우팅 테이블에서 제거됩니다. 이 보조 경로(보조 ISP)는 대신 PIX(Private Internet Exchange) 라우팅 테이블에 설치됩니다.
13. 대화 상자를 닫으려면 OK를 클릭합니다.

**Edit Static Route**

IP Address Type:  IPv4  IPv6

Interface: backup

Network: any4

Gateway IP: 198.51.100.2 Metric: 254

**Options**

None

Tunneled (Default tunnel gateway for VPN traffic)

Tracked

Track ID:  Track IP Address:

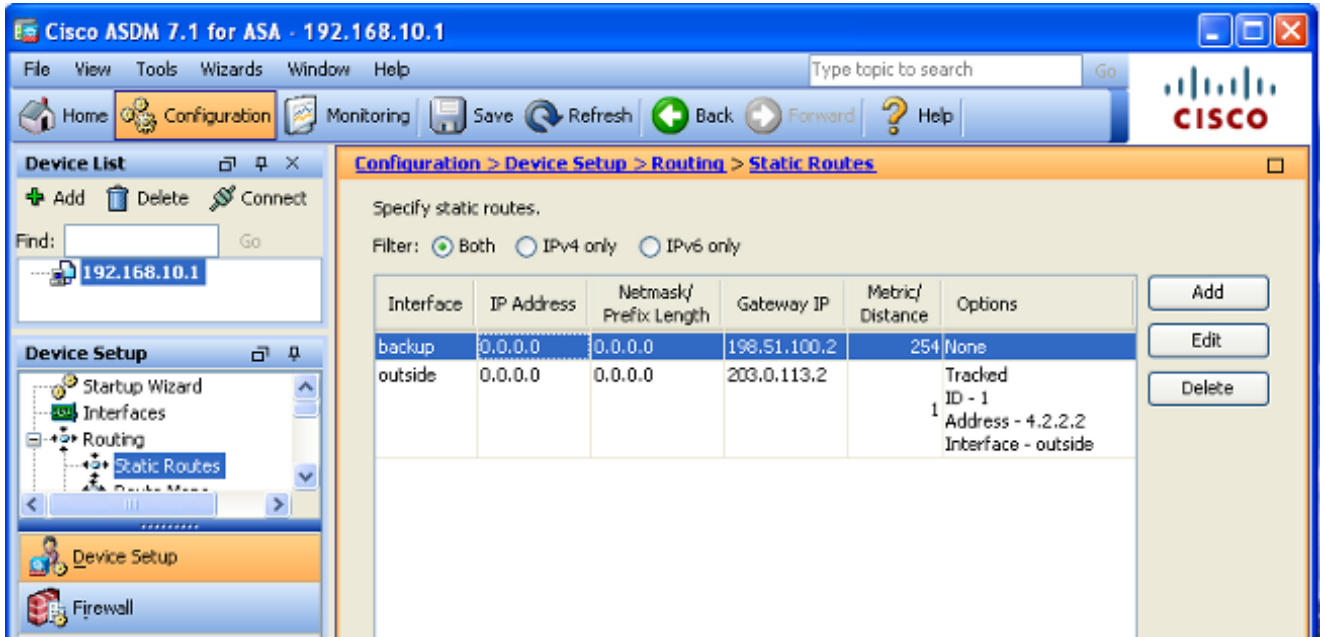
SLA ID:  Target Interface: backup

Monitoring Options

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

OK Cancel Help

컨피그레이션이 Interface(인터페이스) 목록에 나타납니다.




14. ASA 컨피그레이션을 업데이트하려면 라우팅 컨피그레이션을 선택한 다음 Apply를 클릭합니다.

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

구성이 완료되었는지 확인합니다.

 참고: Output [Interpreter Tool](#)([등록된](#) 고객만 해당)은 특정 show 명령을 지원합니다. show 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

컨피그레이션이 완료되었는지 확인하려면 다음 show 명령을 사용합니다.

