配置ASA的冗餘或備用ISP鏈路

目錄

簡介

本文檔介紹如何配置Cisco ASA 5500系列靜態路由跟蹤功能以使用冗餘或備份網際網路連線。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本9.x或更高版本的Cisco ASA 5555-X系列
- Cisco ASDM版本7.x或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

相關產品

您也可以將此配置與Cisco ASA 5500系列版本9.1(5)配合使用。

註：在ASA 5505系列上配置第四個介面時需要backup interface命令。有關詳細資訊，請參閱思科安全裝置命令參考7.2版中的備份介面部分。

背景資訊

本節概述本文檔中介紹的靜態路由跟蹤功能，以及開始之前提出的一些重要建議。

靜態路由跟蹤功能概述

使用靜態路由的一個問題是，不存在可確定路由是啟動還是關閉的內在機制。

即使下一跳網關不可用，該路由仍保留在路由表中。

僅當安全裝置上的關聯介面關閉時，才會從路由表中刪除靜態路由。

為了解決此問題，靜態路由跟蹤功能用於跟蹤靜態路由的可用性。

此功能從路由表中刪除靜態路由，並在發生故障時用備用路由替換靜態路由。

靜態路由跟蹤允許ASA在主租用線路不可用時使用到輔助ISP的廉價連線。

為了實現此冗餘，ASA將靜態路由與您定義的監控目標關聯。

服務等級協定(SLA)操作使用定期ICMP回應請求監控目標。

如果沒有收到回應應答，則會將該對象視為關閉，並從路由表中刪除關聯的路由。

使用先前配置的備份路由來代替已移除的路由。

使用備份路由時，SLA監控操作將繼續嘗試訪問監控目標。

目標再次可用後，第一個路由將替換在路由表中，備份路由將被刪除。

在本文檔中使用的示例中，ASA維護與Internet的兩個連線。

第一個連線是通過主ISP提供的路由器訪問的高速租用線路。

第二個連線是通過輔助ISP提供的DSL數據機訪問的低速數字使用者線路(DSL)。

註：本文檔中描述的配置不能用於負載平衡或負載共用，因為ASA不支援此配置。此配置僅用於冗餘或備份目的。出站流量使用主ISP，如果主ISP發生故障，則使用輔助ISP。主ISP故障

會導致流量暫時中斷。

只要租用線路處於活動狀態且主要ISP網關可訪問，DSL連線即處於空閒狀態。

但是，如果與主ISP的連線中斷，ASA將更改路由表以將流量定向到DSL連線。

使用靜態路由跟蹤來實現此冗餘。

ASA配置了靜態路由，該路由將所有Internet流量定向到主ISP。

SLA監控進程每10秒檢查一次，以確認主ISP網關可訪問。

如果SLA監控過程確定無法到達主ISP網關，則從路由表中刪除將流量定向到該介面的靜態路由。

為了替換該靜態路由，安裝了將流量定向到輔助ISP的備用靜態路由。

此備用靜態路由通過DSL數據機將流量定向到輔助ISP，直到通向主要ISP的鏈路可訪問。

此配置提供了一種相對便宜的方法，可確保出站Internet訪問仍然對ASA後面的使用者可用。

如本文檔所述，此設定並非始終適用於對ASA後資源的入站訪問。需要具備高級網路技能才能實現無縫入站連線。

本檔案沒有說明這些技能。

重要建議

在嘗試本文檔中所述的配置之前，您必須選擇可以響應網際網路控制消息協定(ICMP)回應請求的監控目標。

目標可以是您選擇的任何網路對象，但推薦的目標與您的Internet服務提供商(ISP)連線密切相關。

以下是一些可能的監控目標：

- ISP網關地址
- 另一個ISP管理的地址
- ASA必須與之通訊的另一網路上的伺服器，如身份驗證、授權和記帳(AAA)伺服器
- 另一個網路上的永續性網路對象（夜間可以關閉的台式機或筆記型電腦不是很好的選擇）

