为冗余或备用ISP链路配置ASA

目录

简介

本文档介绍如何配置Cisco ASA 5500系列静态路由跟踪功能以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。

相关产品

您还可以将此配置用于Cisco ASA 5500系列版本9.1(5)。

注意：backup interface命令是配置ASA 5505系列上的第四个接口所必需的。有关详细信息，请参阅Cisco安全设备命令参考7.2版的备份接口部分。

背景信息

本节概述本文档中介绍的静态路由跟踪功能，以及在开始之前提出的一些重要建议。

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处于开启还是关闭状态的固有机制。

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。

此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。

静态路由跟踪使ASA能够在主租用线路不可用时以低廉的成本连接到辅助ISP。

为了实现此冗余，ASA将静态路由与您定义的监控目标关联。

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，则会将该对象视为关闭，并从路由表中删除关联的路由。

并用以前配置的备份路由代替所删除的路由。

当使用备份路由时，SLA监控操作会继续尝试访问监控目标。

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维护两个与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。

第二个连接是通过辅助ISP提供的DSL调制解调器访问的低速数字用户线路(DSL)。

注：本文档中介绍的配置不能用于负载均衡或负载共享，因为ASA不支持此配置。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将更改路由表以将流量定向到DSL连接。

使用静态路由跟踪来实现此冗余。

ASA配置了静态路由，该路由将所有Internet流量定向到主ISP。

SLA监控进程每10秒检查一次，以确认主ISP网关可访问。

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廉价的方式，可确保出站Internet访问仍然对ASA后面的用户可用。

如本文档所述，此设置并不总是适用于对ASA后资源的入站访问。要实现无缝的入站连接，需要具备高级网络技能。

本文档中不涉及这些技能。

重要建议

在尝试本文档中介绍的配置之前，您必须选择可以响应Internet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Internet服务提供商(ISP)连接密切相关的目标。

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
- ASA必须与之通信的另一网络上的服务器，例如身份验证、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计算机）

本文档假设ASA完全正常运行且经过配置，以允许思科自适应安全设备管理器(ASDM)进行配置更改。

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

配置

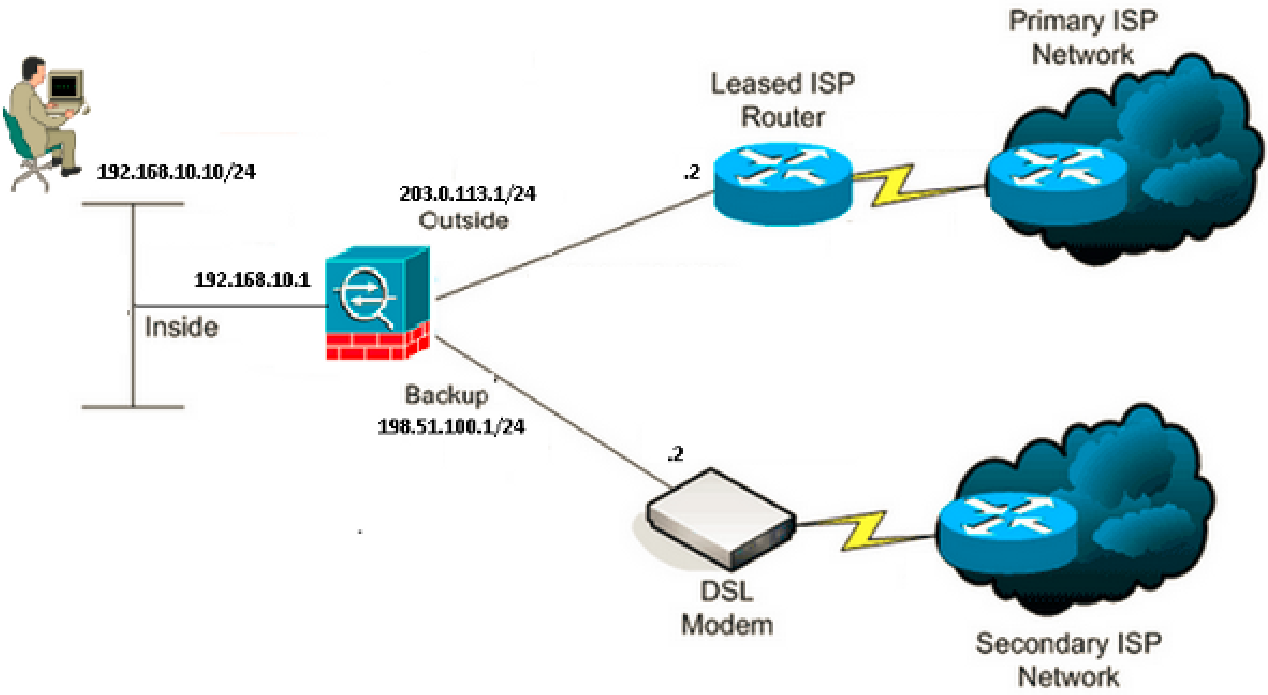
使用本节中描述的信息配置ASA以使用静态路由跟踪功能。

注：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

注：此配置中使用的IP地址不能在Internet上合法路由。它们是RFC 1918地址，在实验室环境中使用。

网络图

本部分提供的示例使用此网络设置：



CLI 配置

使用此信息可通过CLI配置ASA:

