

# 在开放最短路径优先中配置身份验证

## 目录

---

### [简介](#)

### [先决条件](#)

#### [要求](#)

#### [使用的组件](#)

#### [规则](#)

### [背景信息](#)

### [配置](#)

#### [网络图](#)

#### [明文认证的配置](#)

#### [MD5认证的配置](#)

### [验证](#)

#### [验证明文身份验证](#)

#### [验证 MD5 身份验证](#)

### [故障排除](#)

#### [明文身份验证故障排除](#)

#### [MD5 身份验证故障排除](#)

### [相关信息](#)

---

## 简介

本文档介绍如何配置开放最短路径优先(OSPF)身份验证并允许灵活验证OSPF邻居。

## 先决条件

### 要求

本文档的读者必须熟悉OSPF路由协议的基本概念。请参阅或有关OSPF路由协议的信息。

### 使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco 2503 路由器
- Cisco IOS® 软件版本 12.2(27)


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。

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 背景信息

本文档显示了开放路径最短优先 (OSPF) 身份验证的示例配置，使用该身份验证方法可以灵活地对 OSPF 邻居进行身份验证。您可以在 OSPF 中启用身份验证，以便通过安全方式交换路由更新信息。OSPF 身份验证可以是“无”（或“空”）、“简单”或“MD5”。身份验证方法“无”表示不对 OSPF 使用身份验证，这是默认方法。使用简单身份验证时，口令在网络上以明文方式发送。如果使用 MD5 身份验证，则口令不会通过网络传递。MD5 是 RFC 1321 中指定的消息摘要算法。MD5 被认为是最安全的 OSPF 认证模式。当配置身份认证时，您必须在整个区域中配置相同类型的身份认证。在 Cisco IOS 软件版本 12.0(8) 中，每个接口都支持身份验证。[RFC 2328 附录 D 中也提到了相关信息](#)。

 注意：只有注册的思科客户端可以访问这些站点和工具。

以下是 OSPF 支持的三种不同类型的身份验证：

- 空身份验证 — 又称为类型 0，表示不在数据包报头中包含身份验证信息。这种模式是默认模式。
- 明文身份验证 — 又称为类型 1，它使用简单的明文口令。
- MD5 Authentication — 也称为类型 2，它使用 MD5 加密密码。

身份验证无需设置。但是，如果已设置，则相同网段上的所有对等路由器必须使用相同的口令和身份验证方法。本文档中的示例演示了如何配置明文身份验证和 MD5 身份验证。

## 配置

本部分提供了用于配置本文档所述功能的信息。

## 网络图

本文档使用此网络设置。



网络图

## 明文认证的配置

当某个区域中的设备无法支持更安全的 MD5 身份验证时，将使用明文身份验证。明文身份验证使互连网络容易受到“嗅探器攻击”，受到这种攻击时，数据包会被协议分析程序捕获，并且口令可被

读取。但是，当您执行 OSPF 重新配置而不考虑安全性时，此身份验证类型非常有用。例如，在共享同一个广播网络的较旧和较新的 OSPF 路由器上可以使用单独的口令，以防止路由器之间的通信。明文身份验证口令在整个区域中不必相同，但它们在邻居之间必须相同。

- 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` 命令启用特定区域中路由器所有接口的身份验证。您也可以使用 `ip ospf authentication` 命令为接口配置明文身份验证。如果在接口所属的区域下配置了不同的身份验证方法或者未配置身份验证方法，则可以使用此命令。它将会覆盖针对该区域配置的身份验证方法。如果属于同一区域的不同接口需要使用不同的身份验证方法，则此命令非常有用

## MD5认证的配置

MD5 身份验证提供的安全性高于明文身份验证。此方法使用 MD5 算法来基于 OSPF 数据包的内容计算出一个散列值，并计算出一个口令（或密钥）。此散列值将与密钥 ID 以及非递减序号一起在数据包中传输。知道同一口令的接收方将计算出其自己的散列值。如果消息中没有变化，接收方的散列值必须与随消息传输的发送方的散列值匹配。

