

採用OSPF的ASA/PIX配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[組態](#)

[ASDM配置](#)

[配置OSPF身份驗證](#)

[Cisco ASA CLI配置](#)

[Cisco IOS路由器\(R2\)CLI配置](#)

[Cisco IOS路由器\(R1\)CLI配置](#)

[Cisco IOS路由器\(R3\)CLI配置](#)

[使用ASA重新分發到OSPF](#)

[驗證](#)

[疑難排解](#)

[點對點網路的靜態鄰居配置](#)

[疑難排解指令](#)

[相關資訊](#)

簡介

本文檔介紹如何配置Cisco ASA以通過開放最短路徑優先(OSPF)學習路由、執行身份驗證和重新分發。

請參閱[PIX/ASA 8.X:有關EIGRP配置的詳細資訊](#)，請在思科自適應安全裝置(ASA)上配置EIGRP。

注意：ASA/PIX不支援非對稱路由。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- Cisco ASA/PIX必須運行7.x版或更高版本。
- 多情景模式不支援OSPF;它僅在單一模式下受支援。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行軟體版本8.0和更新版本的Cisco 5500系列調適型安全裝置(ASA)
- 思科自適應安全裝置管理器(ASDM)軟體版本6.0及更高版本

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

本文檔中的資訊也適用於運行軟體版本8.0及更高版本的Cisco 500系列PIX防火牆。

慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

背景資訊

OSPF使用鏈路狀態演算法來構建和計算到達所有已知目標的最短路徑。OSPF區域中的每台路由器都包含相同的鏈路狀態資料庫，該資料庫是每台路由器可用介面和可到達鄰居的清單。

OSPF比RIP的優點包括：

- 與RIP更新相比，OSPF鏈路狀態資料庫更新的傳送頻率較低，並且鏈路狀態資料庫會立即更新，而不是隨著過時資訊的超時而逐漸更新。
- 路由決策基於開銷，這是通過特定介面傳送資料包所需的開銷指示。安全裝置根據鏈路頻寬而不是到達目的地的跳數來計算介面的成本。可以配置開銷以指定首選路徑。

最短路徑優先演算法的缺點是需要大量的CPU週期和記憶體。

安全裝置可以在不同的介面集上同時運行兩個OSPF協定進程。如果您有使用相同IP地址的介面（NAT允許這些介面共存，但OSPF不允許重疊地址），則可能需要運行兩個進程。或者，您可能希望在內部運行一個進程，在外部運行另一個進程，並在兩個進程之間重新分配路由的子集。同樣，您可能需要將私有地址與公有地址分開。

您可以從另一個OSPF路由進程、RIP路由進程或在啟用OSPF的介面上配置的靜態路由和連線路由將路由重分發到OSPF路由進程中。

安全裝置支援以下OSPF功能：

- 支援區域內路由、區域間路由和外部（I類和II類）路由。
- 支援虛擬鏈路。
- OSPF LSA泛洪。
- OSPF資料包的身份驗證（口令和MD5身份驗證）。
- 支援將安全裝置配置為指定路由器或指定備份路由器。還可以將安全裝置設定為ABR。但是

