

为冗余或备用ISP链路配置ASA

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[静态路由跟踪功能概述](#)

[重要建议](#)

[配置](#)

[网络图](#)

[CLI 配置](#)

[ASDM 配置](#)

[验证](#)

[确认配置已完成](#)

[确认已安装备份路由 \(CLI方法 \)](#)

[确认已安装备份路由 \(ASDM方法 \)](#)

[故障排除](#)

[调试命令](#)

[不必要地删除了所跟踪的路由](#)

简介

本文档介绍如何配置Cisco ASA 5500系列自适应安全设备(ASA)以使用静态路由跟踪功能，以便设备使用冗余或备份互联网连接。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本9.x或更高版本的Cisco ASA 5555-X系列
- Cisco ASDM 7.x版或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本节概述本文档中介绍的静态路由跟踪功能，以及开始之前的一些重要建议。

静态路由跟踪功能概述

使用静态路由的一个问题是，不存在可确定路由是打开还是关闭的固有机制。即使下一跳网关不可用，路由表中也会保留该路由。只有在安全设备上的相关接口失效时，才会从路由表中删除静态路由。为了解决此问题，使用静态路由跟踪功能来跟踪静态路由的可用性。该功能从路由表中删除静态路由，并在发生故障时将其替换为备用路由。

静态路由跟踪允许ASA在主租用线路不可用时使用与辅助ISP的廉价连接。为了实现此冗余，ASA将静态路由与您定义的监控目标相关联。服务级别协议(SLA)操作使用定期ICMP回应请求监控目标。如果未收到回应应答，则该对象会被视为关闭，并且相关路由会从路由表中删除。并用以前配置的备份路由代替所删除的路由。当备份路由正在使用时，SLA监控操作会继续尝试到达监控目标。目标再次可用后，将替换路由表中的第一个路由，并删除备份路由。

在本文档中使用的示例中，ASA维护两个到Internet的连接。

- 第一个连接是通过主ISP提供的路由器访问的高速租用线路。
- 第二个连接是低速数字用户线路(DSL)，通过辅助ISP提供的DSL调制解调器访问。
- 本文档中描述的配置不能用于负载均衡或负载共享，因为ASA不支持该配置。

此配置仅用于冗余或备份用途。出站流量使用主ISP，如果主ISP发生故障，则使用辅助ISP。主ISP故障会导致流量临时中断。

只要租用线路处于活动状态，并且主ISP网关可访问，DSL连接就处于空闲。但是，如果与主ISP的连接断开，ASA会更改路由表以将流量定向到DSL连接。为了实现此冗余，使用静态路由跟踪。

ASA配置了静态路由，将所有Internet流量定向到主ISP。SLA监控进程每十秒检查一次，以确认主ISP网关可到达。如果SLA监控进程确定主ISP网关不可访问，则从路由表中删除将流量定向到该接口的静态路由。为替换该静态路由，安装了一条备用静态路由，用于将流量定向到辅助ISP。此备用静态路由通过DSL调制解调器将流量定向到辅助ISP，直到主ISP的链路可访问为止。

此配置提供了一种相对便宜的方法，可确保ASA后面的用户仍可访问出站互联网。如本文档所述，此设置并不总适合对ASA后的资源进行入站访问。要实现无缝入站连接，需要高级网络技能。本文档中不涉及这些技能。

重要建议

在尝试本文档中描述的配置之前，必须选择可响应互联网控制消息协议(ICMP)回应请求的监控目标。目标可以是您选择的任何网络对象，但建议使用与您的Internet服务提供商(ISP)连接紧密关联的目标。以下是一些可能的监控目标：

- ISP 网关地址
- 由另一个ISP管理的地址
- 另一网络上的服务器，例如ASA必须与之通信的身份验证、授权和记帐(AAA)服务器
- 另一个网络上的持久性网络对象（不宜选择晚间可能关闭的桌面或笔记本电脑）