本文檔假定ASA已完全正常運行並經過配置，以允許思科自適應安全裝置管理器(ASDM)進行配置更改。

提示：有關如何允許ASDM配置裝置的資訊，請參閱CLI手冊1: Cisco ASA系列常規操作CLI配置指南9.1中的為ASDM配置HTTPS訪問部分。

設定

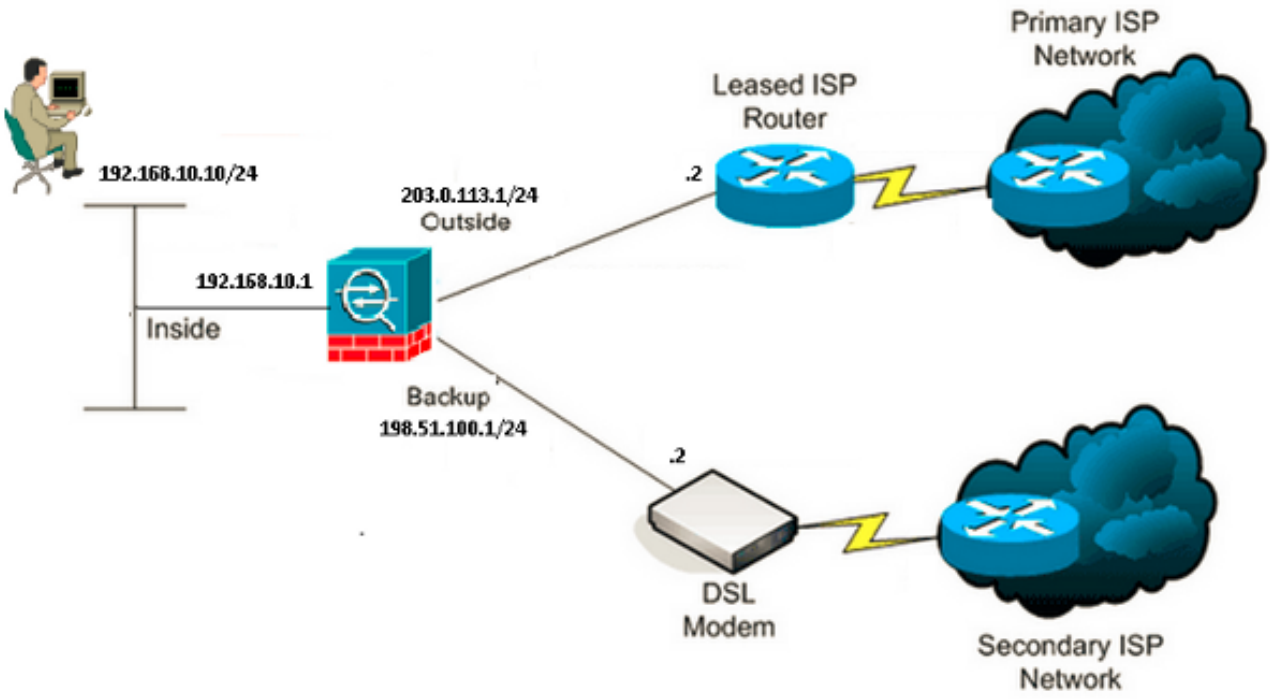
使用本節中介紹的資訊配置ASA以使用靜態路由跟蹤功能。

註：使用命令查詢工具(僅限註冊客戶)可獲取有關本節中使用的命令的更多資訊。

註：此配置中使用的IP地址在Internet上不能合法路由。它們是RFC 1918地址，在實驗室環境中使用。

網路圖表

本節提供的範例使用以下網路設定：



CLI組態

使用以下資訊通過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
```

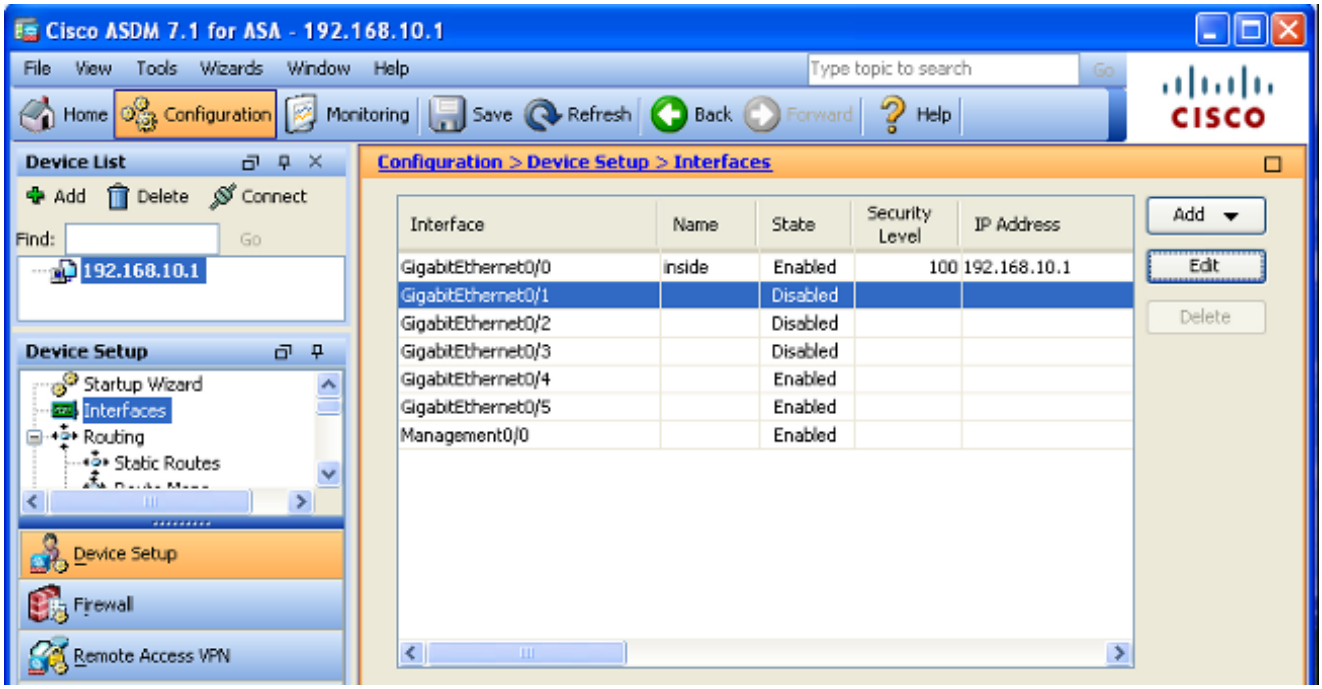
```
!--- monitoring protocol and the target network object whose availability the tracking
!--- process monitors.  Specify the number of packets to be sent with each poll.
!--- Specify the rate at which the monitor process repeats (in seconds).