<#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
```

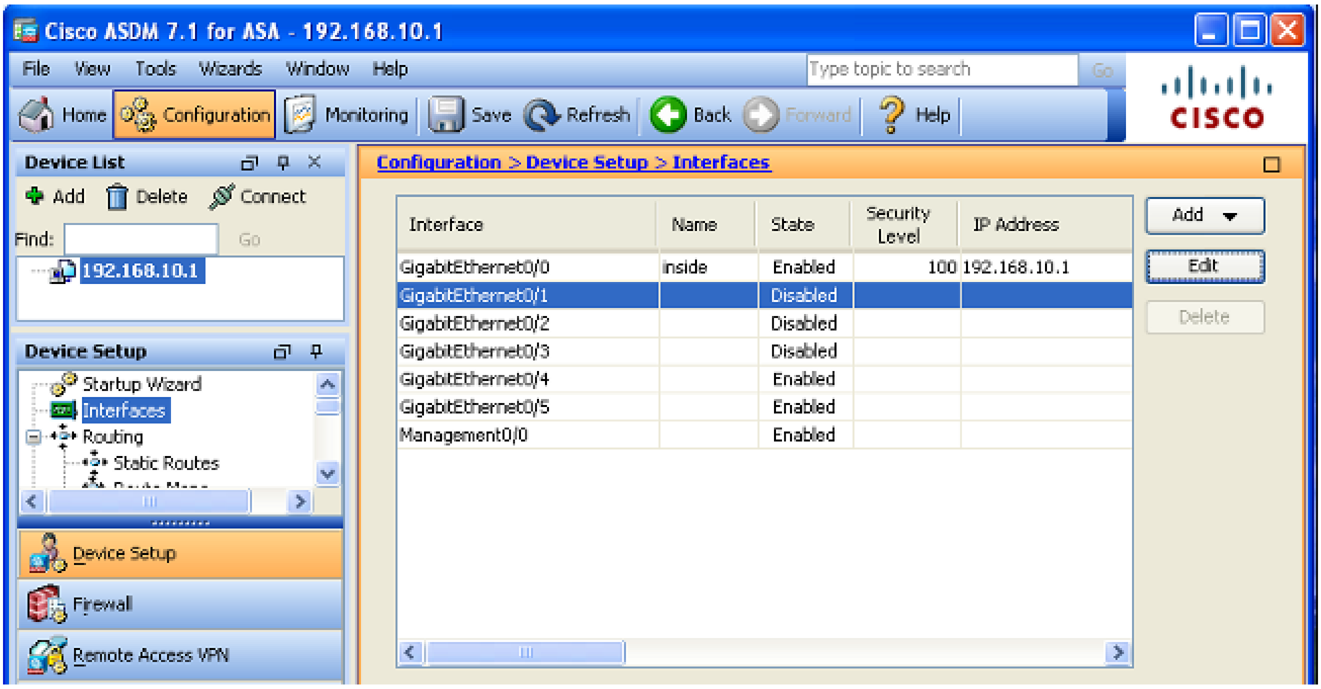
```
 nat (inside,outside) dynamic interface
object network inside_network
 nat (inside,backup) dynamic interface