- show running-config sla monitor - 이 명령의 출력에는 컨피그레이션의 SLA 명령이 표시됩니다.

```
<#root>
```

```
ASA#
```

```
show running-config sla monitor
```

```
sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10
 sla monitor schedule 123 life forever start-time now
```

- show sla monitor configuration - 이 명령의 출력에는 작업의 현재 컨피그레이션 설정이 표시

됩니다.

<#root>

ASA#

```
show sla monitor configuration 123
```

```
IP SLA Monitor, Infrastructure Engine-II.  
Entry number: 123  
Owner:  
Tag:  
Type of operation to perform: echo  
Target address: 4.2.2.2  
Interface: outside  
Number of packets: 3  
Request size (ARR data portion): 28  
Operation timeout (milliseconds): 5000  
Type Of Service parameters: 0x0  
Verify data&colon; No  
Operation frequency (seconds): 10  
Next Scheduled Start Time: Start Time already passed  
Group Scheduled : FALSE  
Life (seconds): Forever  
Entry Ageout (seconds): never  
Recurring (Starting Everyday): FALSE  
Status of entry (SNMP RowStatus): Active  
Enhanced History:
```

- show sla monitor operational-state - 이 명령의 출력에는 SLA 작업의 작업 통계가 표시됩니다

- 기본 ISP가 실패하기 전에 작동 상태가 됩니다.

<#root>

ASA#

```
show sla monitor operational-state 123
```

```
Entry number: 123  
Modification time: 13:30:40.672 IND Sun Jan 4 2015  
Number of Octets Used by this Entry: 2056  
Number of operations attempted: 46  
Number of operations skipped: 0  
Current seconds left in Life: Forever  
Operational state of entry: Active  
Last time this entry was reset: Never  
Connection loss occurred: FALSE
```

```
Timeout occurred: FALSE
```

```
Over thresholds occurred: FALSE
```



Latest RTT (milliseconds): 1

Latest operation start time: 13:38:10.672 IND Sun Jan 4 2015

Latest operation return code: OK

RTT Values:

RTTAvg: 1	RTTMin: 1	RTTMax: 1
NumOfRTT: 3	RTTSum: 3	RTTSum2: 3

- 기본 ISP에 장애가 발생하고 ICMP에 시간 초과가 발생한 경우 작동 상태는 다음과 같습니다.

<#root>

ASA#

show sla monitor operational-state

Entry number: 123  
Modification time: 13:30:40.671 IND Sun Jan 4 2015  
Number of Octets Used by this Entry: 2056  
Number of operations attempted: 57  
Number of operations skipped: 0  
Current seconds left in Life: Forever  
Operational state of entry: Active  
Last time this entry was reset: Never  
Connection loss occurred: FALSE

Timeout occurred: TRUE

Over thresholds occurred: FALSE

Latest RTT (milliseconds): NoConnection/Busy/Timeout

Latest operation start time: 13:40:00.672 IND Sun Jan 4 2015

Latest operation return code: Timeout

RTT Values:

RTTAvg: 0	RTTMin: 0	RTTMax: 0
NumOfRTT: 0	RTTSum: 0	RTTSum2: 0

백업 경로가 설치되어 있는지 확인합니다(CLI 방법)

백업 경로가 설치되어 있는지 확인하려면 show route 명령을 입력합니다.

기본 ISP에 장애가 발생하기 전에 라우팅 테이블이 다음과 유사하게 표시됩니다.

```
<#root>
```

```
ASA#
```

```
show 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 203.0.113.2 to network 0.0.0.0
```

```
C 203.0.113.0 255.255.255.0 is directly connected, outside
C 192.168.10.0 255.255.255.0 is directly connected, inside
C 198.51.100.0 255.255.255.0 is directly connected, backup
S* 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside
```

기본 ISP에 장애가 발생하면 고정 경로가 제거되고 백업 경로가 설치되면 라우팅 테이블이 다음과 유사하게 표시됩니다.

```
<#root>
```

```
ASA#
```

```
show 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
```