- ，將安全裝置配置為ASBR的功能僅限於預設資訊（例如，注入預設路由）。
- 支援末節區域和非末節區域。
- 區域邊界路由器第3類LSA過濾。

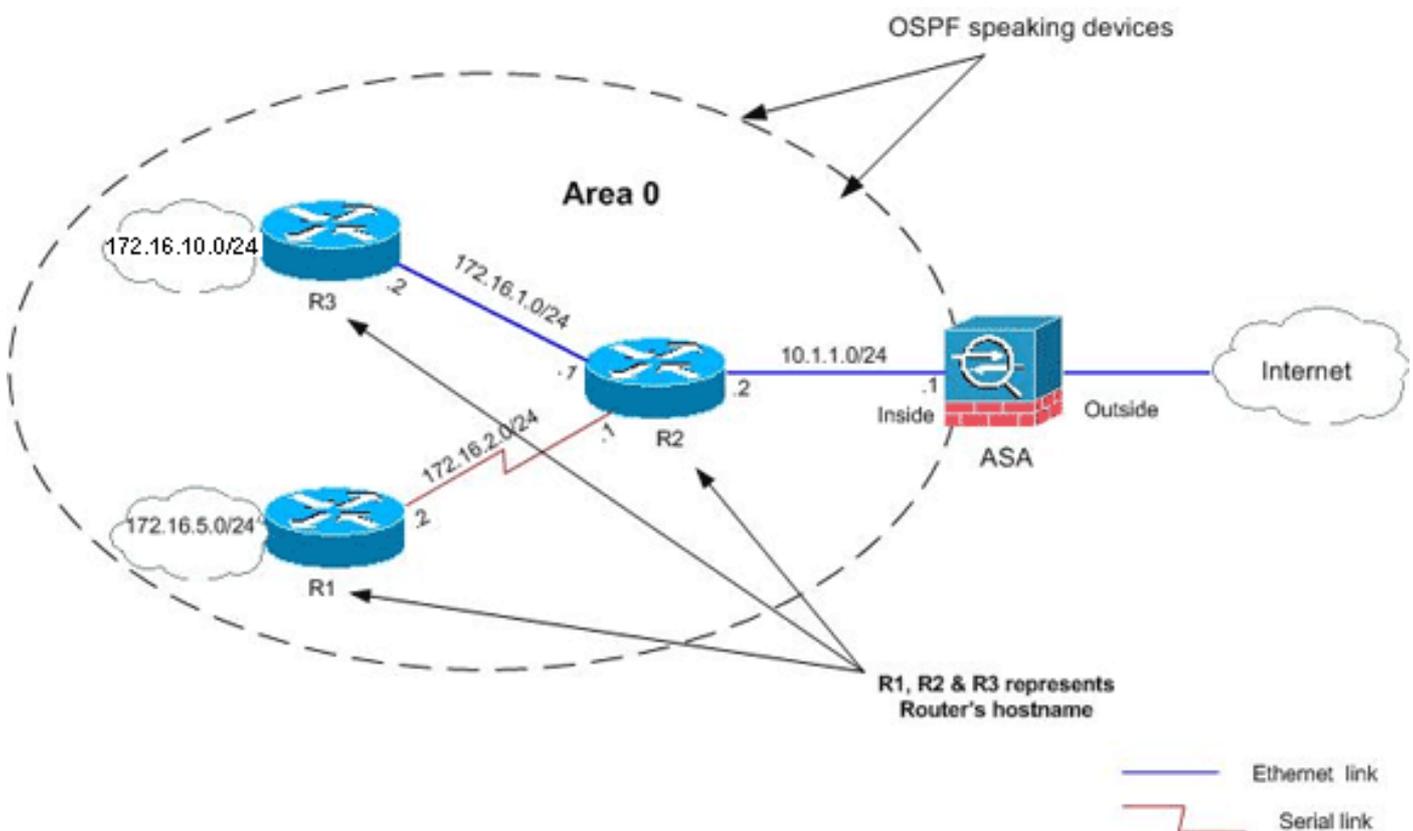
設定

本節提供用於設定本文中所述功能的資訊。

註：使用[Command Lookup Tool](#)(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



在此網路拓撲中，Cisco ASA內部介面IP地址為10.1.1.1/24。目標是在Cisco ASA上配置OSPF，以便通過相鄰路由器(R2)動態學習到內部網路(172.16.1.0/24、172.16.2.0/24、172.16.5.0/24和172.16.10.0/24)的路由。R2通過另外兩台路由器 (R1和R3) 獲知到遠端內部網路的路由。

組態

本檔案會使用以下設定：

- [ASDM配置](#)
- [配置OSPF身份驗證](#)
- [Cisco ASA CLI配置](#)
- [Cisco IOS路由器\(R2\)CLI配置](#)
- [Cisco IOS路由器\(R1\)CLI配置](#)
- [Cisco IOS路由器\(R3\)CLI配置](#)

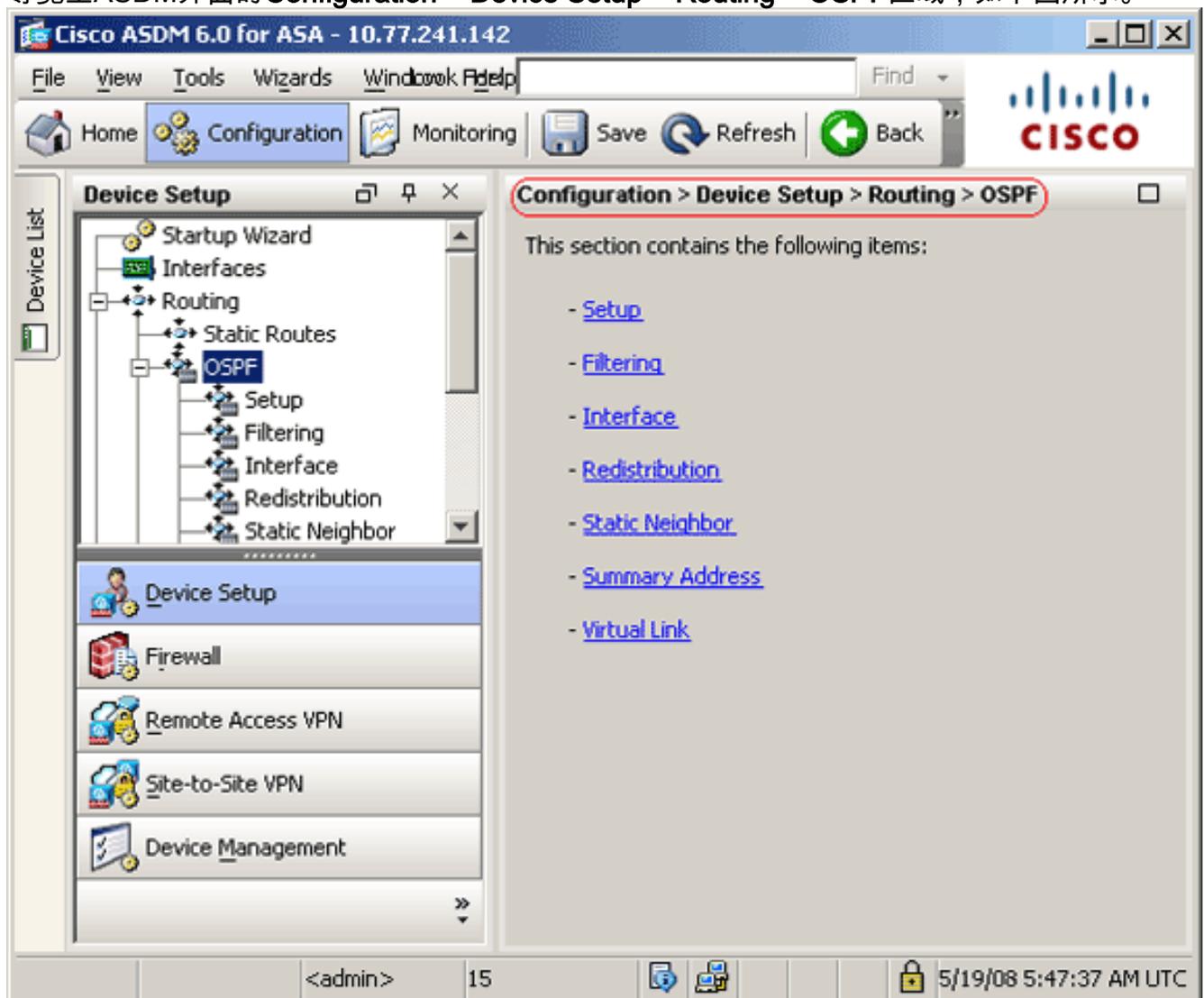
- [使用ASA重新分發到OSPF](#)

