

在開放最短路徑優先中配置身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[純文字檔案身份驗證的配置](#)

[MD5身份驗證的配置](#)

[驗證](#)

[驗證明文身份驗證](#)

[驗證MD5身份驗證](#)

[疑難排解](#)

[純文字檔案身份驗證故障排除](#)

[MD5身份驗證故障排除](#)

[相關資訊](#)

簡介

本文檔介紹如何配置開放最短路徑優先(OSPF)身份驗證並允許靈活地對OSPF鄰居進行身份驗證。

必要條件

需求

本文檔的讀者必須熟悉OSPF路由協定的基本概念。請參閱或有關OSPF路由協定的資訊。

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據。

- 思科2503路由器
- Cisco IOS®軟體版本12.2(27)

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。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

背景資訊

本文檔顯示了開放最短路徑優先(OSPF)身份驗證的配置示例，允許靈活地對OSPF鄰居進行身份驗證。您可以在OSPF中啟用身份驗證，以便以安全方式交換路由更新資訊。OSPF身份驗證可以是無(或null)、簡單或MD5。身份驗證方法「none」表示OSPF不使用身份驗證，它是預設方法。使用簡單身份驗證時，口令會以明文形式通過網路傳輸。使用MD5驗證時，密碼不會通過網路傳遞。MD5是RFC 1321中指定的消息摘要演算法。MD5被認為是最安全的OSPF身份驗證模式。配置身份驗證時，必須使用相同型別的身份驗證配置整個區域。在Cisco IOS軟體版本12.0(8)中，每個介面都支援身份驗證。[RFC 2328 \(附錄D\)](#)中也提到了這一點。



注意：只有註冊的思科客戶端可以訪問這些站點和工具。

以下是OSPF支援的三種不同型別的身份驗證：

- Null Authentication — 這也稱為Type 0，這意味著資料包報頭中不包含任何身份驗證資訊。這是預設設定。
- 純文字檔案身份驗證 — 也稱為型別1，它使用簡單的明文密碼。
- MD5 Authentication — 也稱為Type 2，它使用MD5加密密碼。

不需要設定身份驗證。但是，如果已設定，則同一網段上的所有對等路由器必須具有相同的密碼和身份驗證方法。本文檔中的示例演示了純文字檔案和MD5身份驗證的配置。

設定

本節提供用於設定本檔案中所述功能的資訊。

網路圖表

本檔案會使用此網路設定。



網路圖表

純文字檔案身份驗證的配置

當區域內的裝置無法支援更安全的MD5身份驗證時，使用純文字檔案身份驗證。純文字檔案身份驗證使網際網路容易受到「嗅探器攻擊」的攻擊，在這種攻擊中，資料包由協定分析器捕獲，並且密

碼可以被讀取。但是，當您執行OSPF重新配置時，它非常有用，而不是為了安全。例如，在共用公共廣播網路的較舊和較新OSPF路由器上可以使用單獨的口令，以防止路由器之間通訊。整個區域的明文身份驗證密碼不必相同，但在鄰居之間必須相同。

- R2-2503
- R1-2503

R2-2503

```
interface Loopback0
 ip address 10.70.70.70 255.255.255.255
!
interface Serial0
 ip address 192.168.64.10 255.255.255.0
 ip ospf authentication-key c1$c0

!--- The Key value is set as "c1$c0 ". !--- It is the password that is sent across the network.

!
router ospf 10
 log-adjacency-changes
 network 10.70.0.70 0.255.255.255 area 0
 network 192.168.10.10 0.0.0.255 area 0
 area 0 authentication

!--- Plain text authentication is enabled for !--- all interfaces in Area 0.
```


R1-2503

```
interface Loopback0
 ip address 172.16.10.36 255.255.255.240
!
interface Serial0
 ip address 192.168.0.10 255.255.255.0
 ip ospf authentication-key c1$c0

!--- The Key value is set as "c1$c0 ". !--- It is the password that is sent across the network.

!
router ospf 10
 network 172.16.0.0 0.0.255.255 area 0
 network 192.168.10.10 0.0.0.255 area 0
 area 0 authentication

!--- Plain text authentication is enabled !--- for all interfaces in Area 0.
```

 注意：配置中的 `area authentication` 命令啟用特定區域中路由器所有介面的身份驗證。您也可以使用介面下的 `ip ospf authentication` 命令為介面配置純文字檔案身份驗證。如果在介面所屬的區域下配置了不同的身份驗證方法或沒有配置身份驗證方法，可以使用此命令。它將覆蓋為區域配置的身份驗證方法。如果屬於同一區域的不同介面需要使用不同的身份驗證方法，則此命令非常有用