!--- 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 配置

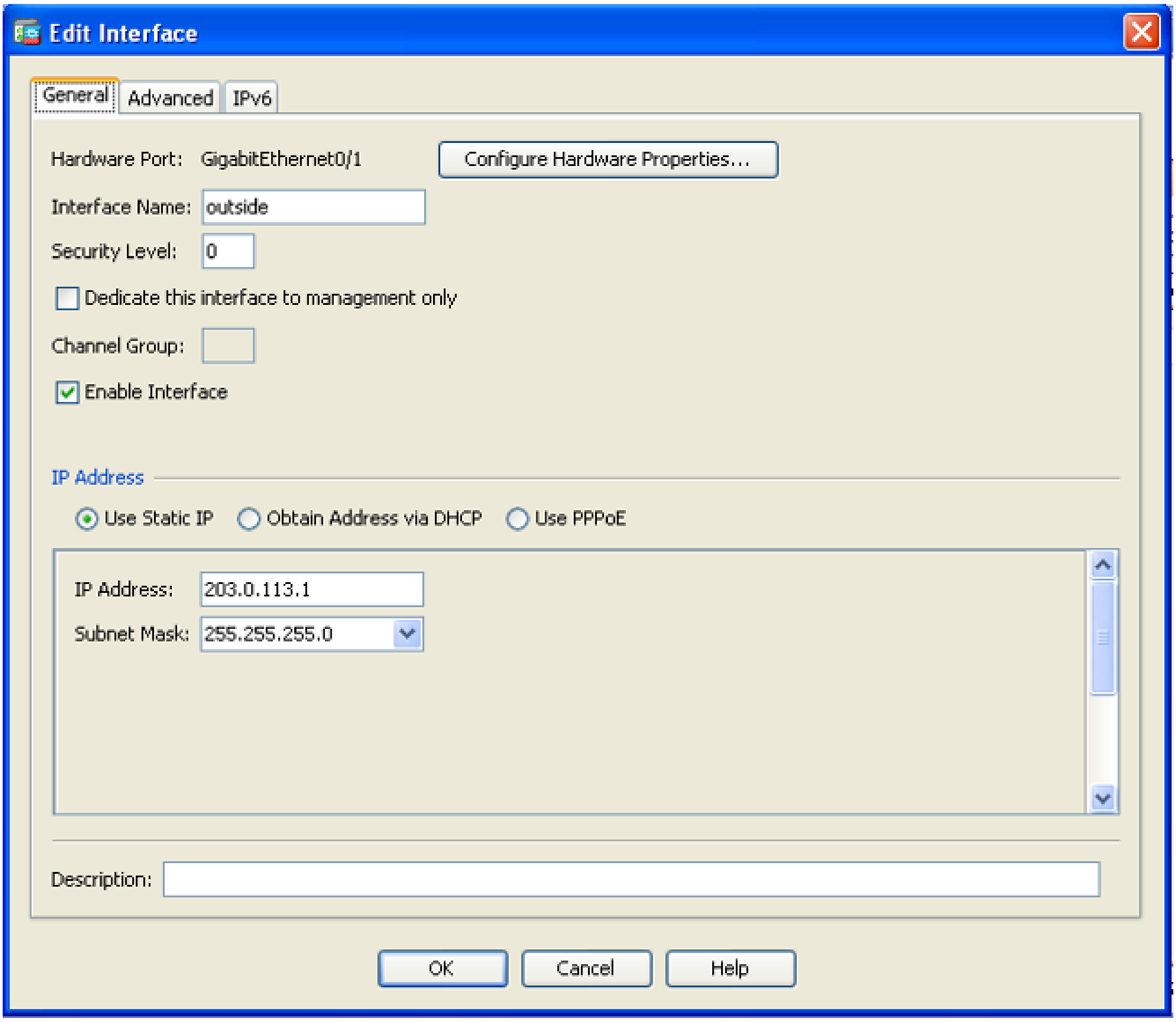
完成以下步骤，以便使用ASDM应用配置冗余或备份ISP支持：

1. 在ASDM应用中，单击Configuration，然后单击Interfaces。



Interface	Name	State	Security Level	IP Address
GigabitEthernet0/0	inside	Enabled	100	192.168.10.1
GigabitEthernet0/1		Disabled		
GigabitEthernet0/2		Disabled		
GigabitEthernet0/3		Disabled		
GigabitEthernet0/4		Enabled		
GigabitEthernet0/5		Enabled		
Management0/0		Enabled		

2. 从接口列表中选择GigabitEthernet0/1，然后单击Edit。 此对话框出现：



Hardware Port: GigabitEthernet0/1

Interface Name: outside

Security Level: 0

□ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 203.0.113.1

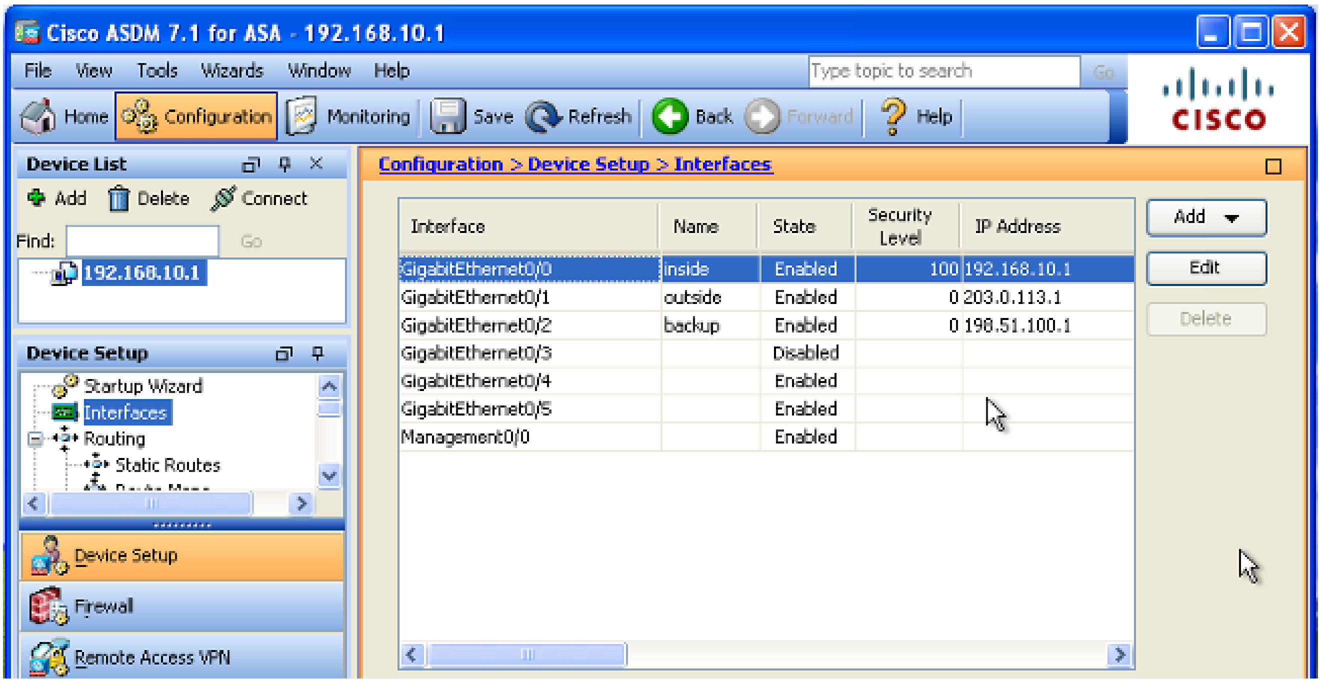
Subnet Mask: 255.255.255.0

Description:

3. 选中Enable Interface复选框，并在Interface Name、Security Level、IP Address和Subnet Mask字段中输入相应的值。