本文档假设ASA完全可操作且已配置，以便允许思科自适应安全设备管理器(ASDM)进行配置更改。

有关如何允许ASDM配置设备的信息，请参阅CLI[手册1的配置HTTPS ASDM访问部分](#)：Cisco ASA系列常规操作CLI配置指南，9.1。

配置

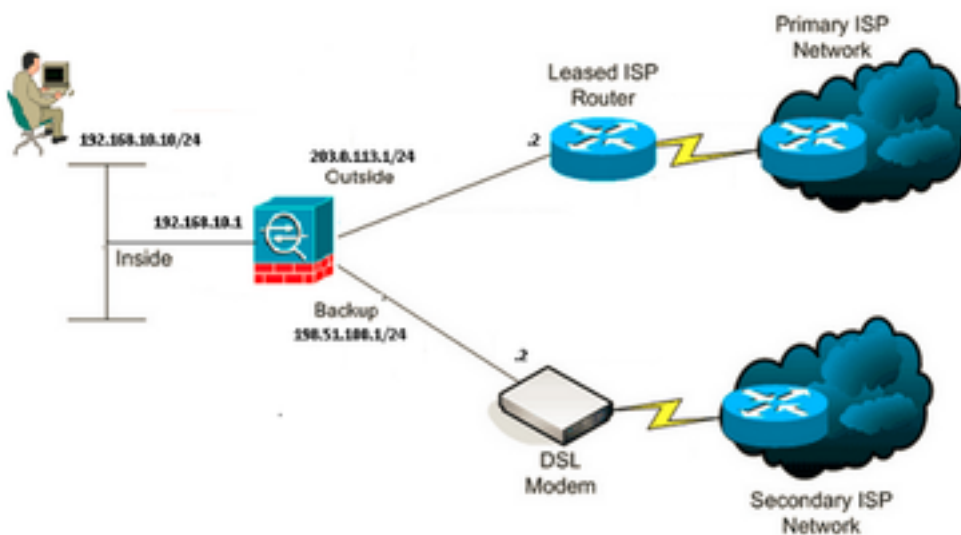
使用本节中介绍的信息配置ASA以使用静态路由跟踪功能。

使用[命令查找工具](#)(仅注册客户)，以获取有关本节中使用的命令的详细信息。

此配置中使用的IP地址在Internet上不可合法路由。它们是[RFC 1918](#)地址，用于实验环境。

网络图

本节提供的示例使用以下网络设置：



CLI 配置

使用以下信息通过CLI配置ASA:

```