MD5身份驗證的配置

MD5身份驗證比純文字檔案身份驗證提供更高的安全性。此方法使用MD5演算法根據OSPF資料包的內容和密碼（或金鑰）計算雜湊值。該雜湊值隨金鑰ID和非遞減序列號一起在資料包中傳輸。知道相同密碼的接收方會計算自己的雜湊值。如果消息中沒有變化，接收方的雜湊值必須與與該消息一起傳輸的傳送方的雜湊值匹配。

金鑰ID允許路由器引用多個口令。這使得密碼遷移更加簡單和安全。例如，要從一個密碼遷移到另一個密碼，請在不同的金鑰ID下配置一個密碼，然後刪除第一個金鑰。序列號可防止重放攻擊，在該攻擊中，OSPF資料包會被捕獲、修改並重新傳輸到路由器。與純文字檔案身份驗證一樣，MD5身份驗證密碼在整個區域中不必相同。但是，它們需要在鄰居之間保持相同。

 注意：思科建議您在所有路由器上配置 `service password-encryption` 命令。這會導致路由器在顯示任何組態檔時加密密碼，並保護路由器組態的文字副本免受觀察。

- R2-2503
- R1-2503

R2-2503

```
interface Loopback0
 ip address 10.70.70.70 255.255.255.255
!
interface Serial0
 ip address 192.168.64.10 255.255.255.0
 ip ospf message-digest-key 1 md5 c1$c0

!--- Message digest key with ID "1" and !--- Key value (password) is set as "c1$c0 ".

!
router ospf 10
 network 192.168.10.10 0.0.0.255 area 0
 network 10.70.0.70 0.255.255.255 area 0
 area 0 authentication message-digest

!--- MD5 authentication is enabled for !--- all interfaces in Area 0.
```


R1-2503

```
interface Loopback0
 ip address 172.16.10.36 255.255.255.240
!
interface Serial0
 ip address 192.168.0.10 255.255.255.0
 ip ospf message-digest-key 1 md5 c1$c0

!--- Message digest key with ID "1" and !--- Key (password) value is set as "c1$c0 ".

!
router ospf 10
 network 172.16.0.0 0.0.255.255 area 0
 network 192.168.10.10 0.0.0.255 area 0
 area 0 authentication message-digest

!--- MD5 authentication is enabled for !--- all interfaces in Area 0.
```

 注意：此配置中的[area authentication message-digest](#)命令啟用特定區域中所有路由器介面的身份驗證。您也可以使用介面下的[ip ospf authentication message-digest](#)命令為特定介面配置MD5身份驗證。如果在介面所屬的區域下配置了不同的身份驗證方法或沒有配置身份驗證方法，可以使用此命令。它將覆蓋為區域配置的身份驗證方法。如果屬於同一區域的不同介面需要使用不同的身份驗證方法，則此命令非常有用。

驗證

以下各節提供的資訊可用於確認您的配置是否正常工作。

驗證明文身份驗證

如以下輸出所示，使用show ip ospf interface命令檢視為介面配置的身份驗證型別。在這裡，Serial 0介面配置為純文字檔案身份驗證。

```
<#root>
```

```
R1-2503#
```

```
show ip ospf interface serial0
```

```
Serial0 is up, line protocol is up
 Internet Address 192.168.0.10/24, Area 0
 Process ID 10, Router ID 172.16.10.36, Network Type POINT_TO_POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT_TO_POINT,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
Hello due in 00:00:04
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 4 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

Simple password authentication enabled

show ip ospf neighbor命令會顯示鄰居表，其中包含鄰居詳細資訊，如以下輸出所示。

```
<#root>
```

```
R1-2503#
```

```
show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.70.70.70	1	FULL/ -	00:00:31	192.168.64.10	Serial0

show ip route 命令會顯示路由表，如以下輸出所示。

```
<#root>
```

```
R1-2503#
```

```
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, 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
```

```
    10.70.0.70/32 is subnetted, 1 subnets
O       10.70.70.70 [110/65] via 192.168.64.10, 00:03:28, Serial0
    172.16.0.0/28 is subnetted, 1 subnets
C       172.16.10.32 is directly connected, Loopback0
C       192.168.10.10/24 is directly connected, Serial0
```