密钥 ID 允许路由器参考多个口令。这样就可以更方便且更安全地迁移口令。例如，要从一个口令迁移到另一个口令，可在一个不同的密钥 ID 下配置一个口令，然后删除第一个密钥。序号可防止重放攻击，受到这种攻击时，OSPF 数据包将被捕获、修改并重新传输到路由器。与明文身份验证一样，MD5 身份验证口令不必在整个区域中相同。但是，它们在邻居之间必须相同。

 注意：Cisco 建议您在所有路由器上配置 `service password-encryption` 命令。这会导致路由器在配置文件的任意显示中加密口令，并保护路由器配置的文本副本不被观察。

- 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](#)命令启用特定区域中所有路由器接口的身份验证。您也可以在接口下使用 `ip ospf authentication message-digest` 命令来为特定接口配置 MD5 身份验证。如果在接口所属的区域下配置了不同的身份验证方法或者未配置身份验证方法，则可以使用此命令。它将会覆盖针对该区域配置的身份验证方法。如果属于相同区域的不同接口需要使用不同的身份验证方法，则此配置将非常有用。

## 验证

您可以参考下列部分中的信息来确保您的配置正常工作。

### 验证明文身份验证

使用 `show ip ospf interface` 命令可以查看为接口配置的身份验证类型，如此输出所示。这里，为明文身份验证配置了 Serial 0 接口。

```
<#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 命令显示包括邻居详细信息的邻居表，如此输出所示。

```
<#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 命令显示路由表，如此输出所示。

```
<#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
```

## 验证 MD5 身份验证

使用 show ip ospf interface 命令可以查看为接口配置的身份验证类型，如此输出所示。这里，已配置了 Serial 0 接口以使用密钥 ID“1”进行 MD5 身份验证。

```
<#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 命令显示包括邻居详细信息的邻居表，如此输出所示。

```
<#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 命令显示路由表，如此输出所示。

```
<#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
```

## 故障排除

您可以参考以下部分中的信息来对您的配置进行故障排除。发出 `debug ip ospf adj` 命令以捕获身份验证进程。必须在建立邻居关系之前发出此debug命令。

---

 注意：使用[debug命令之前](#)，请参阅有关Debug命令的重要信息。

---

### 明文身份验证故障排除

当明文身份验证成功时，将显示 R1-2503 的 `deb ip ospf adj` 输出。

```
<#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#
```

这是当路由器上配置的身份验证类型不匹配时，debug ip ospf adj 命令的输出。此输出显示，路由器 R1-2503 使用了类型 1 身份验证，而路由器 R2-2503 是针对类型 0 身份验证配置的。也就是说，路由器 R1-2503 是针对明文身份验证（类型 1）配置的，而路由器 R2-2503 是针对空身份验证（类型 0）配置的。

```
<#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.
```

这是当身份验证密钥（口令）值不匹配时，debug ip ospf adj 命令的输出。在这种情况下，两个路由器都是针对明文身份验证（类型 1）配置的，但密钥（口令）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 身份验证故障排除

这是MD5身份验证成功时R1-2503的debug ip ospf adj命令输出。

```
<#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#
```

这是当路由器上配置的身份验证类型不匹配时，debug ip ospf adj 命令的输出。此输出显示，路由器 R1-2503 使用了类型 2 (MD5) 身份验证，而路由器 R2-2503 使用了类型 1 身份验证 (明文身份验证)。

```
<#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.
```

这是当用于身份验证的密钥 ID 不匹配时，debug ip ospf adj 命令的输出。此输出显示，路由器 R1-2503 将 MD5 身份验证与密钥 ID 1 一起使用，而路由器 R2-2503 将 MD5 身份验证与密钥 ID 2 一起使用。

```
<#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
```

当MD5身份验证的密钥1和密钥2都配置为迁移的一部分时，R1-2503的此debug ip ospf adj命令输出显示。

```
<#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 Serial10, state 2WAY

R1-2503#

## 相关信息

- [在虚拟链路上配置 OSPF 认证](#)
- [为什么 show ip ospf neighbor 命令显示邻居阻塞在初始状态？](#)
- [OSPF 命令](#)
- [OSPF 配置示例](#)
- [IP 路由 支持页](#)
- [思科技术支持和下载](#)

## 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）。