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 track 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 x.x.x.x 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 track
!--- 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.**

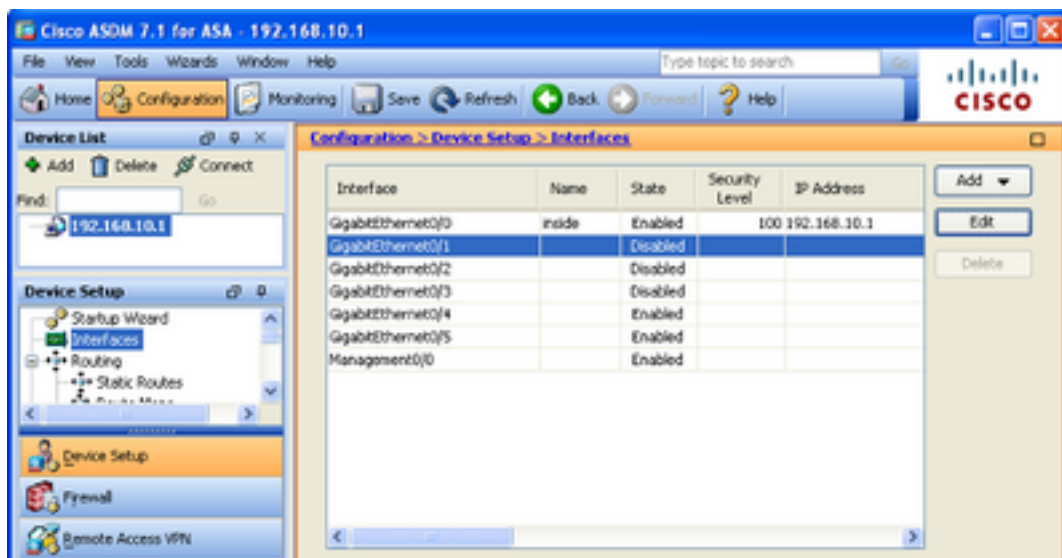
```
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
priority-queue inside
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map 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