驗證MD5身份驗證

如以下輸出所示，使用show ip ospf interface命令檢視為介面配置的身份驗證型別。在這裡，Serial 0介面已配置為使用金鑰ID "1"進行MD5身份驗證。

```
<#root>
```

```
R1-2503#
```

```
show ip ospf interface serial0
```

```
Serial0 is up, line protocol is up
 Internet Address 192.168.0.10/24, Area 0
 Process ID 10, Router ID 172.16.10.36, Network Type POINT_TO_POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT_TO_POINT,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:05
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 4 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 10.70.70.70
 Suppress hello for 0 neighbor(s)

 Message digest authentication enabled
 Youngest key id is 1
```

show ip ospf neighbor命令會顯示鄰居表，其中包含鄰居詳細資訊，如以下輸出所示。

```
<#root>
```

```
R1-2503#
```

```
show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.70.70.70	1	FULL/ -	00:00:34	192.168.64.10	Serial0

```
R1-2503#
```

show ip route 命令會顯示路由表，如以下輸出所示。

```
<#root>
```

```
R1-2503#
```

```
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, 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
```

```
10.70.0.70/32 is subnetted, 1 subnets
 0 10.70.70.70 [110/65] via 192.168.64.10, 00:01:23, Serial0
```

```
172.16.0.0/28 is subnetted, 1 subnets
C    172.16.10.32 is directly connected, Loopback0
C    192.168.10.10/24 is directly connected, Serial0
```

疑難排解

以下各節提供了可用於對配置進行故障排除的資訊。發出debug ip ospf adj 命令以擷取驗證程式。必須在建立鄰居關係之前發出此debug命令。

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

純文字檔案身份驗證故障排除

R1-2503的deb ip ospf adj輸出顯示了明文身份驗證成功的時間。

```
<#root>
```

```
R1-2503#
```

```
debug ip ospf adj
```

```
00:50:57: %LINK-3-UPDOWN: Interface Serial0, changed state to down
00:50:57: OSPF: Interface Serial0 going Down
00:50:57: OSPF: 172.16.10.36 address 192.168.0.10 on Serial0 is dead,
state DOWN
00:50:57: OSPF: 10.70.70.70 address 192.168.64.10 on Serial0 is dead,
state DOWN
00:50:57: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from
FULL to DOWN, Neighbor Down: Interface down or detached
00:50:58: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
seq 0x80000009
00:50:58: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to down
00:51:03: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:51:03: OSPF: Interface Serial0 going Up
00:51:04: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
seq 0x8000000A
00:51:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to up
00:51:13: OSPF: 2 Way Communication to 10.70.70.70 on Serial0,
state 2WAY
00:51:13: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2486 opt 0x42
flag 0x7 len 32
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x19A4 opt 0x42
flag 0x7 len 32 mtu 1500 state EXSTART
00:51:13: OSPF: First DBD and we are not SLAVE
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2486 opt 0x42
flag 0x2 len 72 mtu 1500 state EXSTART
00:51:13: OSPF: NBR Negotiation Done. We are the MASTER
00:51:13: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2487 opt 0x42
flag 0x3 len 72
00:51:13: OSPF: Database request to 10.70.70.70
00:51:13: OSPF: sent LS REQ packet to 192.168.64.10, length 12
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2487 opt 0x42
```



```
flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2488 opt 0x42
flag 0x1 len 32
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2488 opt 0x42
flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Exchange Done with 10.70.70.70 on Serial0
00:51:13: OSPF: Synchronized with 10.70.70.70 on Serial0, state FULL

!--- Indicates the neighbor adjacency is established.

00:51:13: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from LOADING
to FULL, Loading Done
00:51:14: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
seq 0x8000000B
R1-2503#
```

當路由器上配置的身份驗證型別不匹配時，這是debug ip ospf adj命令的輸出。此輸出顯示，路由器R1-2503使用型別1身份驗證，而路由器R2-2503配置為型別0身份驗證。這表示路由器R1-2503配置為純文字檔案身份驗證（型別1），而路由器R2-2503配置為空身份驗證（型別0）。

```
<#root>
R1-2503#
debug ip ospf adj
00:51:23: OSPF: Rcv pkt from 192.168.64.10, Serial0 :
Mismatch
Authentication type
.
!--- Input packet specified type 0, you use type 1.
```

當驗證金鑰（密碼）值不相符時，debug ip ospf adj指令的輸出如下。在這種情況下，兩台路由器都配置為純文字檔案身份驗證（型別1），但金鑰（密碼）值不匹配。