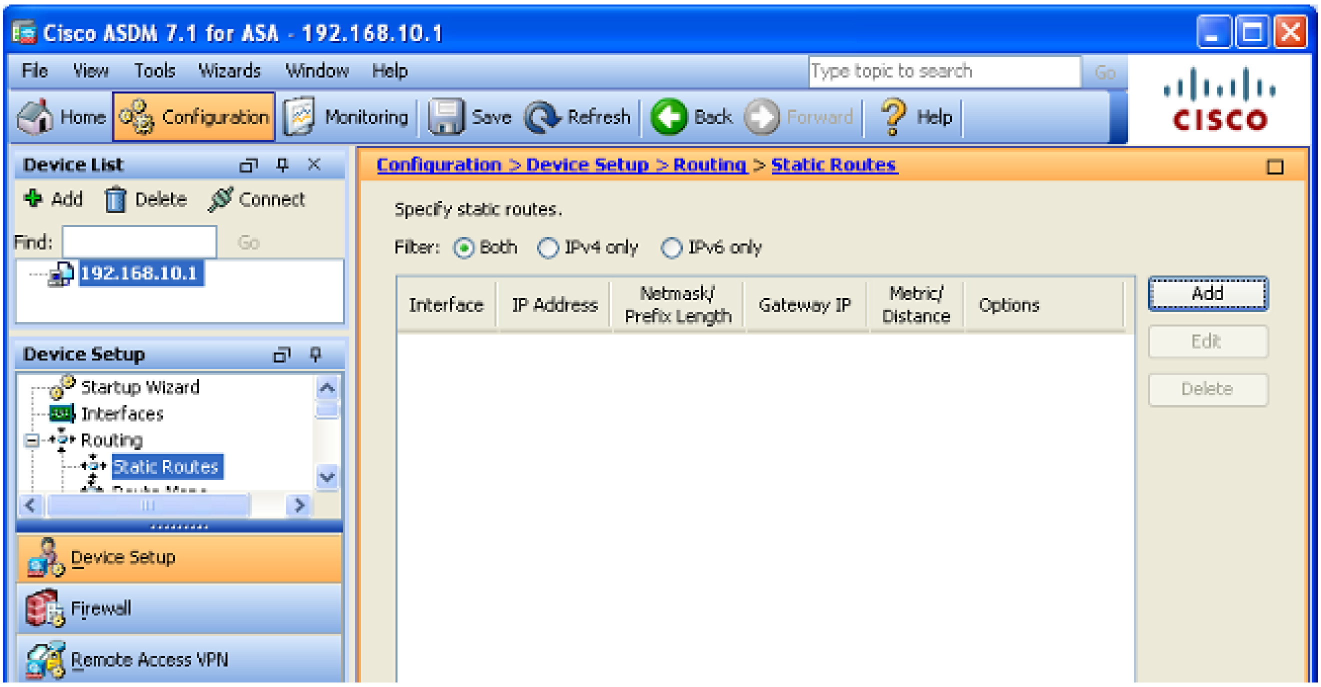
4. 单击 OK 关闭对话框。

5. 根据需要配置其他接口，然后单击Apply以更新ASA配置：



Interface	Name	State	Security Level	IP Address
GigabitEthernet0/0	inside	Enabled	100	192.168.10.1
GigabitEthernet0/1	outside	Enabled	0	203.0.113.1
GigabitEthernet0/2	backup	Enabled	0	198.51.100.1
GigabitEthernet0/3		Disabled		
GigabitEthernet0/4		Enabled		
GigabitEthernet0/5		Enabled		
Management0/0		Enabled		

6. 选择Routing，然后单击ASDM应用左侧的Static Routes:

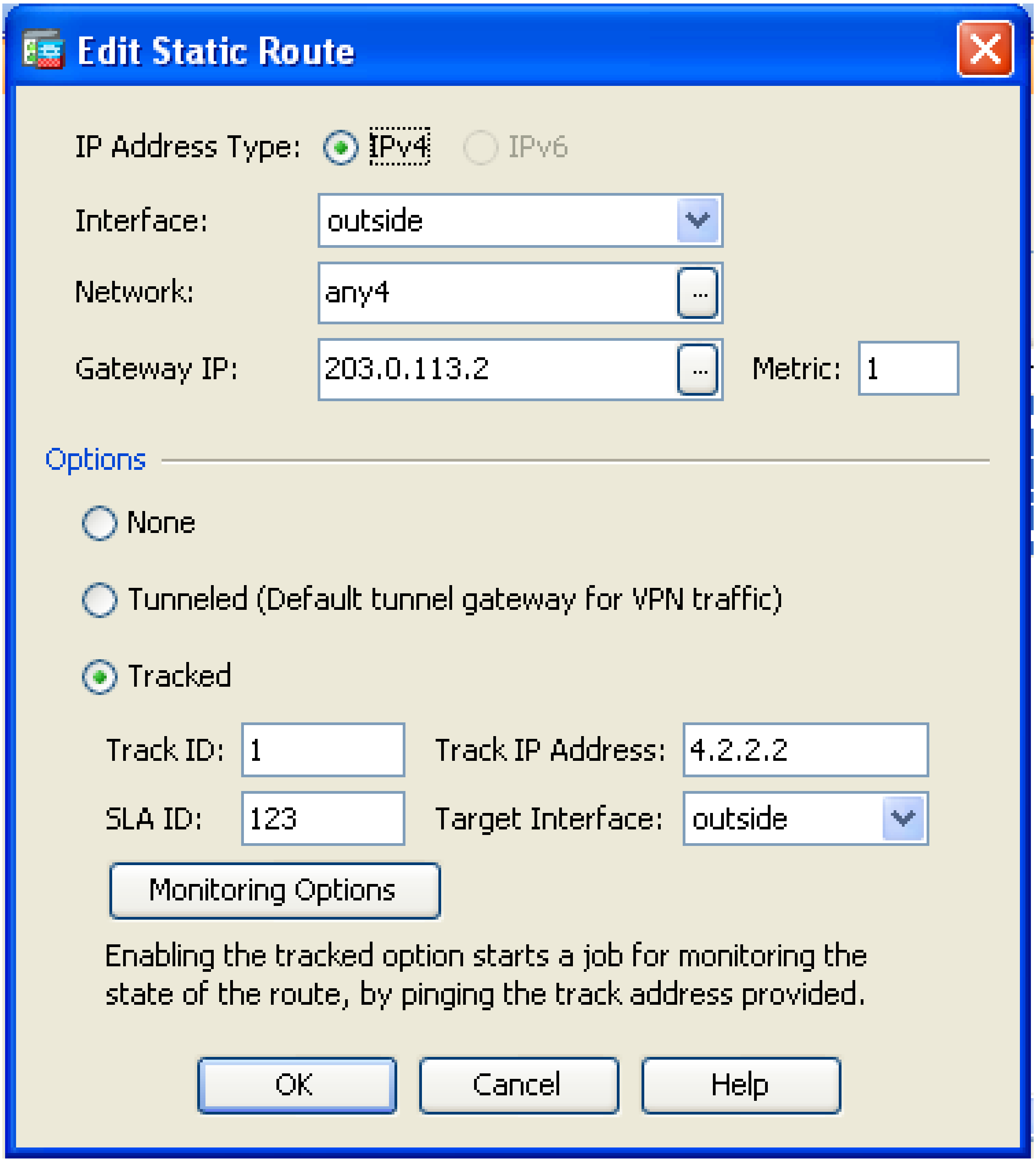


Specify static routes.

Filter: ● Both ○ IPv4 only ○ IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options

7. 单击 Add 添加新的静态路由。此对话框出现：


Edit Static Route

IP Address Type: ● IPv4 ○ IPv6

Interface: outside

Network: any4

Gateway IP: 203.0.113.2

Metric: 1

Options

○ None

○ Tunneled (Default tunnel gateway for VPN traffic)