ASDM配置

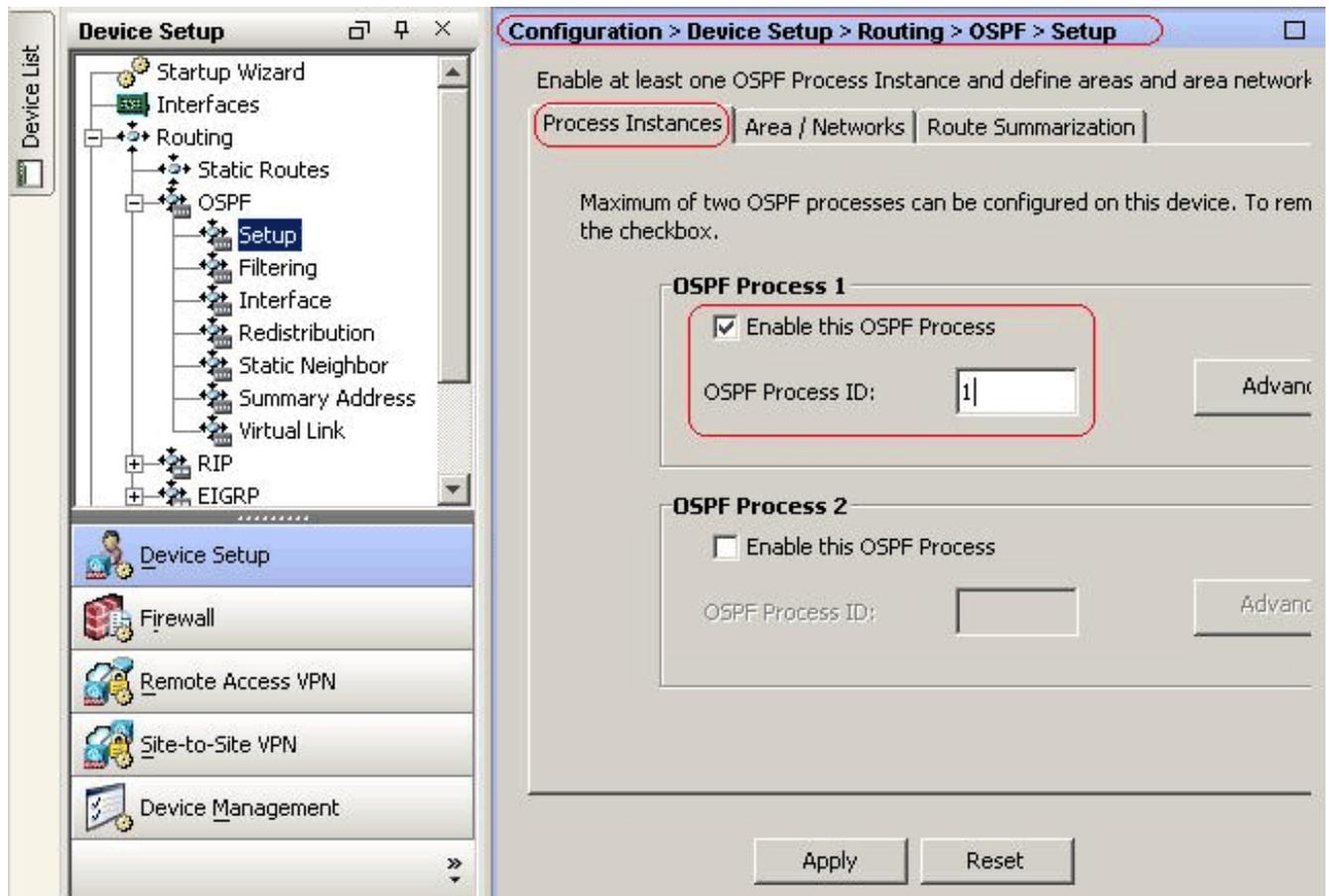
自適應安全裝置管理器(ASDM)是一種基於瀏覽器的應用程式，用於配置和監控安全裝置上的軟體。ASDM從安全裝置載入，然後用於配置、監控和管理裝置。您還可以使用ASDM Launcher (僅限 Windows) 以比Java小程式更快的速度啟動ASDM應用程式。本節介紹使用ASDM配置本文檔中所述功能所需的資訊。

完成以下步驟，以便在Cisco ASA中配置OSPF:

1. 使用ASDM登入到Cisco ASA。
2. 導覽至ASDM介面的**Configuration > Device Setup > Routing > OSPF**區域，如下圖所示。



3. 在**Setup > Process Instances**頁籤上啟用OSPF路由進程，如下圖所示。在本示例中，OSPF ID進程為1。



4. 您可以在**Setup > Process Instances**頁籤上按一下**Advanced**，以配置可選的高級OSPF路由進程引數。您可以編輯特定於進程的設定，例如Router ID、Adjacency Changes、Administrative Route Distances、Timers和Default Information Originate設定。

Edit OSPF Process Advanced Properties

OSPF Process: Router ID:

Ignore LSA MOSPF (suppress the sending of syslog messages when router receives a LSA MOSPF packets) RFC1583 Compatible (calculate summary route costs per RFC 1583)

Adjacency Changes

Enable this for the firewall to send a syslog message when an OSPF neighbor goes up/down. Log Adjacency Changes

Enable this for the firewall to send a syslog for each state change. Log Adjacency Change Details

Administrative Route Distances

Inter Area (distance for all routes from one area to another area)	Intra Area (distance for all routes within an area)	External (distance for all routes from other routing domains, learned by redistribution)
<input type="text" value="110"/>	<input type="text" value="110"/>	<input type="text" value="110"/>

Timers (in seconds)

SPF Delay Time (between when OSPF receives a topology change and when it starts a SPF calculation)	SPF Hold Time (between two consecutive SPF calculations)	LSA Group Pacing (interval at which OSPF LSAs are collected into a group and refreshed)
<input type="text" value="5"/>	<input type="text" value="10"/>	<input type="text" value="240"/>

Default Information Originate

Configure this to generate default external route into an OSPF routing domain.