```

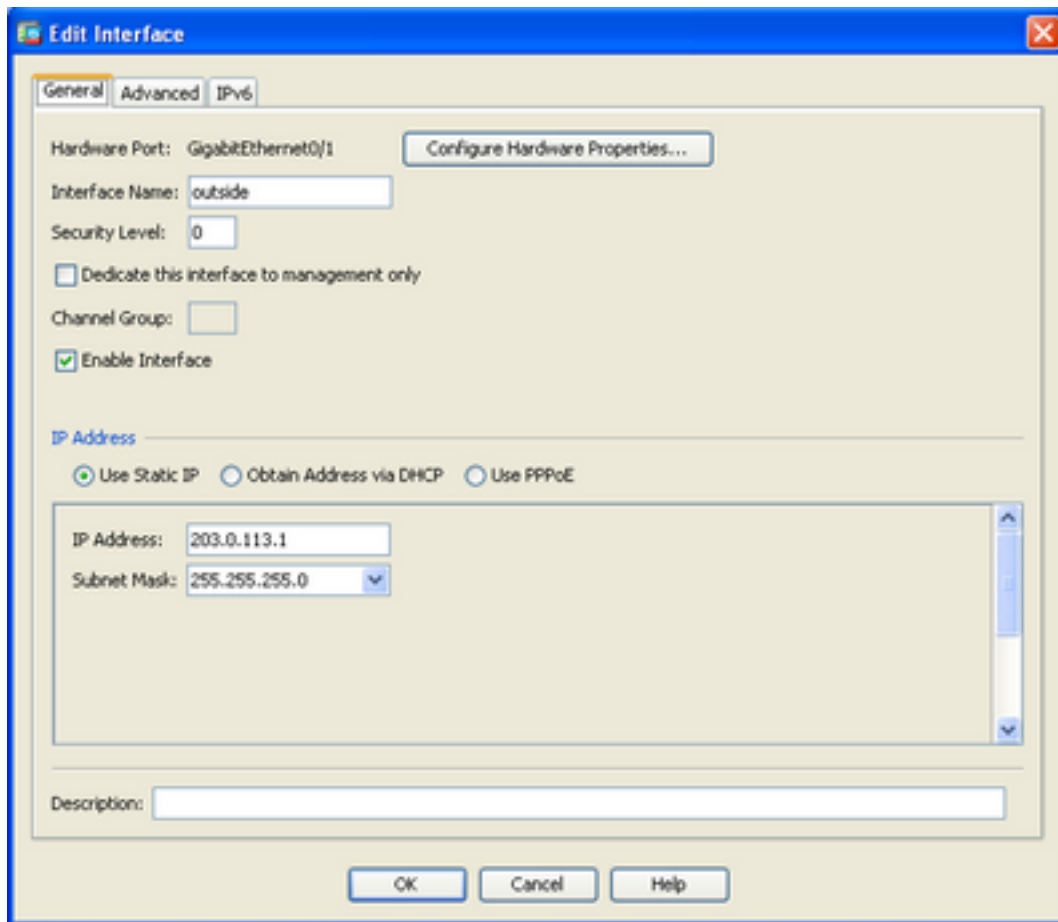
ASDM 配置

要使用ASDMApplication配置冗余或备用ISP支持，请完成以下步骤：

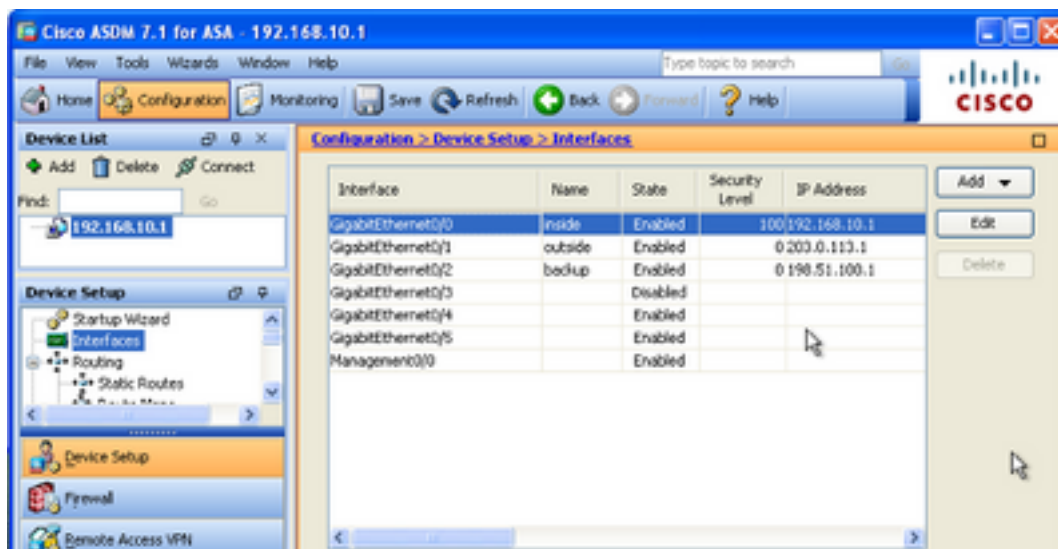
1. 在ASDM应用程序中，单击**Configuration**，然后单击**Interfaces**。



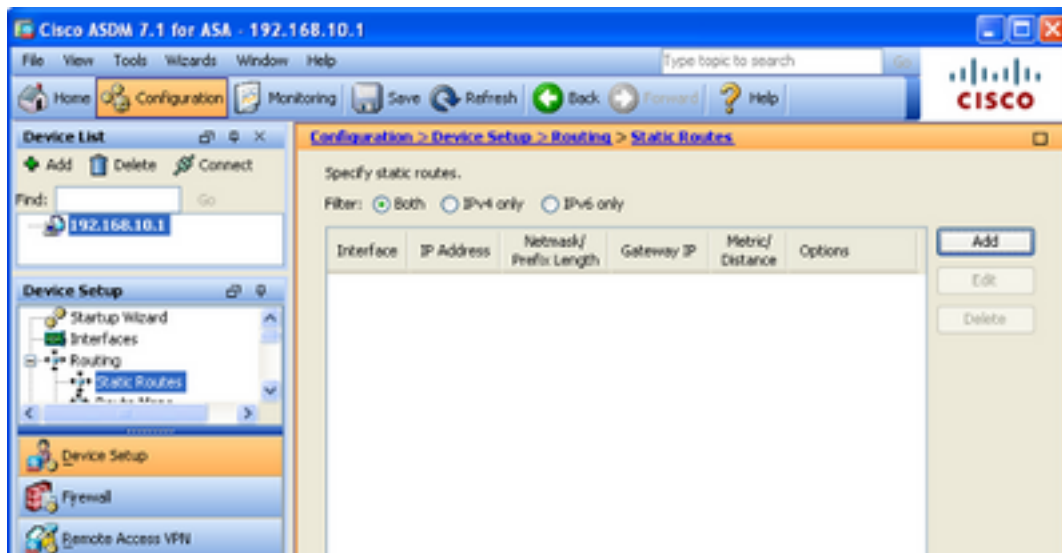
2. 从“接口”列表中选择GigabitEthernet0/1，然后单击**编辑**。此对话框出现：



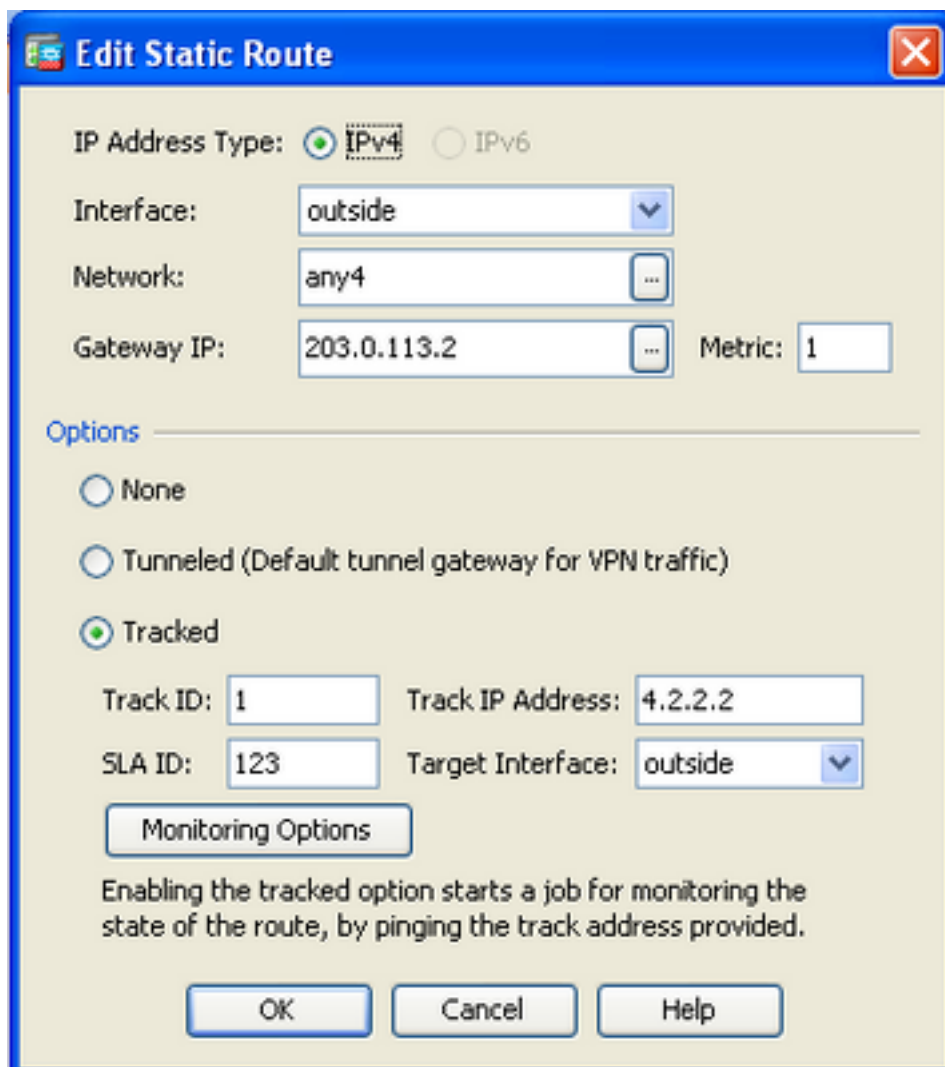
3. 选中启用接口复选框，并在接口名称、安全级别、IP地址和子网掩码字段中输入相应的值。