● Tracked

Track ID: 1

Track IP Address: 4.2.2.2

SLA ID: 123

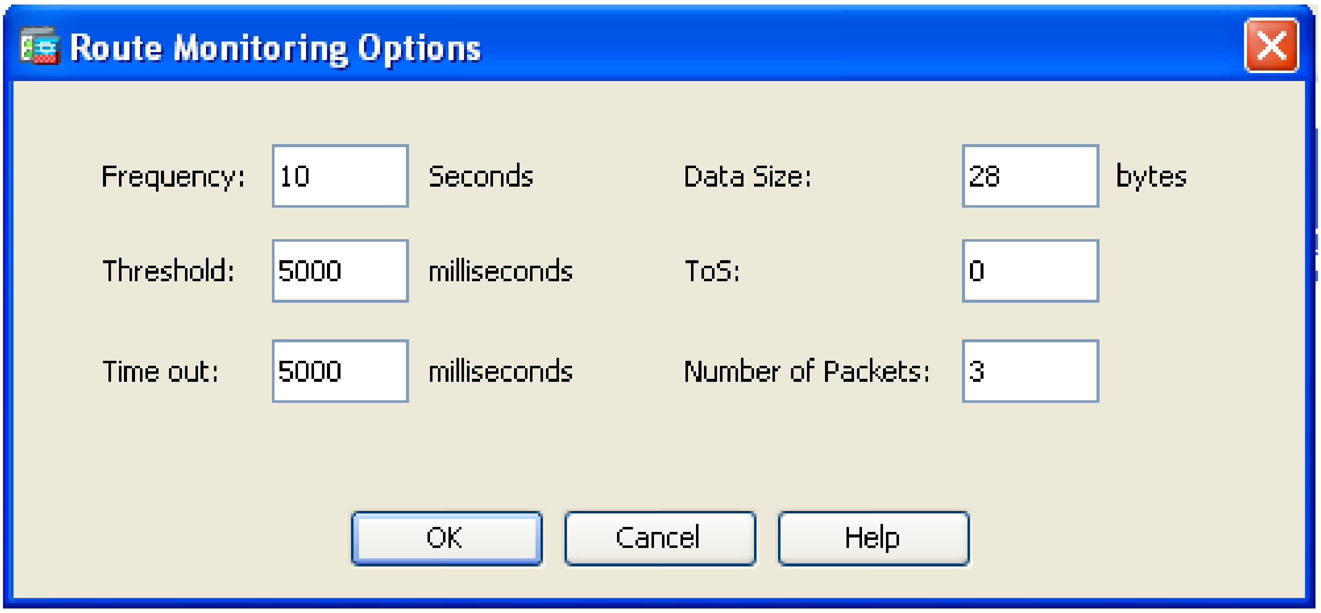
Target Interface: outside

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

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，4.2.2.2是使用ICMP回显进行监控的对象。

9. 在Options区域中，点击Tracked单选按钮，并在Track ID、SLA ID和Track IP Address字段中输入相应的值。

10. 单击 Monitoring Options。此对话框出现：



Frequency: 10 Seconds

Threshold: 5000 milliseconds

Time out: 5000 milliseconds

Data Size: 28 bytes

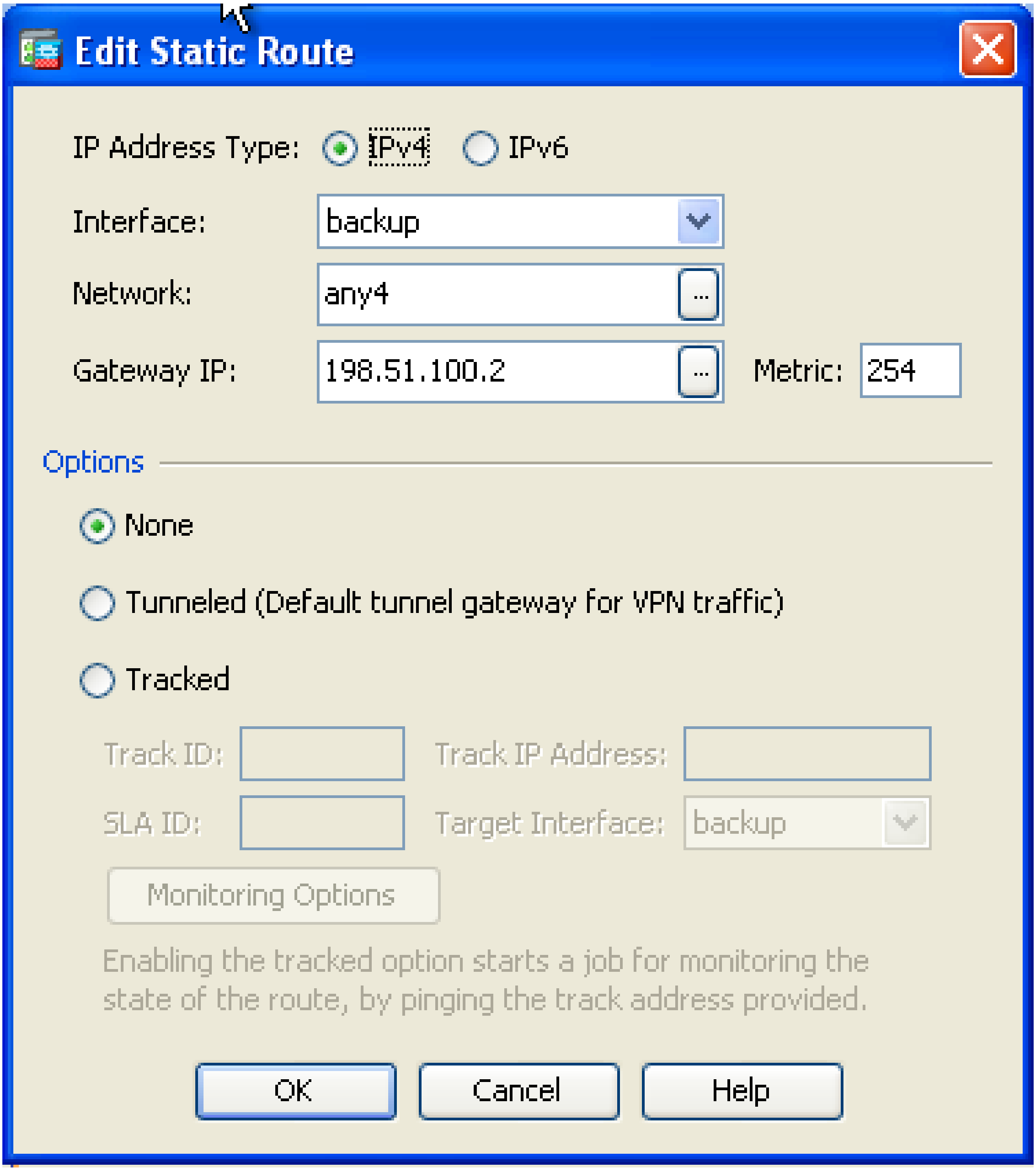
ToS: 0

Number of Packets: 3

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。要使其成为辅助路由，请用较高的度量（如 254）配置此路由。如果主路由（主 ISP）失败，则从路由表中删除该路由。此辅助路由（辅助ISP）安装在专用Internet Exchange(PIX)路由表中。

13. 单击OK以关闭对话框：



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:

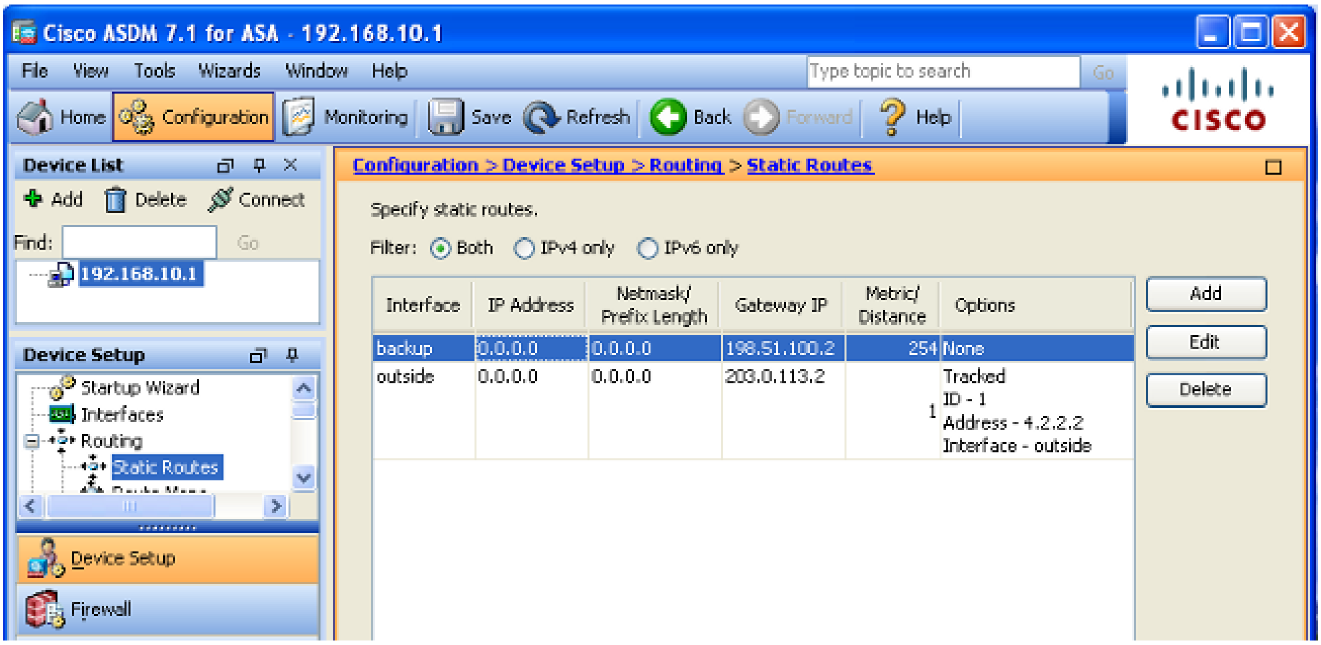
Track IP Address:

SLA ID:

Target Interface: backup

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

配置将显示在Interface列表中：



Configuration > Device Setup > Routing > Static Routes

Specify static routes.

Filter: ● Both ○ IPv4 only ○ IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
backup	0.0.0.0	0.0.0.0	198.51.100.2	254	None
outside	0.0.0.0	0.0.0.0	203.0.113.2	1	Tracked ID - 1 Address - 4.2.2.2 Interface - outside

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

注意:Output Interpreter Tool(仅注册客户)支持某些show命令。使用输出解释器工具来查看 show 命令输出的分析。

使用以下show命令验证配置是否完整：

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

```
<#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 — 此命令的输出显示操作的当前配置设置。

<#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 — 此命令的输出显示SLA操作的操作统计信息。
  - 在主 ISP 发生故障之前，正常运行的状态如下：

    <#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
```

- 在主ISP发生故障（且ICMP响应超时）后，这是运行状态：

```
<#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
```

确认备份路由已安装（CLI方法）

输入show route命令以确认备用路由已安装。

在主ISP发生故障之前，路由表如下所示：

```
<#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
```

在主ISP发生故障、删除静态路由并安装备用路由后，路由表将如下所示：

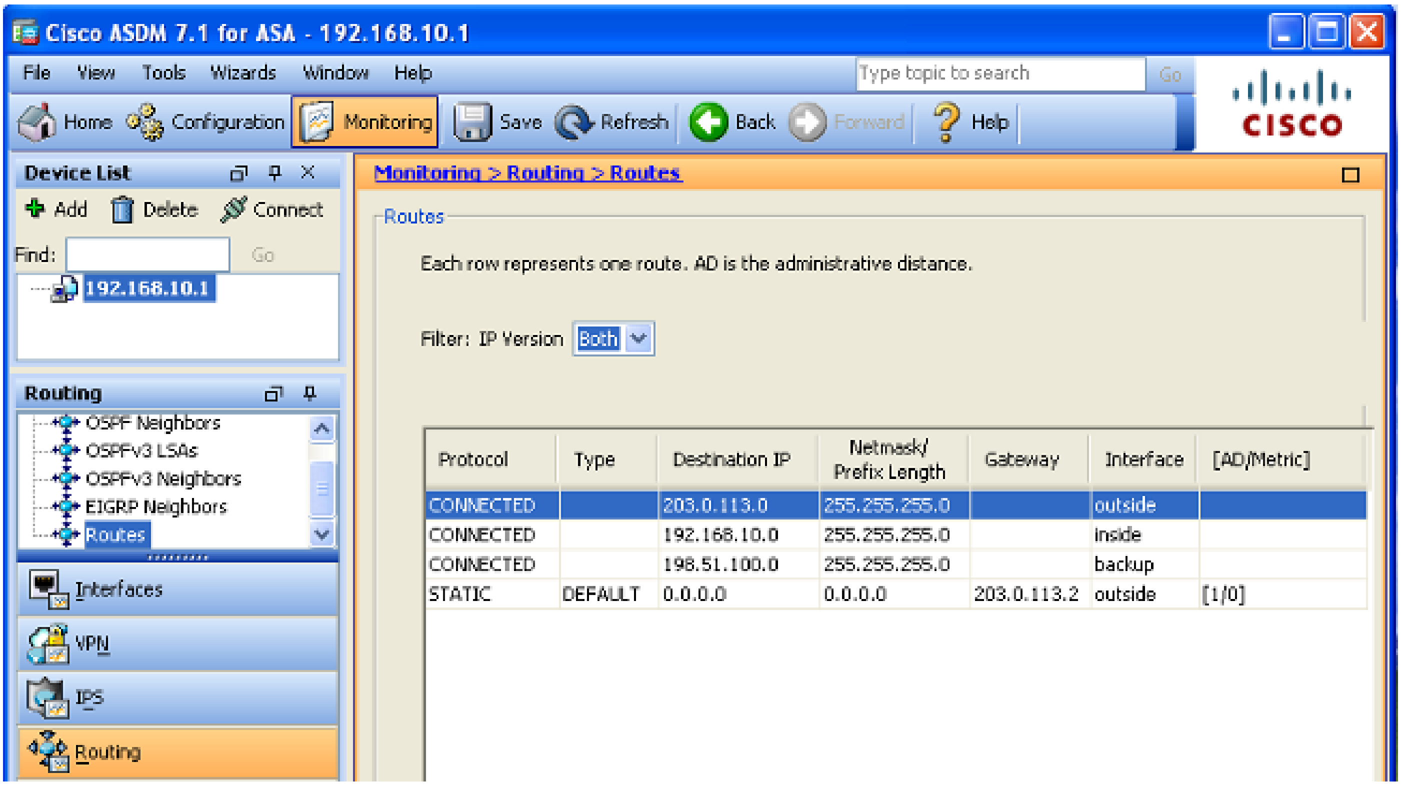
<#root>

```
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
```