Enable Default Information Originate Always advertise the default route

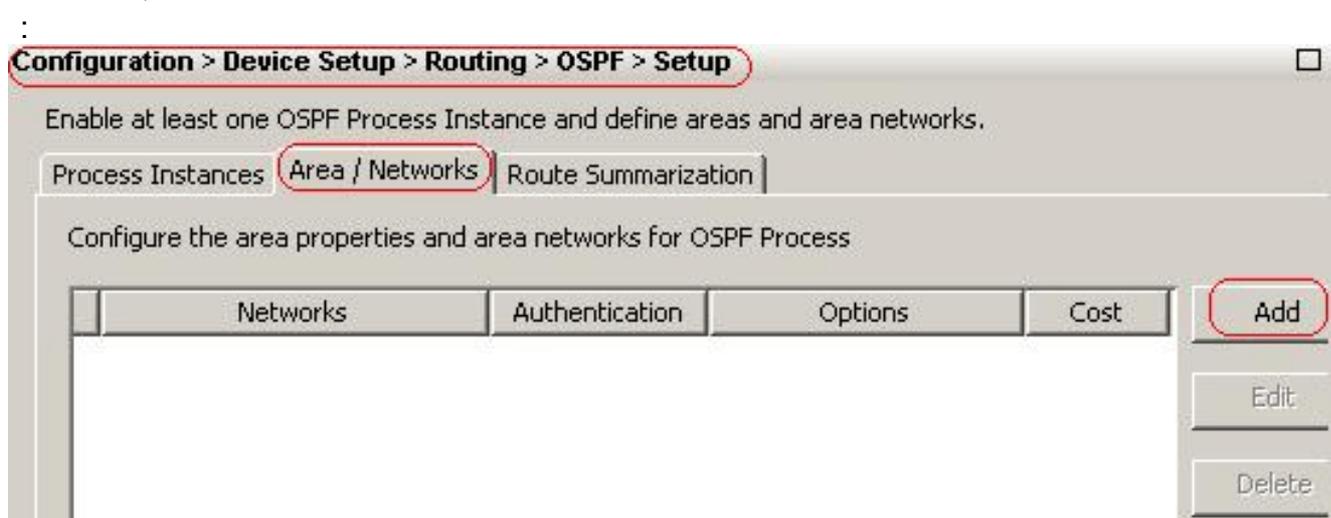
Metric Value: Metric Type: Route Map:

OK Cancel Help

此清單說明每個欄位：OSPF Process — 顯示正在配置的OSPF進程。您無法更改此值。路由器ID — 要使用固定路由器ID，請在Router ID欄位中輸入採用IP地址格式的路由器ID。如果將此值留空，安全裝置上的最高級別的IP地址將用作路由器ID。在本示例中，路由器ID使用內部介面(10.1.1.1)的IP地址進行靜態配置。Ignore LSA MOSPF — 選中此覈取方塊可在安全裝置收到第6類(MOSPF)LSA資料包時抑制系統日誌消息的傳送。預設情況下未選中此設定。RFC 1583相容 — 選中此覈取方塊可根據RFC 1583計算彙總路由成本。取消選中此覈取方塊可根據RFC 2328計算彙總路由成本。為了最大程度降低路由環路的可能性，OSPF路由域中的所有OSPF裝置都應以相同方式設定RFC相容性。預設情況下，此設定處於選中狀態。Adjacency Changes — 包含定義導致傳送系統日誌消息的鄰接更改的設定。Log Adjacency Changes — 選中此覈取方塊可使OSPF鄰居啟動或關閉時安全裝置傳送系統日誌消息。預設情況下，此設定處於選中狀態。Log Adjacency Changes Detail — 選中此覈取方塊可讓安全裝置在任何狀態發生更改時傳送系統日誌消息，而不僅僅是鄰居啟動或關閉時。預設情況下未選中此設定。Administrative Route Distances — 包含基於路由型別的路由管理距離的設定。區域間(Inter Area) — 設定從一個區域到另一個區域的所有路由的管理距離。有效值範圍為1到255。預設值為100。Intra Area — 設定區域內所有路由的管理距離。有效值範圍為1到255。

預設值為100。External — 設定通過重分發獲知的其他路由域中的所有路由的管理距離。有效值範圍為1到255。預設值為100。計時器 — 包含用於配置LSA步調和SPF計算計時器的設定。SPF Delay Time — 指定OSPF收到拓撲更改和SPF計算開始之間的時間。有效值範圍為0到65535。預設值為5。SPF Hold Time — 指定連續SPF計算之間的保持時間。有效值範圍為1到65534。預設值為10。LSA Group Pacing — 指定將LSA收集到組中並刷新、校驗和或老化的間隔。有效值範圍為10到1800。預設值為 240。Default Information Originate — 包含ASBR用於生成到OSPF路由域的預設外部路由的設定。Enable Default Information Originate — 選中此覈取方塊以啟用生成到OSPF路由域的預設路由。始終通告預設路由 — 選中此覈取方塊可始終通告預設路由。預設情況下未選中此選項。Metric Value — 指定OSPF預設度量。有效值範圍為0到16777214。預設值為1。Metric Type — 指定與通告到OSPF路由域的預設路由關聯的外部鏈路型別。有效值為1或2，表示型別1或型別2外部路由。預設值為 2。Route Map -(可選)要應用的路由對映的名稱。如果滿足路由對映，則路由過程將生成預設路由。

5. 完成上述步驟後，在**Setup > Area/Networks**頁籤上定義參與OSPF路由的網路和介面，然後按一下**Add**，如下圖所示



系統將顯示Add OSPF Area對話方塊。

Add OSPF Area

OSPF Process: Area ID:

Area Type

Normal

Stub Summary (allows sending LSAs into the stub area)

NSSA Redistribute (imports routes to normal and NSSA areas)

Summary (allows sending LSAs into the NSSA area)

Default Information Originate (generate a Type 7 default)

Metric Value: Metric Type:

Area Networks

Enter IP Address and Mask

IP Address:

Netmask:

IP Address	Netmask
10.1.1.0	255.255.255.0

Authentication

None Password MD5

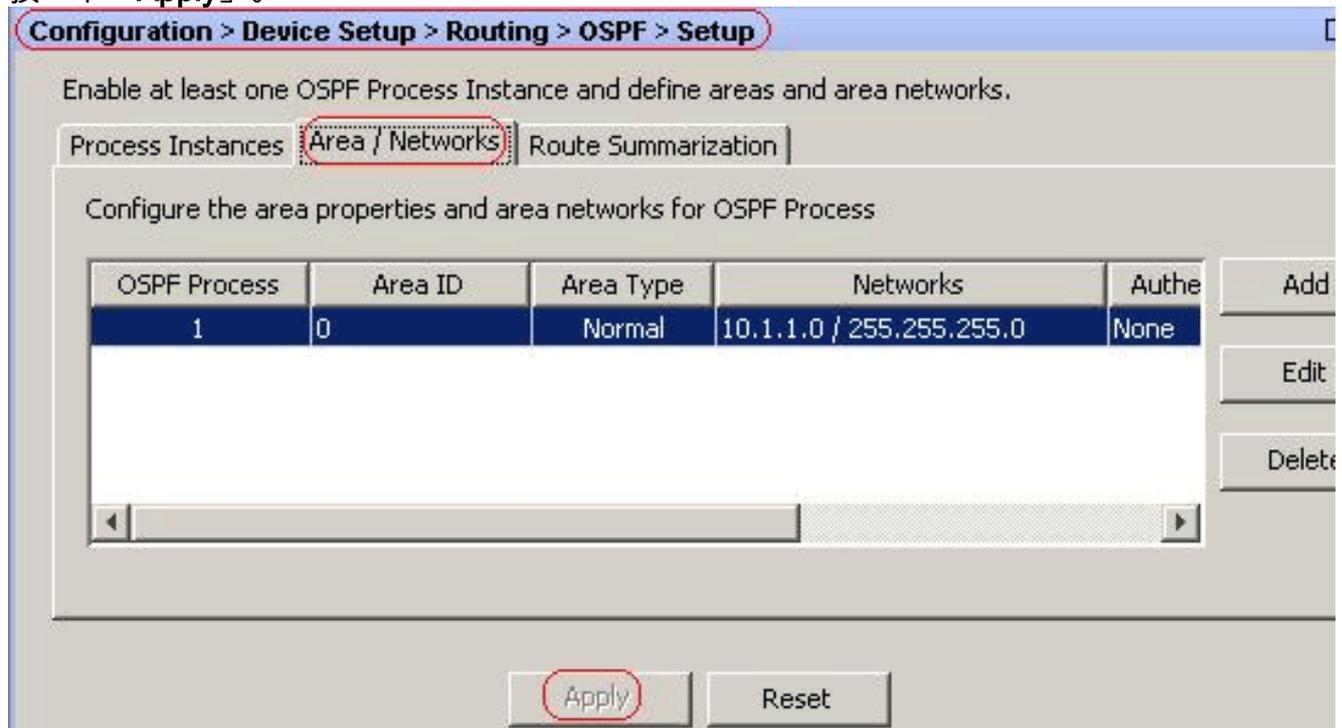
Default Cost:

在本示例中，新增的唯一網路是內部網路(10.1.1.0/24)，因為OSPF僅在內部介面上啟用。注意：只有屬於已定義網路的IP地址介面才能參與OSPF路由過程。

- 按一下「OK」（確定）。此清單說明每個欄位：OSPF進程 — 新增新區域時，為OSPF進程選擇ID。如果安全裝置上只啟用了一個OSPF進程，則預設情況下會選擇該進程。編輯現有區域時，無法更改OSPF進程ID。區域ID — 新增新區域時，輸入區域ID。可以將區域ID指定為十進位制數字或IP地址。有效的十進位制值範圍為0到4294967295。編輯現有區域時不能更改區域ID。在本示例中，區域ID為0。區域型別(Area Type) — 包含所配置區域型別的設定。Normal — 選擇此選項以使該區域成為標準OSPF區域。首次建立區域時，預設情況下會選中此選項。虛設區(Stub) — 選擇此選項以使該區域成為虛設區。末節區域沒有其它任何路由器或區域。末節區域可防止AS外部LSA（第5類LSA）泛洪到末節區域。建立存根區域時，可以取消選中Summary竅取方塊以防止摘要LSA（型別3和4）泛洪到該區域。摘要 — 當所定義的區域是存根區域時，取消選中此竅取方塊可防止LSA傳送到存根區域。對於存根區域，預設情況下選中此竅取方塊。NSSA — 選擇此選項可以使該區域成為非純末節區域。NSSA接受第7類LSA。建立NSSA時，可以取消選中Summary竅取方塊，以防止摘要LSA泛洪到區域中。此外，您可以取消選中Redistribute竅取方塊並啟用Default Information Originate以禁用路由重

分發。Redistribute — 取消選中此覈取方塊可防止將路由匯入NSSA。預設情況下，此覈取方塊處於選中狀態。摘要 — 當所定義的區域是NSSA時，取消選中此覈取方塊可防止LSA傳送到末節區域。預設情況下，NSSA會選中此覈取方塊。Default Information Originate — 選中此覈取方塊以便在NSSA中生成7類預設值。預設情況下取消選中此覈取方塊。Metric Value — 輸入一個值以指定預設路由的OSPF度量值。有效值範圍為0到16777214。預設值為1。Metric Type — 選擇一個值，以便為預設路由指定OSPF度量型別。選項包括1（型別1）或2（型別2）。預設值為2。Area Networks — 包含定義OSPF區域的設定。Enter IP Address and Mask — 包含用於定義區域中的網路的設定。IP Address — 輸入要新增到區域的網路或主機的IP地址。使用網路掩碼為0.0.0.0的0.0.0.0建立預設區域。您只能在一個區域中使用0.0.0.0。Netmask — 選擇要新增到區域中的IP地址或主機的網路掩碼。如果新增主機，請選擇255.255.255.255掩碼。在本例中，10.1.1.0/24是要配置的網路。Add — 將Enter IP Address and Mask區域中定義的網路新增到區域中。新增的網路顯示在Area Networks表中。Delete — 從Area Networks表中刪除所選網路。區域網路(Area Networks) — 顯示為區域定義的網路。IP Address — 顯示網路的IP地址。Netmask — 顯示網路的網路掩碼。Authentication — 包含OSPF區域身份驗證的設定。None — 選擇此選項以禁用OSPF區域身份驗證。這是預設設定。Password — 選擇此選項可使用明文密碼進行區域身份驗證。出於安全考慮，不建議使用此選項。MD5 — 選擇此選項以使用MD5身份驗證。預設成本(Default Cost) — 指定區域的預設成本。有效值範圍為0到65535。預設值為1。