4. 单击“确定”以关闭对话框。
5. 根据需要配置其他接口，然后单击Apply以更新ASA配置：



6. 选择Routing并单击ASDM应用程序左侧的Static Route:



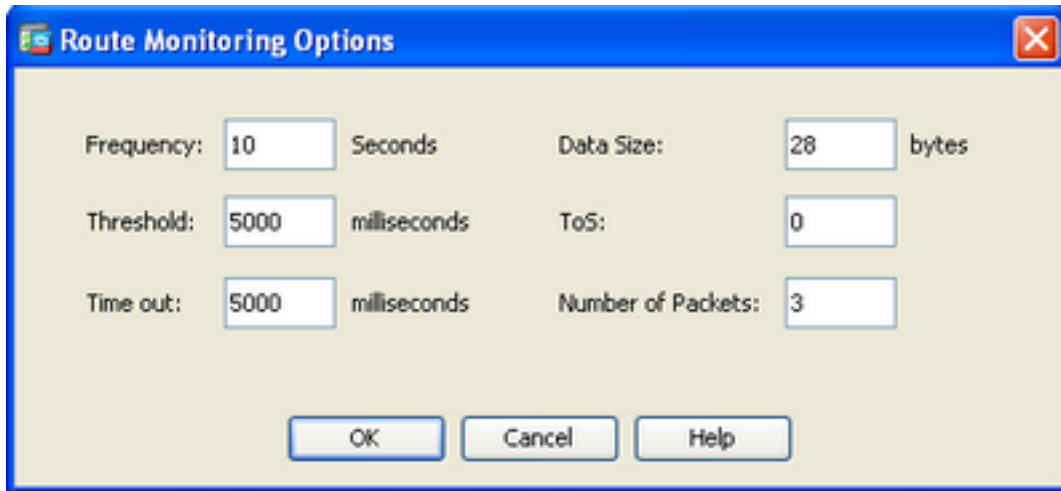
7. 单击Add以添加新的静态路由。此对话框出现：



8. 从 Interface Name 下拉列表中选择路由所在的接口，然后配置到达网关的默认路由。在本示例中，203.0.113.2是主ISP网关，10.0.0.0是使用ICMP回显进行监控的对象。

9. 在“选项”区域，单击“跟踪”按钮，并在“跟踪ID”、“SLA ID”和“跟踪IP地址”字段中输入相应的值。

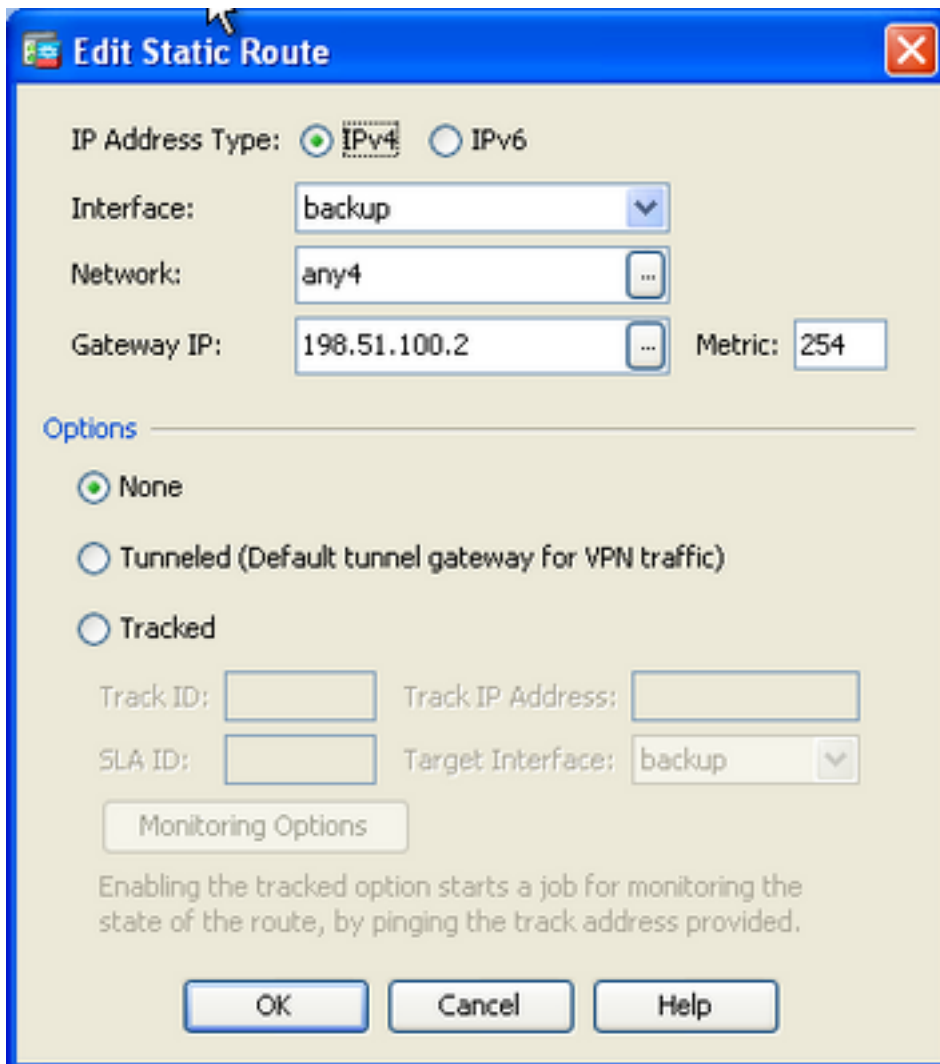
10. 单击“监控选项”。此对话框出现：