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
```

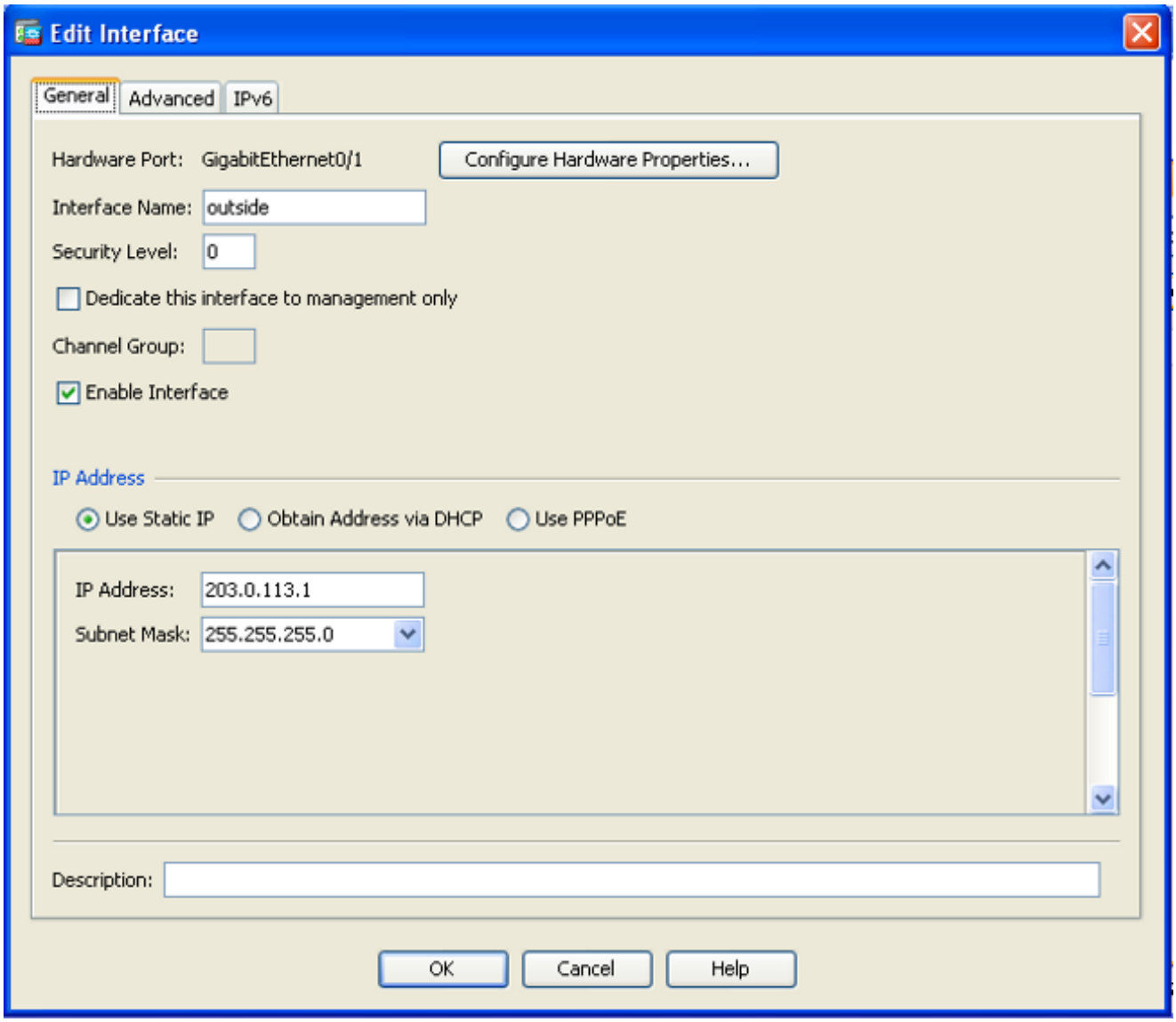
ASDM配置

完成以下步驟，以便使用ASDM應用程式配置冗餘或備份ISP支援：

1. 在ASDM應用程式中，按一下Configuration，然後按一下Interfaces。



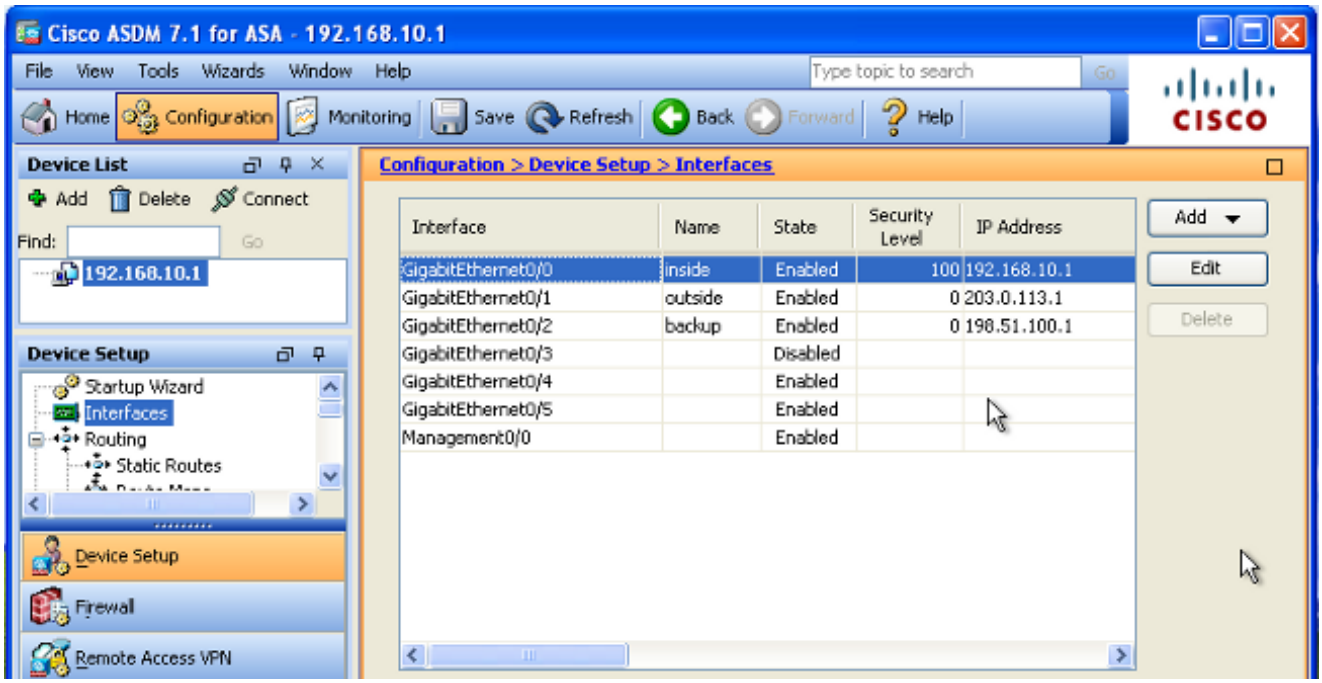
2. 從Interfaces清單中選擇GigabitEthernet0/1，然後按一下Edit。 出現此對話方塊：



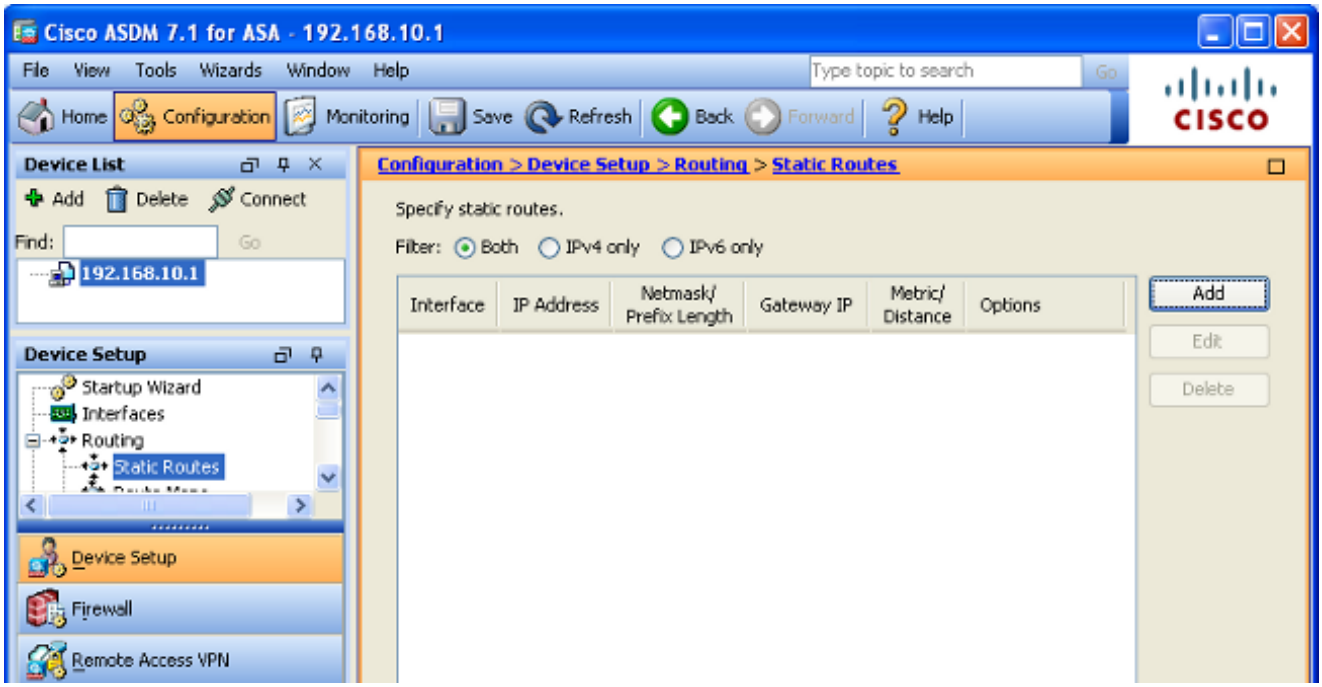
3. 選中Enable Interface復選框，並在Interface Name、Security Level、IP Address和Subnet Mask欄位中輸入相應的值。