7. 按一下「Apply」。



8. 或者，您可以在Filter Rules窗格中定義路由過濾器。路由過濾可以更好地控制OSPF更新中允許傳送或接收的路由。
9. 您可以選擇配置路由重分發。Cisco ASA可以將RIP和EIGRP發現的路由重分發到OSPF路由進程中。您還可以將靜態路由和連線的路由重新分發到OSPF路由進程。在Redistribution窗格中定義路由重分發。
10. OSPF hello資料包作為組播資料包傳送。如果OSPF鄰居位於非廣播網路中，則必須手動定義該鄰居。手動定義OSPF鄰居時，Hello資料包將作為單播消息傳送到該鄰居。若要定義靜態OSPF鄰居，請轉到Static Neighbor窗格。
11. 可以總結從其他路由協定獲知的路由。用於通告彙總的度量是所有更具體路由中的最小度量。總結路由有助於減小路由表的大小。對OSPF使用總結路由會導致OSPF ASBR將一個外部路由通告為該地址覆蓋的所有重分發路由的聚合。只有從其他路由協定重分發到OSPF的路

由才能總結。

12. 在Virtual link (虛擬鏈路) 窗格中，可以向OSPF網路新增區域，並且無法將該區域直接連線到主幹區域；您必須建立虛擬連結。虛擬鏈路連線具有公共區域 (稱為傳輸區域) 的兩台OSPF裝置。其中一個OSPF裝置必須連線到主幹區域。

配置OSPF身份驗證

Cisco ASA支援對來自OSPF路由協定的路由更新進行MD5身份驗證。每個OSPF資料包中的MD5鍵控摘要可防止未經批准的源引入未經授權的或錯誤的路由消息。在OSPF消息中新增身份驗證可確保您的路由器和Cisco ASA只接受來自配置了相同預共用金鑰的其他路由裝置的路由消息。如果沒有配置此身份驗證，如果有人將具有不同或相反路由資訊的另一個路由裝置引入網路，您的路由器或Cisco ASA上的路由表可能會損壞，並可能引發拒絕服務攻擊。當您為路由裝置 (包括ASA) 之間傳送的EIGRP消息新增身份驗證時，可以防止有目的地或意外將另一台路由器新增到網路以及任何問題。

OSPF路由身份驗證按介面配置。為OSPF消息身份驗證配置的介面上的所有OSPF鄰居必須配置相同的身份驗證模式和金鑰，才能建立鄰接關係。

完成以下步驟，以便在Cisco ASA上啟用OSPF MD5身份驗證：

1. 在ASDM上，導航到Configuration > Device Setup > Routing > OSPF > Interface，然後按一下Authentication頁籤，如下圖所示。



在這種情況下，內部介面上啟用了OSPF。

2. 選擇inside介面，然後按一下Edit。
3. 在Authentication下，選擇MD5 authentication，並在此處新增有關身份驗證引數的詳細資訊。在這種情況下，預共用金鑰為cisco123，金鑰ID為1。

Edit OSPF Interface Authentication

Interface:

Authentication

No authentication
 Area authentication, if defined
 MD5 authentication

Authentication Password

Enter Password: Re-enter Password:

MD5 IDs and Keys

MD5 Key ID:

MD5 Key:

MD5 Key ID	MD5 Key
1	cisco123

4. 按一下「OK」，然後按一下「Apply」。

Configuration > Device Setup > Routing > OSPF > Interface

Configure Interface specific OSPF routing parameters.

Specify the authentication properties for each interface.

Interface	Authentication Type
inside	MD5
dmz	Area
outside	Area

Cisco ASA CLI配置

Cisco ASA

```

ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!--- Inside interface configuration interface
Ethernet0/1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ospf cost 10 !--- OSPF
authentication is configured on the inside interface
ospf message-digest-key 1 md5 <removed> ospf
authentication message-digest ! !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0
ospf cost 10 ! !--- Output Suppressed icmp unreachable
rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin
no asdm history enable arp timeout 14400 ! !--- OSPF
Configuration router ospf 1
  network 10.1.1.0 255.255.255.0 area 0
  log-adj-changes
!

!--- This is the static default gateway configuration in
order to reach Internet route outside 0.0.0.0 0.0.0.0
192.168.1.1 1 ciscoasa#

```

Cisco IOS路由器(R2)CLI配置

Cisco IOS路由器(R2)

```

!--- Interface that connects to the Cisco ASA. !---
Notice the OSPF authentication parameters interface
Ethernet0
ip address 10.1.1.2 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco123

!--- Output Suppressed !--- OSPF Configuration router
ospf 1
  log-adjacency-changes
  network 10.1.1.0 0.0.0.255 area 0
  network 172.16.1.0 0.0.0.255 area 0
  network 172.16.2.0 0.0.0.255 area 0

```

Cisco IOS路由器(R1)CLI配置

Cisco IOS路由器(R1)

```

!--- Output Suppressed !--- OSPF Configuration router
ospf 1
  log-adjacency-changes
  network 172.16.5.0 0.0.0.255 area 0