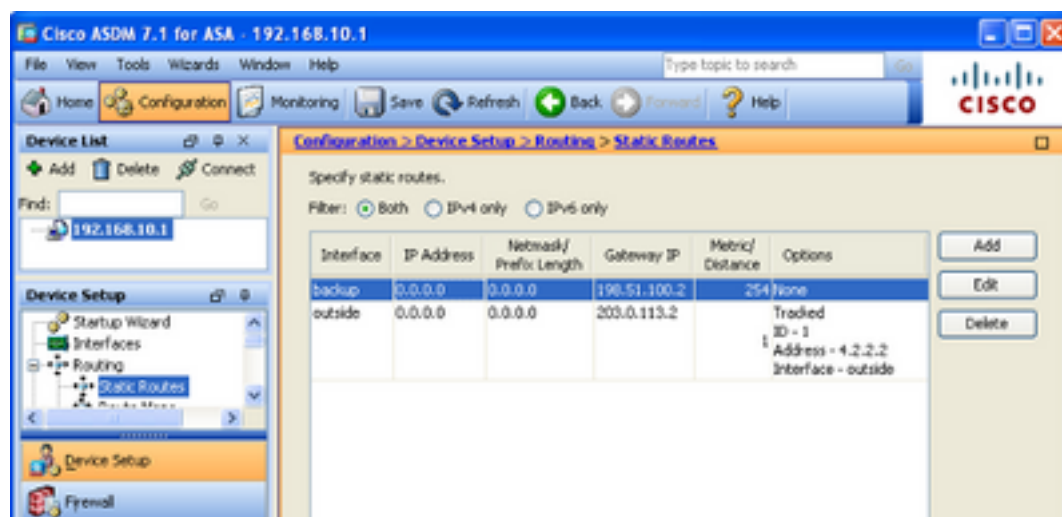
11. 为频率和其他监控选项输入适当的值，然后单击**确定**。

12. 添加辅助 ISP 的另一个静态路由，以提供到达 Internet 的路由。为使其成为辅助路由，请使用更高度量（如254）配置此路由。如果主路由（主ISP）发生故障，该路由将从路由表中删除。此辅助路由（辅助ISP）将安装在专用Internet交换(PIX)路由表中。

13. 单击“确定”以关闭对话框：



配置显示在接口列表中：



14. 选择路由配置，然后单击Apply以更新ASA配置。

验证

使用本部分可确认配置能否正常运行。

确认配置已完成

使用这些show命令以验证您的配置是否完整：

- **show running-config sla monitor** — 此命令的输出显示配置中的SLA命令。