4. 按一下「OK」以關閉對話方塊。

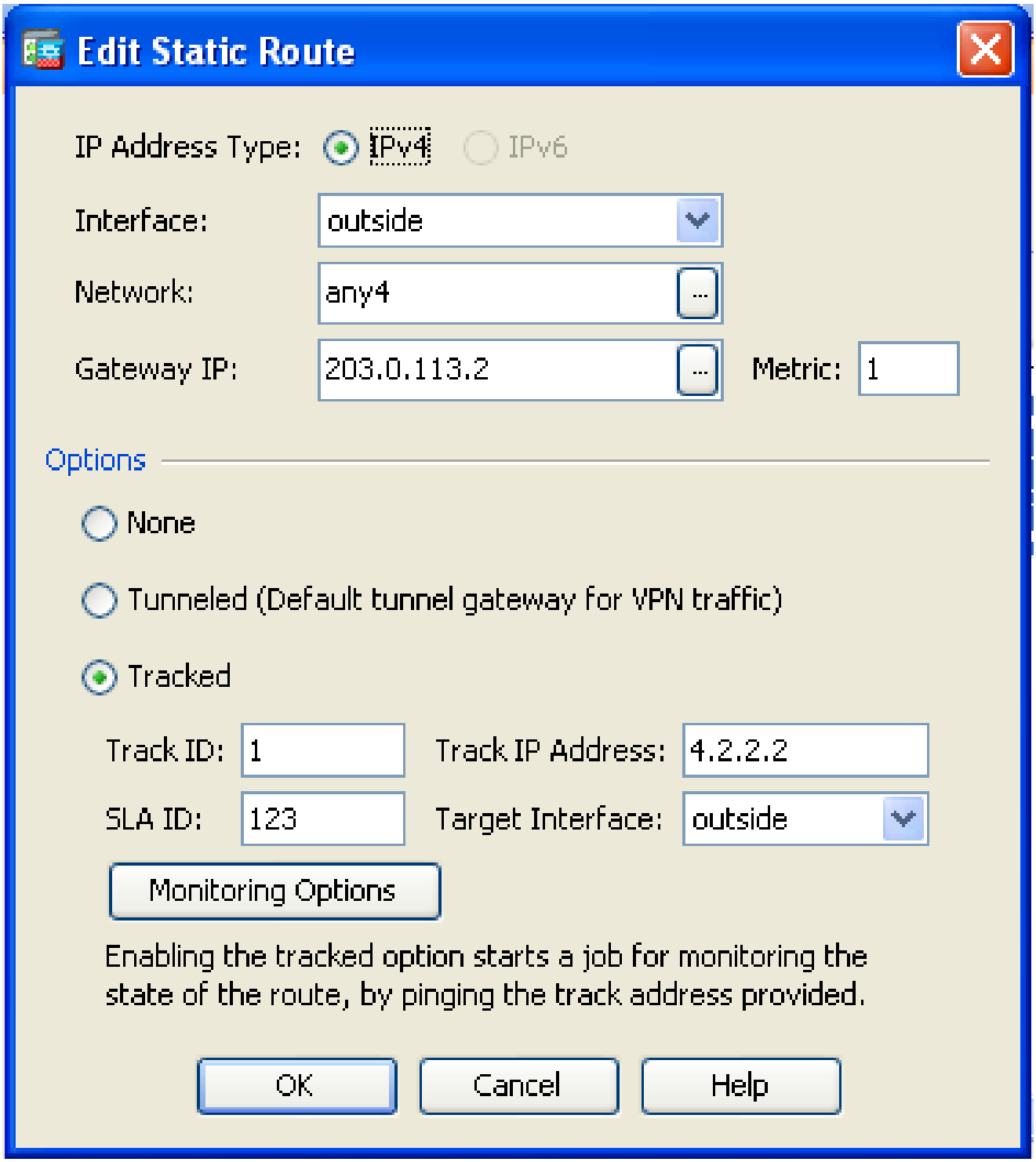
5. 根據需要配置其他介面，然後按一下Apply以更新ASA配置：



6. 選擇Routing，然後點選位於ASDM應用程式左側的Static Routes:



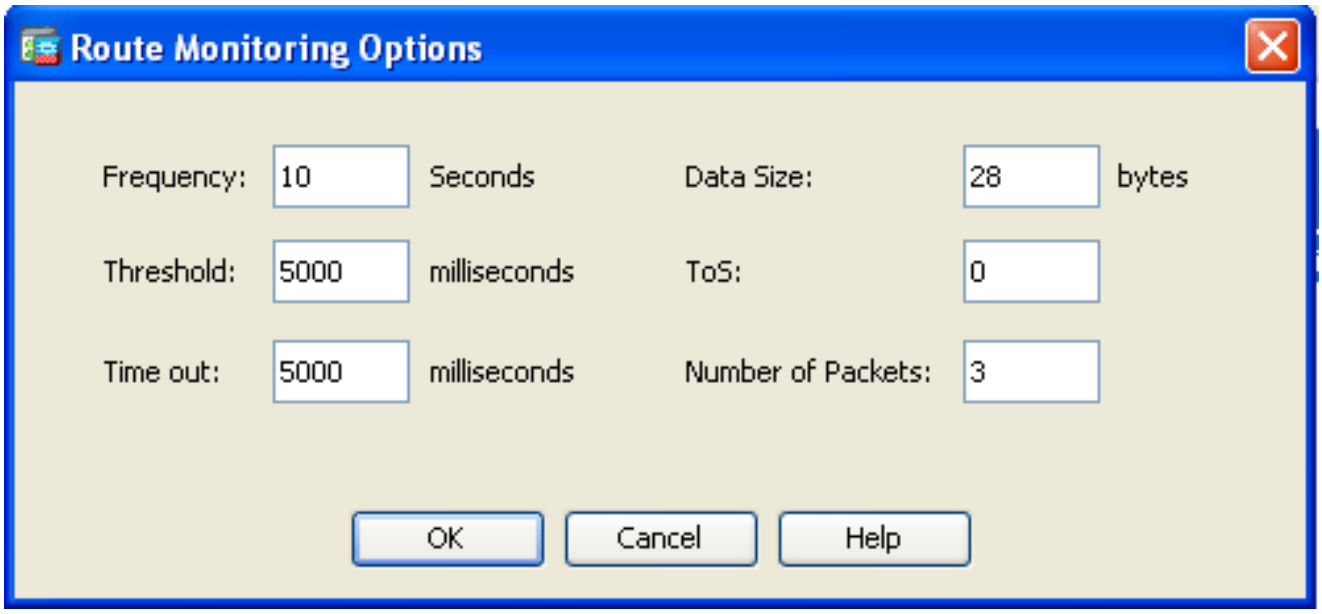
7. 按一下Add以新增新的靜態路由。出現此對話方塊：



8. 從Interface Name下拉選單中，選擇路由所在的介面，並配置到達網關的預設路由。在本例中，203.0.113.2是主ISP網關，4.2.2.2是使用ICMP回應監控的對象。

9. 在「選項」區域中，按一下Tracked單選按鈕，然後在Track ID、SLA ID和Track IP Address欄位中輸入相應的值。

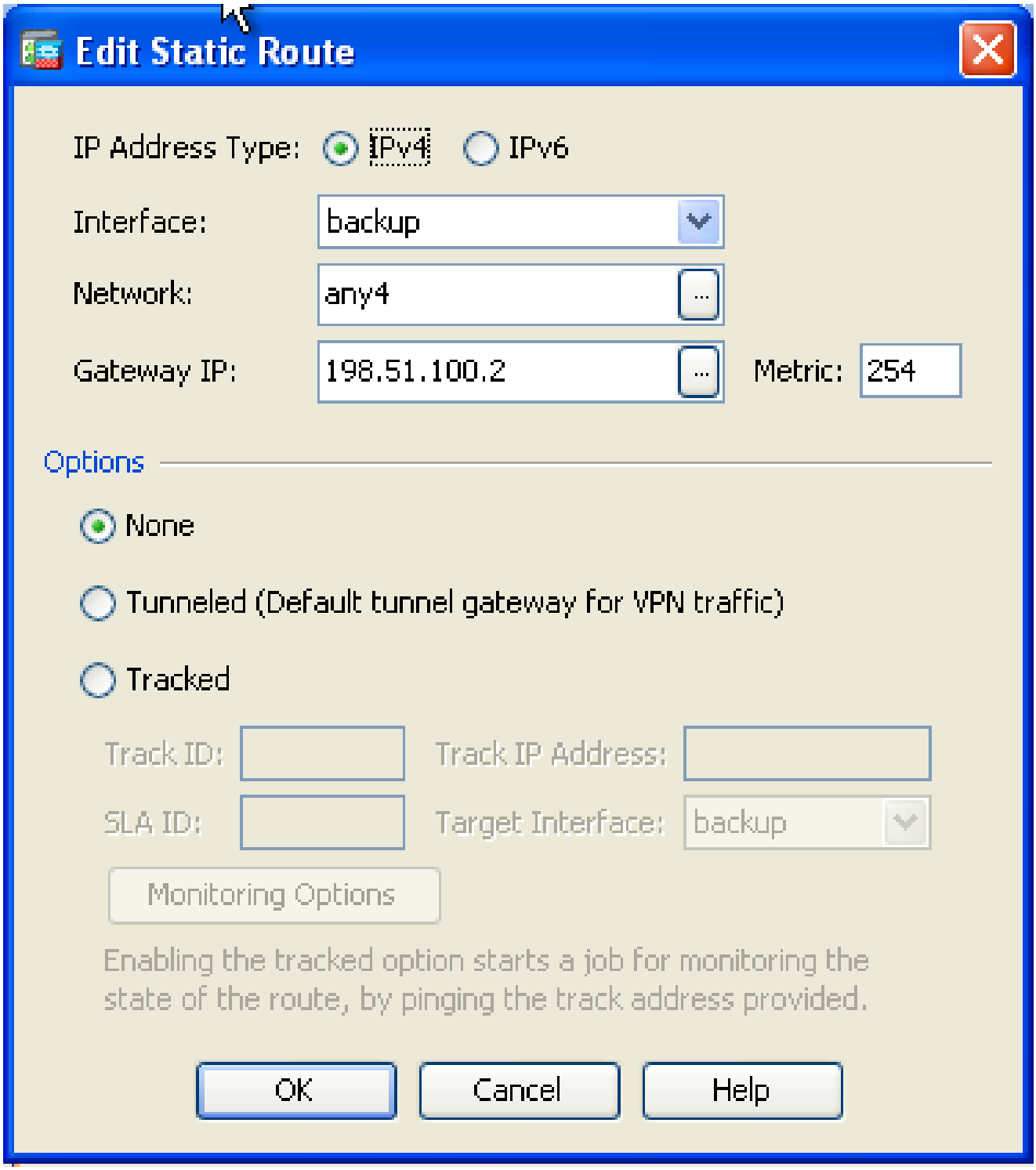