```

```
network 172.16.2.0 0.0.0.255 area 0
```

Cisco IOS路由器(R3)CLI配置

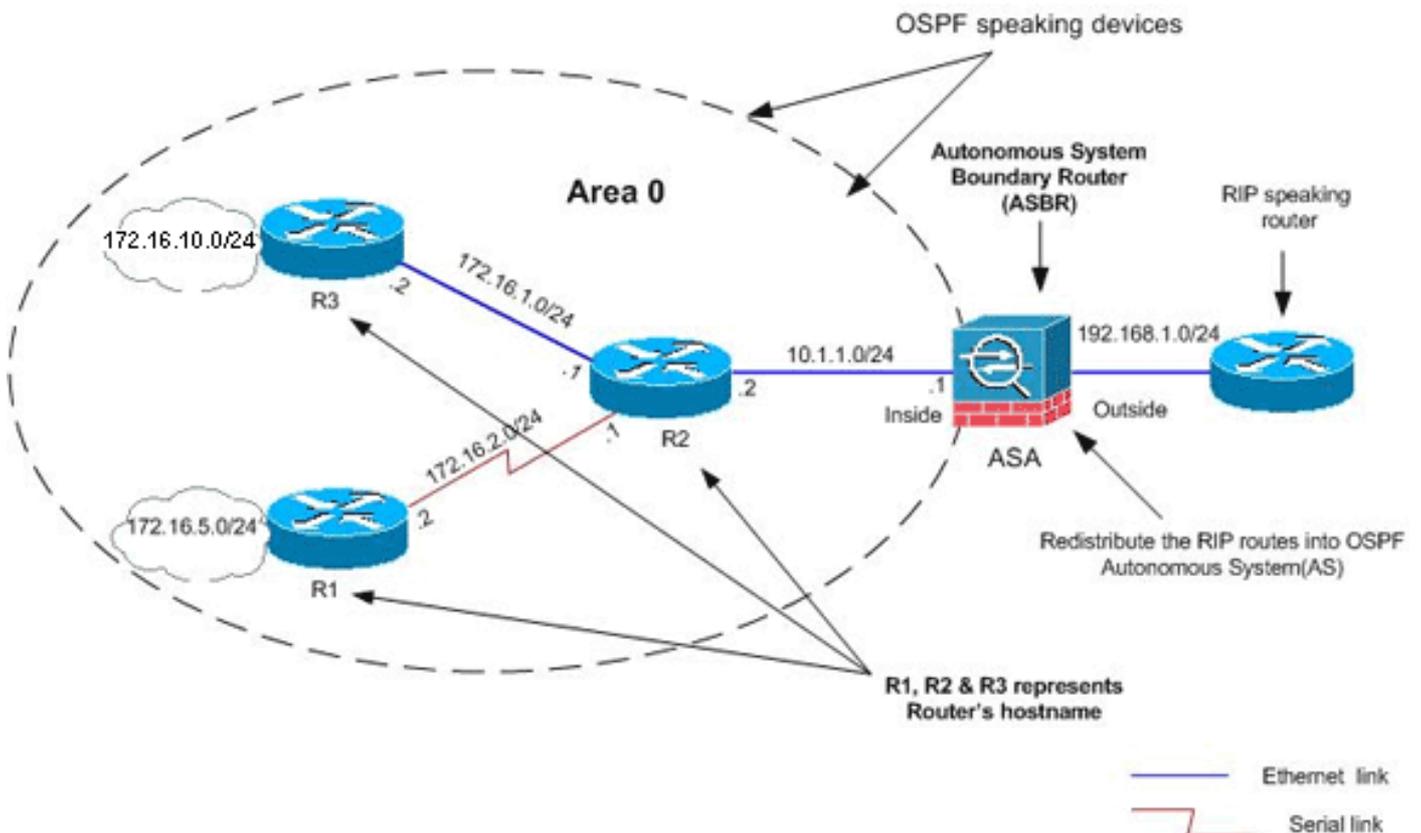
Cisco IOS路由器(R3)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1
log-adjacency-changes
network 172.16.1.0 0.0.0.255 area 0
network 172.16.10.0 0.0.0.255 area 0
```

使用ASA重新分發到OSPF

如前所述，您可以從另一個OSPF路由進程、RIP路由進程或在啟用OSPF的介面上配置的靜態路由和連線路由將路由重分發到OSPF路由進程中。

在此示例中，使用網路圖將RIP路由重分發到OSPF，如下所示：



ASDM配置

1. 選擇 Configuration > Device Setup > Routing > RIP > Setup 以啟用RIP，然後新增網路 192.168.1.0，如下圖所示。

Configuration > Device Setup > Routing > RIP > Setup

Configure the global Routing Information Protocol (RIP) parameters. You can configure the setting of the RIP routing process.

Enable RIP routing

Enable auto-summarization

Enable RIP version Version 1 Version 2

(If global version in not configured then device sends Version 1 and receives Versions 1 & 2.)

Enable default information originate Route Map:

Networks

IP Network to Add:

192.168.1.0

Passive Interfaces

Global passive: Configure all the interfaces as passive globally. This setting will override the individual

Interface	Passive
inside	<input type="checkbox"/>
dmz	<input type="checkbox"/>

2. 按一下「Apply」。
3. 選擇 Configuration > Device Setup > Routing > OSPF > Redistribution > Add 以將 RIP 路由重分發到 OSPF。

Configuration > Device Setup > Routing > OSPF > Redistribution

Define the conditions for redistributing routes from one OSPF process to another.

OSPF Process	Protocol	Match	Subnets	Metric Value	Metric Type

4. 按一下「OK」，然後按一下「Apply」。

Add OSPF Redistribution Entry

OSPF Process: 1

Protocol

Static Connected OSPF

RIP EIGRP

Optional

Match

Internal External 1 External 2 NSSA External 1 NSSA External 2

Metric Value: Metric Type: 2 Tag Value: Use subnets

Route Map:

等效的CLI配置

ASA的CLI配置，用於將RIP重新分發到OSPF AS

```

router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 log-adj-changes
 redistribute rip subnets

router rip
 network 192.168.1.0

```

將RIP路由重分發到OSPF AS後，您可以看到鄰居IOS路由器(R2)的路由表。

R2#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, su - IS-IS summary, 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