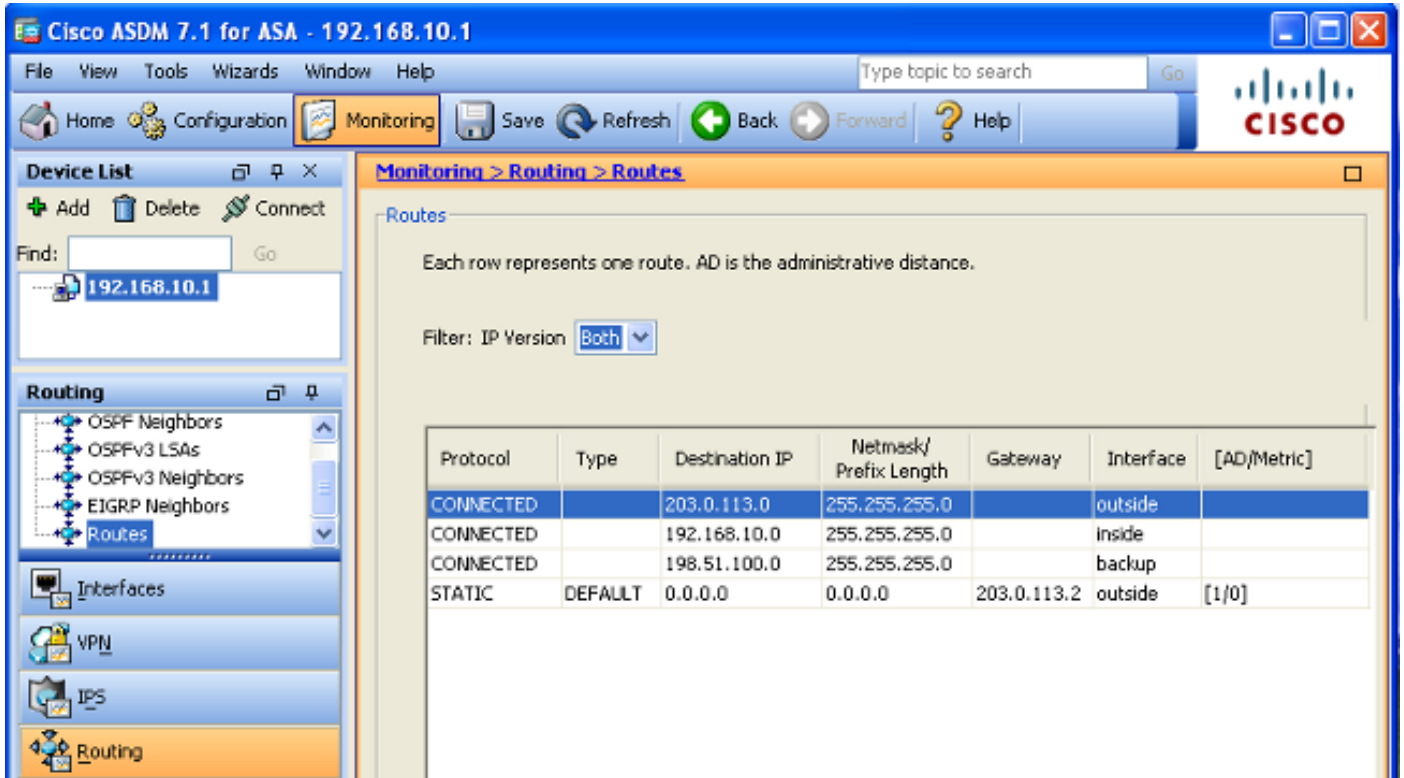
```
Gateway of last resort is 198.51.100.2 to network 0.0.0.0
```

```
C 203.0.113.0 255.255.255.0 is directly connected, outside
C 192.168.10.0 255.255.255.0 is directly connected, inside
C 198.51.100.0 255.255.255.0 is directly connected, backup
S* 0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

## 백업 경로가 설치되어 있는지 확인합니다(ASDM 방법)

백업 경로가 ASDM을 통해 설치되었는지 확인하려면 Monitoring > Routing으로 이동한 다음 라우팅 트리에서 Routes를 선택합니다.

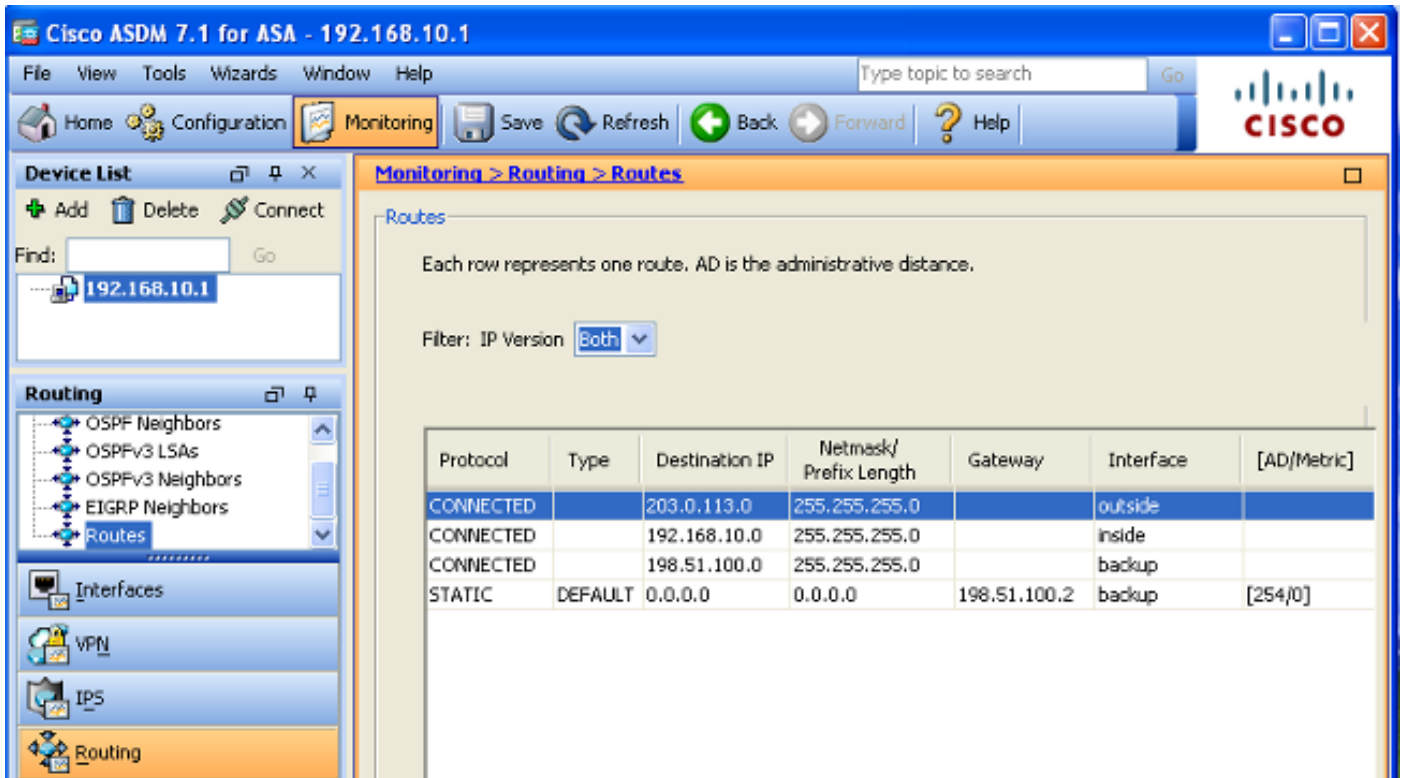
기본 ISP에 장애가 발생하기 전에 라우팅 테이블이 다음 이미지에 표시된 것과 유사하게 나타납니다. DEFAULT 경로는 외부 인터페이스를 통해 203.0.113.2를 가리킵니다.



The screenshot shows the Cisco ASDM 7.1 for ASA interface. The main window displays the 'Monitoring > Routing > Routes' page. The left sidebar shows the 'Routing' section selected. The main content area shows a table of routes. The table has the following data:

Protocol	Type	Destination IP	Netmask/Prefix Length	Gateway	Interface	[AD/Metric]
CONNECTED		203.0.113.0	255.255.255.0		outside	
CONNECTED		192.168.10.0	255.255.255.0		inside	
CONNECTED		198.51.100.0	255.255.255.0		backup	
STATIC	DEFAULT	0.0.0.0	0.0.0.0	203.0.113.2	outside	[1/0]

기본 ISP에 장애가 발생하면 경로가 제거되고 백업 경로가 설치됩니다. 이제 기본 경로는 백업 인터페이스를 통해 198.51.100.2를 가리킵니다.



## 문제 해결

이 절에서는 몇 가지 유용한 debug 명령을 제공하고 추적된 경로가 불필요하게 제거되는 문제를 해결하는 방법에 대해 설명합니다.

### 디버그 명령

다음과 같은 debug 명령을 사용하여 컨피그레이션 문제를 해결할 수 있습니다.

- debug sla monitor trace - 이 명령의 출력에는 에코 작업의 진행률이 표시됩니다.
  - 추적된 개체(기본 ISP 게이트웨이)가 작동 중이고 ICMP가 정상적으로 작동하면 다음과 같은 출력이 표시됩니다.

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=1 OK
IP SLA Monitor(123) Scheduler: Updating result
```