10. 按一下Monitoring Options。出現此對話方塊：



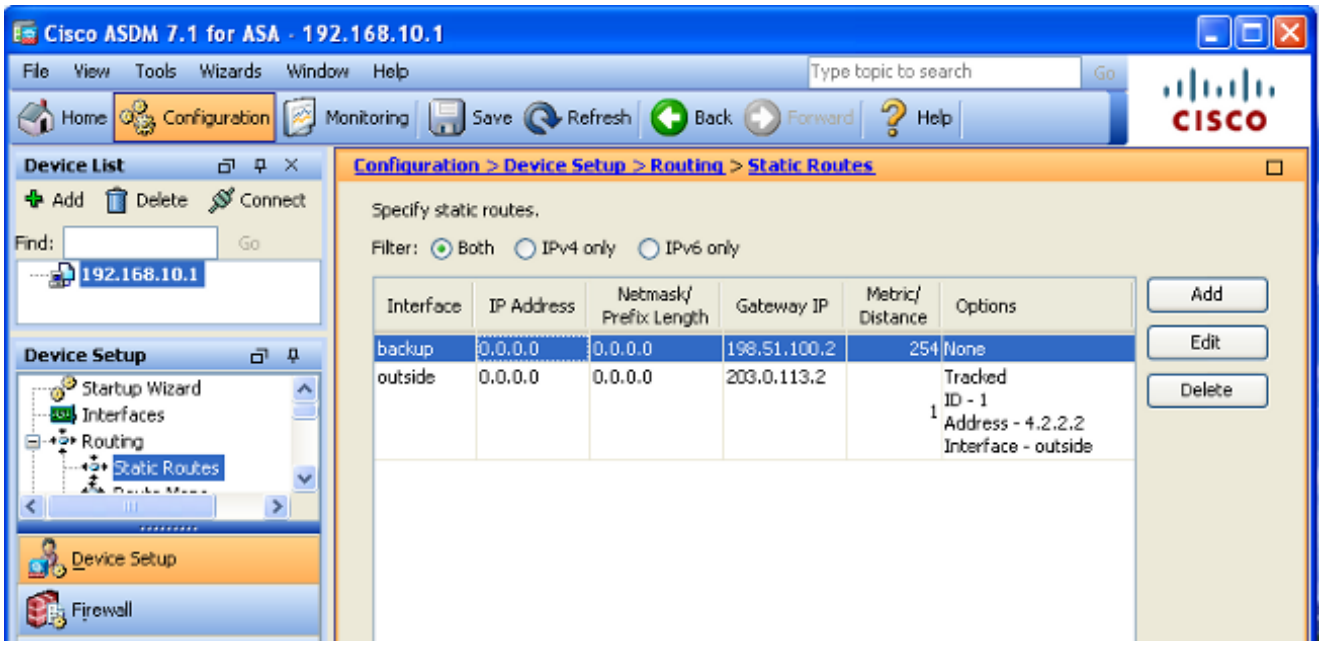
11. 為頻率和其他監視選項輸入適當的值，然後按一下確定。

12. 為輔助ISP新增另一條靜態路由，以便提供到達Internet的路由。為了使其成為輔助路由，請用更高的度量配置此路由，例如254。如果主路由（主ISP）發生故障，該路由將從路由表中刪除。此輔助路由（輔助ISP）安裝在專用Internet Exchange(PIX)路由表中。

13. 按一下「OK」以關閉對話方塊：



配置將顯示在Interface清單中：



14. 選擇路由配置，然後按一下Apply以更新ASA配置。

驗證

使用本節內容，確認您的組態是否正常運作。

確認配置已完成

註:Output Interpreter Tool(僅供已註冊客戶)支援某些show命令。使用Output Interpreter工具檢視show指令輸出的分析。

使用以下show命令驗證您的組態是否完成：

- show running-config sla monitor — 此命令的輸出顯示配置中的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 — 此命令的輸出顯示操作的當前配置設定。

<#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: 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 — 此命令的輸出顯示SLA操作的操作統計資訊。
  - 在主ISP發生故障之前，這是運行狀態：

<#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
```