```
ASA# show running-config sla monitor
sla monitor 123
  type echo protocol ipIcmpEcho 10.0.0.0 interface outside
  num-packets 3
  frequency 10
sla monitor schedule 123 life forever start-time now
```

- **show sla monitor configuration** — 此命令的输出显示操作的当前配置设置。

```
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: 10.0.0.0
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** — 此命令的输出显示SLA操作的运行统计信息。

在主 ISP 发生故障之前，正常运行的状态如下：

```
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
```

在主ISP发生故障（和ICMP回显超时）后，此状态为运行状态：

```
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
```

确认已安装备份路由（CLI方法）

输入**show route**命令以确认已安装备份路由。

在主ISP发生故障之前，路由表将如下所示：

```
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

主ISP发生故障后，会删除静态路由，并安装备用路由，路由表如下所示：

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

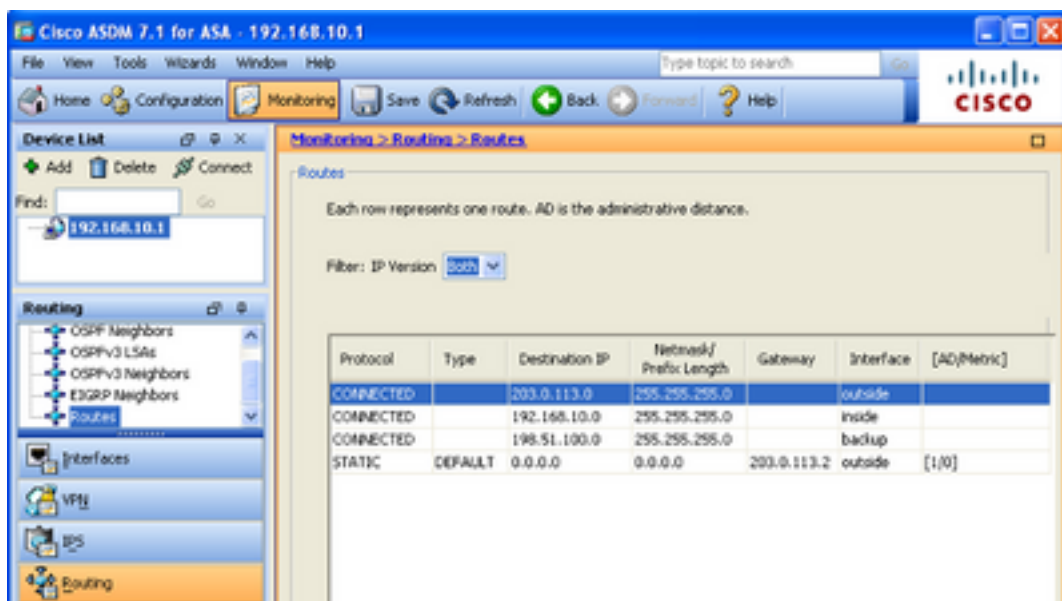
```
C 203.0.113.0 255.255.255.0 is directly connected, outside
C 192.168.10.0 255.255.255.0 is directly connected, inside
C 198.51.100.0 255.255.255.0 is directly connected, backup
```

S* 0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup

确认已安装备份路由 (ASDM方法)

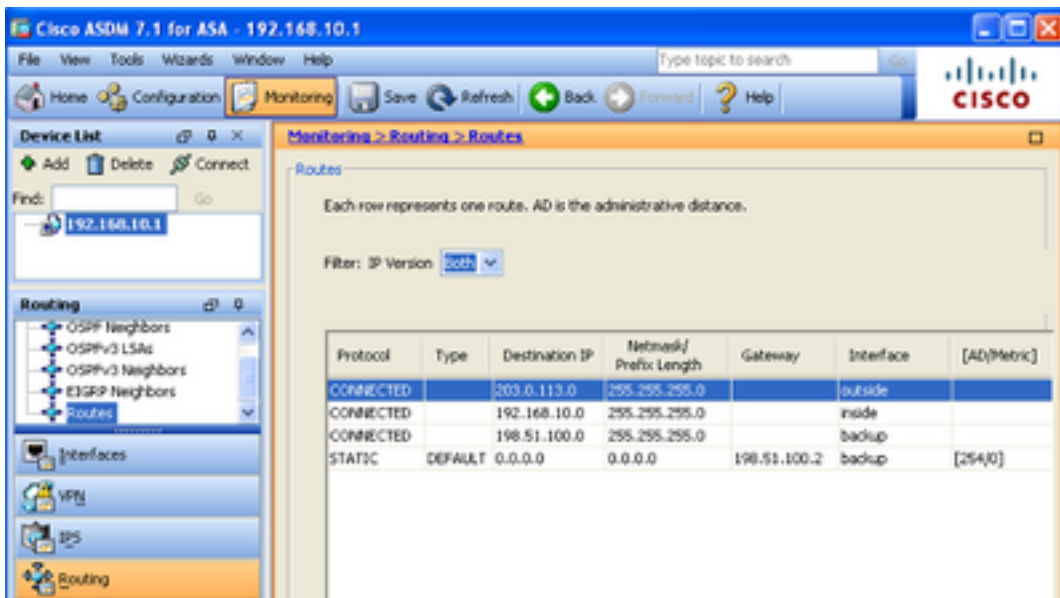
要确认备份路由是通过ASDM安装的，请导航到**Monitoring > Routing**，然后从Routing树中选择Routes。

在主ISP发生故障之前，路由表将类似于下一个映像中显示的路由表。请注意,DEFAULTRoute通过外部接口指向**203.0.113.2**:



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]

主ISP发生故障后，该路由将被删除，并安装备用路由。DEFAULTRoute现在通过backupinterface指向**198.51.100.2**:



故障排除

本节提供一些有用的debug命令，并介绍如何排除不必要地删除跟踪的路由的问题。

调试命令

您可以使用以下debug命令来排除配置问题：

- **debug sla monitor trace** — 此命令的输出显示回声操作的进度。

如果跟踪的对象（主ISP网关）为up状态且ICMP回显成功，则输出显示类似于以下内容：