```
<#root>
R1-2503#
debug ip ospf adj
00:51:33: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication Key - Clear Text
```

MD5身份驗證故障排除

這是MD5身份驗證成功時R1-2503的debug ip ospf adj 命令輸出。

<#root>

R1-2503#

debug ip ospf adj

00:59:03: OSPF: Send with youngest Key 1

00:59:13: OSPF: Send with youngest Key 1

00:59:17: %LINK-3-UPDOWN: Interface Serial0, changed state to down

00:59:17: OSPF: Interface Serial0 going Down

00:59:17: OSPF: 172.16.10.36 address 192.168.0.10 on Serial0 is dead, state DOWN

00:59:17: OSPF: 10.70.70.70 address 192.168.64.10 on Serial0 is dead, state DOWN

00:59:17: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from FULL to DOWN, Neighbor Down: Interface down or detached

00:59:17: OSPF: Build router LSA for area 0, router ID 172.16.10.36, seq 0x8000000E

00:59:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down

00:59:32: %LINK-3-UPDOWN: Interface Serial0, changed state to up

00:59:32: OSPF: Interface Serial0 going Up

00:59:32: OSPF: Send with youngest Key 1

00:59:33: OSPF: Build router LSA for area 0, router ID 172.16.10.36, seq 0x8000000F

00:59:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up

00:59:42: OSPF: Send with youngest Key 1

00:59:42: OSPF: 2 Way Communication to 10.70.70.70 on Serial0, state 2WAY

!--- Both neighbors configured for Message !--- digest authentication with Key ID "1".

00:59:42: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2125 opt 0x42 flag 0x7 len 32

00:59:42: OSPF: Send with youngest Key 1

00:59:42: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x11F3 opt 0x42 flag 0x7 len 32 mtu 1500 state EXSTART

00:59:42: OSPF: First DBD and we are not SLAVE

00:59:42: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2125 opt 0x42 flag 0x2 len 72 mtu 1500 state EXSTART

00:59:42: OSPF: NBR Negotiation Done. We are the MASTER

00:59:42: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2126 opt 0x42 flag 0x3 len 72

00:59:42: OSPF: Send with youngest Key 1

00:59:42: OSPF: Send with youngest Key 1

00:59:42: OSPF: Database request to 10.70.70.70

00:59:42: OSPF: sent LS REQ packet to 192.168.64.10, length 12

00:59:42: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2126 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE

00:59:42: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2127 opt 0x42 flag 0x1 len 32

00:59:42: OSPF: Send with youngest Key 1

00:59:42: OSPF: Send with youngest Key 1

00:59:42: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2127 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE

00:59:42: OSPF: Exchange Done with 10.70.70.70 on Serial0

00:59:42: OSPF: Synchronized with 10.70.70.70 on Serial0, state FULL

00:59:42: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from LOADING to FULL, Loading Done

```
00:59:43: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x80000010
00:59:43: OSPF: Send with youngest Key 1
00:59:45: OSPF: Send with youngest Key 1
R1-2503#
```

當路由器上配置的身份驗證型別不匹配時，這是debug ip ospf adj命令的輸出。此輸出顯示，路由器R1-2503使用型別2(MD5)身份驗證，而路由器R2-2503使用型別1身份驗證（純文字檔案身份驗證）。

```
<#root>
```

```
R1-2503#
```

```
debug ip ospf adj
```

```
00:59:33: OSPF: Rcv pkt from 192.168.64.10, Serial0 :
```

```
Mismatch
Authentication type.
```

```
!--- Input packet specified type 1, you use type 2.
```

當用於身份驗證的金鑰ID不匹配時，這是debug ip ospf adj命令的輸出。此輸出顯示，路由器R1-2503使用金鑰ID 1的MD5身份驗證，而路由器R2-2503使用金鑰ID 2的MD5身份驗證。

```
<#root>
```

```
R1-2503#
```

```
debug ip ospf adj
```

```
00:59:33: OSPF: Send with youngest Key 1
00:59:43: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication Key - No message digest key 2 on interface
```

R1-2503的此debug ip ospf adj命令輸出顯示，MD5身份驗證的金鑰1和金鑰2都配置為遷移的一部分。

```
<#root>
```

```
R1-2503#
```

```
debug ip ospf adj
```

```
00:59:43: OSPF: Send with youngest Key 1
00:59:53: OSPF: Send with youngest Key 2
```

```
!--- Informs that this router is also configured !--- for Key 2 and both routers now use Key 2.  
01:00:53: OSPF: 2 Way Communication to 10.70.70.70  
on Serial0, state 2WAY  
R1-2503#
```

相關資訊

- [在虛擬鏈路上配置OSPF身份驗證](#)
- [為什麼show ip ospf neighbor命令顯示處於Init狀態的鄰居？](#)
- [OSPF命令](#)
- [OSPF配置示例](#)
- [IP 路由支援頁面](#)
- [思科技術支援與下載](#)

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）。