- 主ISP發生故障（且ICMP回應逾時）後，這是工作狀態：

```
<#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
```

確認備份路由已安裝（CLI方法）

輸入show route命令以確認是否已安裝備份路由。

在主ISP發生故障之前，路由表顯示如下：

```
<#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
```

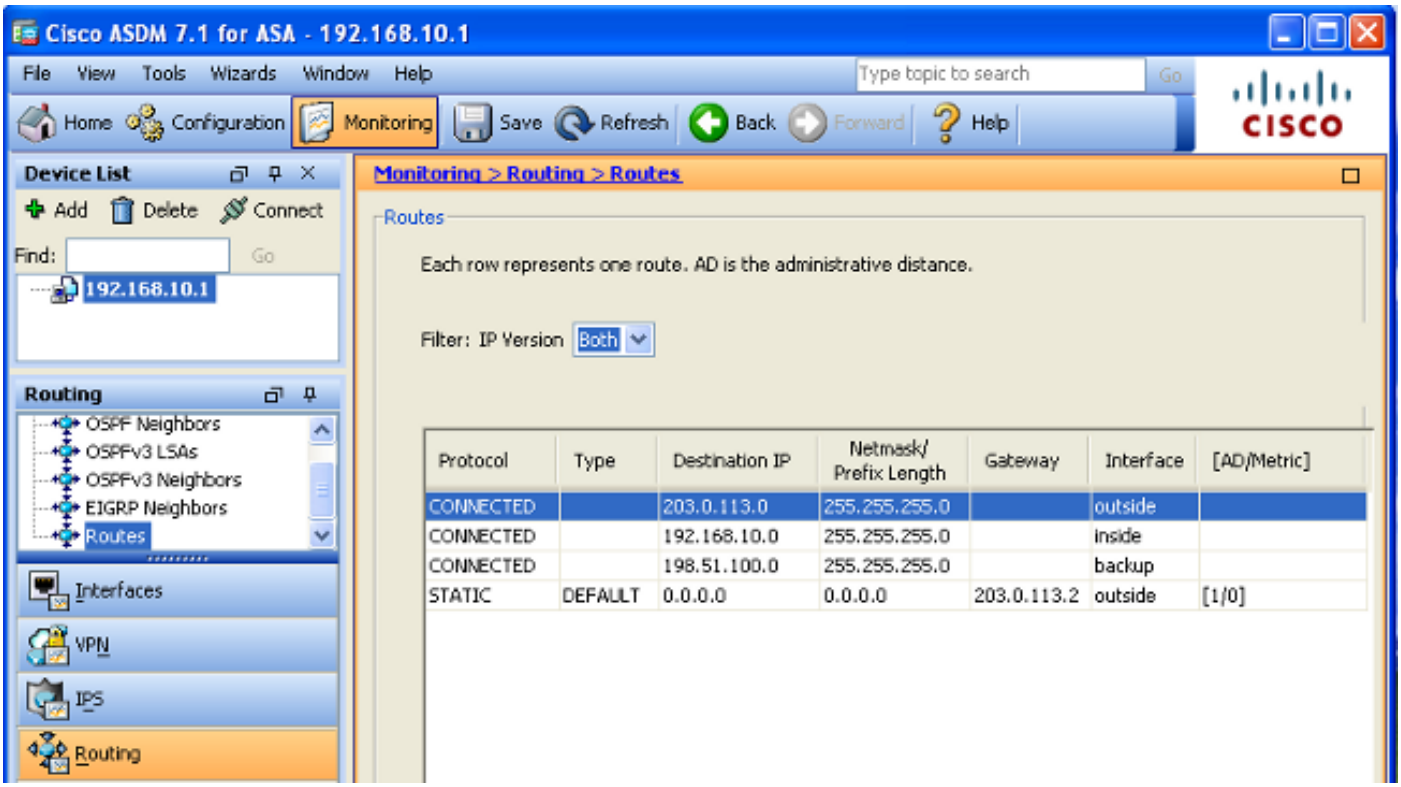
在主ISP發生故障、靜態路由被刪除並安裝了備份路由後，路由表顯示如下：

```
<#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
```