```
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
```

如果跟踪的对象（主ISP网关）关闭，而ICMP回显失败，则输出显示类似如下：

```
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** — 此命令的输出显示SLA监控进程遇到的任何错误。

如果跟踪的对象（主ISP网关）为up状态且ICMP成功，则输出显示类似于以下内容：

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:10.0.0.0
%ASA-6-302020: Built outbound ICMP connection for faddr 10.0.0.0/0
gaddr 203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-6-302021: Teardown ICMP connection for faddr 10.0.0.0/0 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:10.0.0.0 duration 0:00:00
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:10.0.0.0
%ASA-6-302020: Built outbound ICMP connection for faddr 10.0.0.0/0
gaddr 203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-6-302021: Teardown ICMP connection for faddr 10.0.0.0/0 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:10.0.0.0 duration 0:00:00
```

如果跟踪的对象 (主ISP网关) 关闭 , 并且已删除跟踪的路由 , 则输出显示类似于以下内容 :

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:10.0.0.0
%ASA-6-302020: Built outbound ICMP connection for faddr 10.0.0.0/0
gaddr 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302020: Built outbound ICMP connection for faddr 10.0.0.0/0
gaddr 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302020: Built outbound ICMP connection for faddr 10.0.0.0/0
gaddr 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-6-302021: Teardown ICMP connection for faddr 10.0.0.0/0 gaddr
203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302021: Teardown ICMP connection for faddr 10.0.0.0/0 gaddr
203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302021: Teardown ICMP connection for faddr 10.0.0.0/0 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:10.0.0.0 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
```

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

不必要地删除了所跟踪的路由

如果不必要地删除了所跟踪的路由 , 请确保监控目标始终可供接收回声请求。此外 , 请确保监控目标状态 (即目标是否可访问) 与主 ISP 连接的状态紧密相关。

如果您选择的监控目标比ISP网关的距离更远 , 则该路由上的另一条链路可能发生故障 , 或者另一台设备可能会干扰。在此配置中 , 可能会导致SLA监控器断定到主ISP的连接失败 , 并导致ASA不必要地故障切换到辅助ISP链路。

例如 , 如果选择分支机构路由器作为监控目标 , 则 ISP 与分支机构的连接以及沿路的任何其他链路可能发生故障。监控操作发送的ICMP回显失败后 , 即会删除主要跟踪路由 , 即使主要ISP链路仍处于活动状态。

在本示例中 , 用作监控目标的主 ISP 网关由 ISP 管理 , 并位于 ISP 链路的另一端。此配置可确保如果监控操作发送的ICMP回显失败 , ISP链路几乎肯定会关闭。