```

       172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.16.10.1/32 [110/11] via 172.16.1.2, 01:17:29, Ethernet1
O       172.16.5.1/32 [110/65] via 172.16.2.2, 01:17:29, Serial1
C       172.16.1.0/24 is directly connected, Ethernet1
C       172.16.2.0/24 is directly connected, Serial1
       10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Ethernet0
O E2 192.168.1.0/24 [110/20] via 10.1.1.1, 01:17:29, Ethernet0
!--- Redistributed route adversted by Cisco ASA

```

驗證

完成以下步驟以驗證您的配置：

1. 在ASDM上，可以導航到**Monitoring > Routing > OSPF Neighbors**以檢視每個OSPF鄰居。此圖將內部路由器(R2)顯示為活動鄰居。您還可以看到此鄰居所在的介面、鄰居路由器ID、狀態和失效時間。

Monitoring > Routing > OSPF Neighbors

OSPF Neighbors

Each row represents one OSPF Neighbor. Please click the help button for a description of the states.

Neighbor	Priority	State	Dead Time	Address	Interface
172.16.2.1	1	FULL/BDR	0:00:34	10.1.1.2	inside

Last Updated: 5/19/08 3:55:10 PM

2. 此外，如果導航到**監控>路由>路由**，還可以驗證路由表。在此圖中，172.16.1.0/24、172.16.2.0/24、172.16.5.0/24和172.16.10.0/24網路是透過R2(10.1.1.2)得知的。

Monitoring > Routing > Routes

Routes

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

Protocol	Type	Destination IP	Netmask	Gateway	Int
OSPF	-	172.16.10.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.5.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
OSPF	-	172.16.2.0	255.255.255.0	10.1.1.2	inside
CONNECTED	-	10.1.1.0	255.255.255.0	-	inside
CONNECTED	-	10.77.241.128	255.255.255.192	-	dmz
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dmz
CONNECTED	-	192.168.1.0	255.255.255.0	-	outside
STATIC	DEFAULT	0.0.0.0	0.0.0.0	192.168.1.1	outside

3. 您可以在CLI中使用**show route**命令來取得相同的輸出。

```
ciscoasa#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 192.168.1.1 to network 0.0.0.0
```

```
O 172.16.10.1 255.255.255.255 [110/21] via 10.1.1.2, 0:00:06, inside
O 172.16.5.1 255.255.255.255 [110/75] via 10.1.1.2, 0:00:06, inside
O 172.16.1.0 255.255.255.0 [110/20] via 10.1.1.2, 0:00:06, inside
O 172.16.2.0 255.255.255.0 [110/74] via 10.1.1.2, 0:00:06, inside
```

```

C    10.1.1.0 255.255.255.0 is directly connected, inside
C    10.77.241.128 255.255.255.192 is directly connected, dmz
S    10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz
C    192.168.1.0 255.255.255.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside

```

4. 您還可以使用 `show ospf database` 命令來獲取有關學習的網路和ospf拓撲的資訊。

```
ciscoasa#show ospf database
```

```
OSPF Router with ID (192.168.1.2) (Process ID 1)
```

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
172.16.1.2	172.16.1.2	123	0x80000039	0xfd1d	2
172.16.2.1	172.16.2.1	775	0x8000003c	0x9b42	4
172.16.5.1	172.16.5.1	308	0x80000038	0xb91b	3
192.168.1.2	192.168.1.2	1038	0x80000037	0x29d7	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.1	192.168.1.2	1038	0x80000034	0x72ee
172.16.1.1	172.16.2.1	282	0x80000036	0x9e68

5. `show ospf neighbors` 命令在驗證活動鄰居和通訊方資訊時也非常有用。此示例顯示您在步驟 1 中從 ASDM 獲得的相同資訊。

```
ciscoasa#show ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.2.1	1	FULL/BDR	0:00:36	10.1.1.2	inside

疑難排解

本節提供的資訊可能有助於排除 OSPF 故障。

點對點網路的靜態鄰居配置

如果在 ASA 上配置了 *OSPF 網路點對點非廣播*，則必須定義靜態 OSPF 鄰居以通過點對點非廣播網路通告 OSPF 路由。有關詳細資訊，請參閱 [定義靜態 OSPF 鄰居](#)。

疑難排解指令

[輸出直譯器工具](#) (僅供 [已註冊](#) 客戶使用) (OIT) 支援某些 `show` 命令。使用 OIT 檢視 `show` 命令輸出的分析。

附註： 使用 `debug` 指令之前，請先參閱 [有關 Debug 指令的重要資訊](#)。

- `debug ospf events` — 啟用 OSPF 事件的調試。

```

ciscoasa(config)#debug ospf events
OSPF events debugging is on
ciscoasa(config)# int e0/1
ciscoasa(config-if)# no shu
ciscoasa(config-if)#
OSPF: Interface inside going Up
OSPF: Send with youngest Key 1

```

```
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: 2 Way Communication to 172.16.2.1 on inside, state 2WAY
OSPF: Backup seen Event before WAIT timer on inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 172.16.2.1
OSPF: Elect DR 172.16.2.1
      DR: 172.16.2.1 (Id)   BDR: 172.16.2.1 (Id)
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abd opt 0x2 flag 0x7 len 32
OSPF: Send with youngest Key 1
OSPF: End of hello processing
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x12f3 opt 0x42 flag 0x7 len 32  mtu
 1500 state EXSTART
OSPF: First DBD and we are not SLAVE
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abd opt 0x42 flag 0x2 len 152  mt
u 1500 state EXSTART
OSPF: NBR Negotiation Done. We are the MASTER
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abe opt 0x2 flag 0x3 len 132
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Database request to 172.16.2.1
OSPF: sent LS REQ packet to 10.1.1.2, length 12
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abe opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abf opt 0x2 flag 0x1 len 32
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abf opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Exchange Done with 172.16.2.1 on inside
OSPF: Synchronized with 172.16.2.1 on inside, state FULL
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: Neighbor change Event on interface inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
      DR: 172.16.2.1 (Id)   BDR: 192.168.1.2 (Id)
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
```

注意：請參閱Cisco安全裝置命令參考8.0版的[debug ospf](#)部分，瞭解有關各種命令的詳細資訊，這些命令對排除故障非常有用。

相關資訊

- [Cisco 5500系列調適型安全裝置支援頁面](#)
- [Cisco 500系列PIX支援頁面](#)
- [PIX/ASA 8.X:在思科自適應安全裝置\(ASA\)上配置EIGRP](#)
- [技術支援與文件 - Cisco Systems](#)