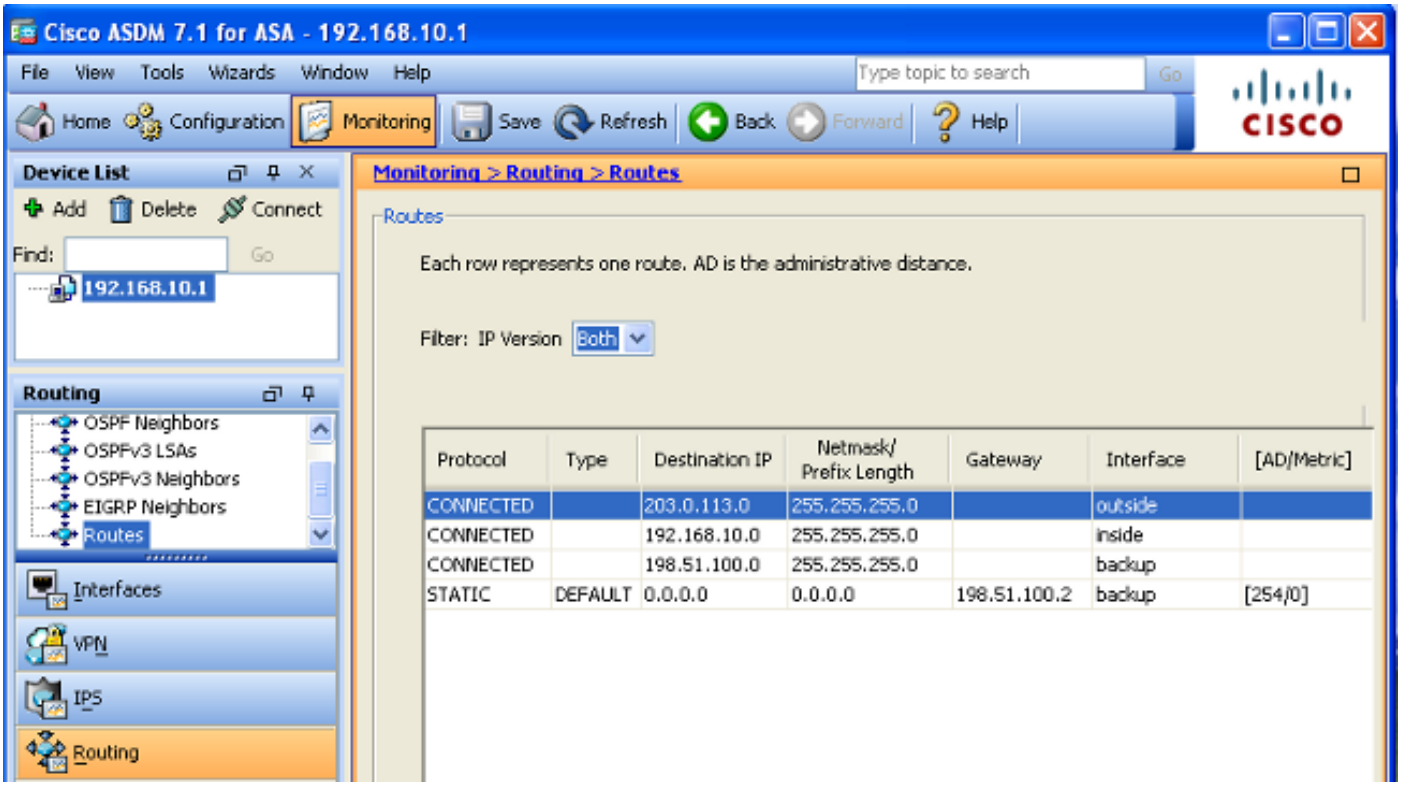
確認已安裝備份路由（ASDM方法）

要確認備份路由是通過ASDM安裝的，請導航到Monitoring > Routing，然後從Routing樹中選擇Routes。

在主ISP發生故障之前，路由表與下一圖中顯示的路由表類似。請注意，DEFAULT路由通過outside介面指向203.0.113.2:



在主ISP發生故障後，會刪除該路由並安裝備用路由。DEFAULT路由現在通過backup介面指向198.51.100.2:



疑難排解

本節提供一些有用的debug命令，並描述如何排除不必要地刪除跟蹤的路由的問題。

Debug指令

您可以使用以下debug指令對組態問題進行疑難排解：

- debug sla monitor trace — 此命令的輸出顯示回應要求操作的進度。
    - 如果跟蹤的對象（主ISP網關）已啟動，並且ICMP回顯成功，則輸出會顯示類似以下內容：

```
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
```

    - 如果跟蹤的對象（主ISP網關）已關閉，並且ICMP回顯失敗，則輸出會顯示類似以下內容：

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: 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 — 此命令的輸出顯示SLA監控進程遇到的任何錯誤。
    - 如果跟蹤的對象（主ISP網關）為up狀態且ICMP成功，則輸出如下所示：

```
%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
```

- 如果跟蹤的對象（主ISP網關）關閉並且刪除了跟蹤的路由，則輸出會顯示類似以下內容：

<#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.
```

不必要地刪除了跟蹤的路由

如果被跟蹤的路由被不必要地刪除，請確保監控目標始終可用於接收回應請求。

此外，請確保監控目標的狀態（即目標是否可訪問）與主ISP連線的狀態密切相關。

如果您選擇的監控目標比ISP網關更遠，則沿該路由的另一條鏈路可能會發生故障，或者其它裝置可能會干擾。

因此，此配置可能導致SLA監控器推斷主ISP的連線失敗，並導致ASA不必要地故障切換到輔助ISP鏈路。

例如，如果您選擇分支機構路由器作為監控目標，到分支機構的ISP連線以及此過程中的任何其他鏈路都可能失敗。

監控操作傳送的ICMP回顯失敗後，即使主ISP鏈路仍處於活動狀態，主跟蹤路由也會被刪除。

在本示例中，用作監控目標的主ISP網關由ISP管理，位於ISP鏈路的另一端。

此配置可確保如果監控操作傳送的ICMP回聲失敗，ISP鏈路幾乎肯定會關閉。

相關資訊

- Cisco ASA 5500-X系列下一代防火牆
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。