- 추적된 객체(기본 ISP 게이트웨이)가 중지되고 ICMP 에코가 실패할 경우 다음과 같이 출력이 표시됩니다.

```
IP SLA Monitor(123) Scheduler: Starting an operation
```

```
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) Scheduler: Updating result
```

- debug sla monitor error - 이 명령의 출력에는 SLA 모니터 프로세스에서 발생하는 모든 오류가 표시됩니다.
  - 추적된 개체(기본 ISP 게이트웨이)가 작동 중이고 ICMP가 성공하면 다음과 같이 출력이 표시됩니다.

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
```

- 추적된 객체(기본 ISP 게이트웨이)가 중지되고 추적된 경로가 제거되면 다음과 같이 출력이 표시됩니다.

<#root>

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:02
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:02
%ASA-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 203.0.113.2,
distance 1, table Default-IP-Routing-Table, on interface outside
```

```
!--- 4.2.2.2 is unreachable, so the route to the Primary ISP is removed.
```

## 추적된 경로가 불필요하게 제거됨

추적 경로가 불필요하게 제거된 경우 모니터링 대상이 에코 요청을 수신할 수 있도록 항상 사용할 수 있는지 확인합니다.

또한 모니터링 대상의 상태(즉, 대상의 도달 가능 여부)가 기본 ISP 연결 상태와 긴밀하게 연결되어 있는지 확인합니다.

ISP 게이트웨이보다 더 먼 모니터링 대상을 선택하면 해당 경로를 따라 다른 링크가 실패하거나 다른 디바이스가 간섭을 일으킬 수 있습니다.

따라서 이 컨피그레이션을 사용하면 SLA 모니터에서 기본 ISP에 대한 연결이 실패했으며 ASA가 불필요하게 보조 ISP 링크로 장애 조치될 수 있습니다.

예를 들어, 지사 라우터를 모니터링 대상으로 선택할 경우 지사에 대한 ISP 연결 및 그 도중에 있는 다른 링크가 실패할 수 있습니다.

모니터링 작업에 의해 전송된 ICMP 에코가 실패하면 기본 ISP 링크가 여전히 활성 상태이더라도 기본 추적 경로가 제거됩니다.

이 예에서는 모니터링 대상으로 사용되는 기본 ISP 게이트웨이가 ISP에서 관리하며 ISP 링크의 다른 쪽에 있습니다.

이 컨피그레이션을 사용하면 모니터링 작업에서 전송한 ICMP 에코가 실패할 경우 ISP 링크가 거의 확실히 다운됩니다.

## 관련 정보

- [Cisco ASA 5500-X Series Next-Generation Firewall](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.