确认备份路由已安装（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，路由表类似于下图所示。请注意，DEFAULT路由通过外部接口指向203.0.113.2:

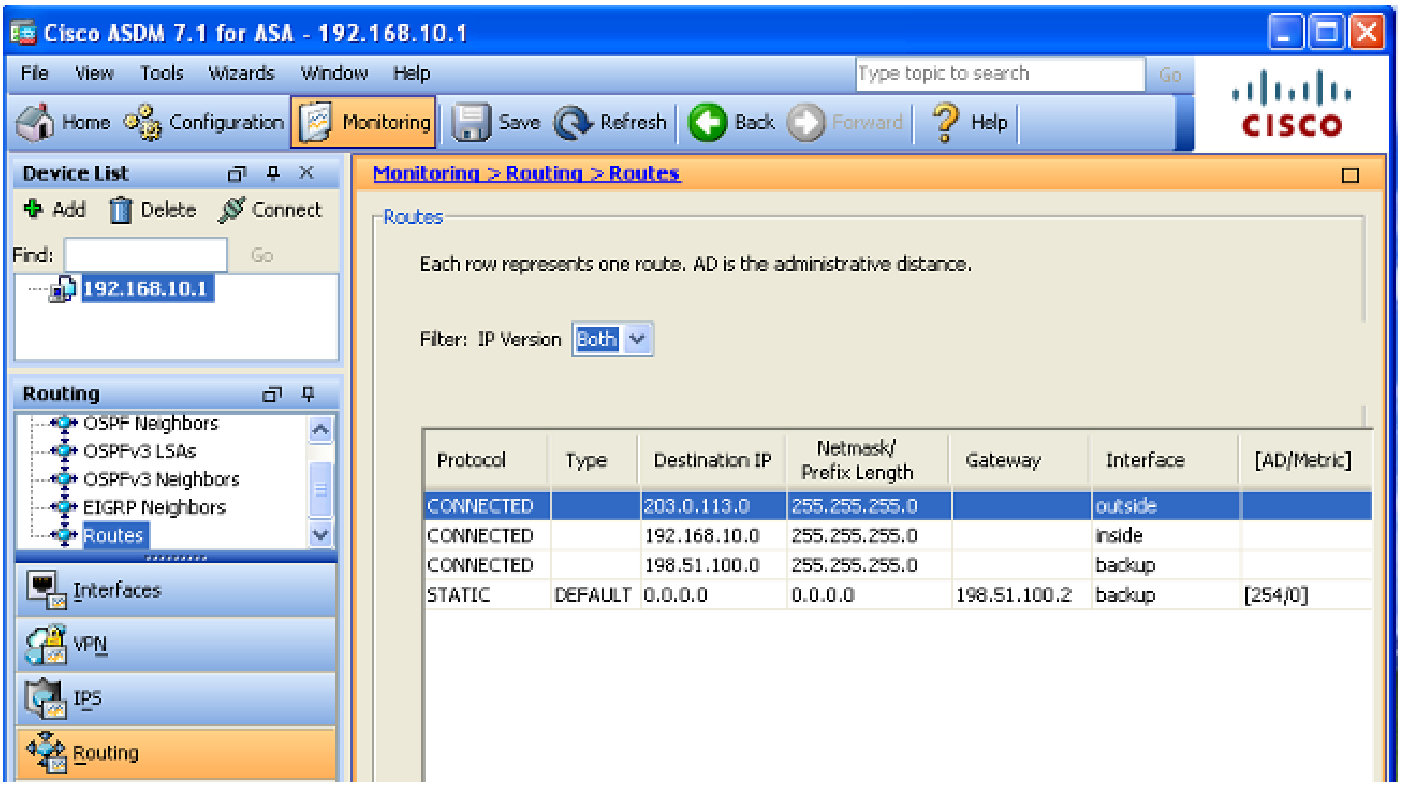


Each row represents one route. AD is the administrative distance.

Filter: IP Version Both

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]

在主ISP发生故障后，该路由将被删除，备用路由将被安装。DEFAULT路由现在通过备份接口指向198.51.100.2:



Each row represents one route. AD is the administrative distance.

Filter: IP Version Both

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	198.51.100.2	backup	[254/0]

故障排除

本节提供一些有用的调试命令，并介绍如何排除被不必要地删除所跟踪路由的问题。

调试命令

您可以使用以下debug命令排除配置问题：

- debug sla monitor trace — 此命令的输出显示回应操作的进度。
  - 如果跟踪的对象（主ISP网关）已启动并且ICMP回送成功，则输出类似于以下内容：

    ```
    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）已关闭，并且ICMP回显失败，则输出如下所示：

    ```
    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）已启用且ICMP成功，则输出如下所示：

    ```
    %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
    ```

- 如果跟踪的对象（主ISP网关）已关闭并且已删除跟踪的路由，则输出将类似如下所示：

  <#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.
  ```

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。

如果您选择比ISP网关更远的监控目标，该路由上的另一条链路可能会发生故障，或者其它设备可能会干扰。

因此，此配置可能导致SLA监控器断定与主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，即使主ISP链路仍处于活动状态，主跟踪路由也会被删除。

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回应失败，ISP链路几乎肯定已断开。

相关信息

- Cisco ASA 5500-X系列下一代防火墙
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。