OSPF 中身份验证配置示例

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
背景信息
Configure
Network Diagram
明文身份验证配置
MD5 身份验证配置
Verify
验证明文身份验证
验证 MD5 身份验证
Troubleshoot
明文身份验证故障排除
MD5 身份验证故障排除
Related Information

Introduction

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。从 Cisco IOS® 软件版本 12.0(8) 开始，已基于每个接口支持身份验证。RFC 2328附录 D 中也提到了相关信息。 思科漏洞 ID CSCdk33792（仅注册客户可访问）中已添加此功能。

Prerequisites

Requirements

本文档的读者应熟悉 OSPF 路由协议的基本概念。有关 OSPF 路由协议的详细信息，请参阅开放最短路径优先文档。

Components Used

本文档中的信息基于以下软件和硬件版本。

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

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

背景信息

OSPF 支持三种不同类型的身份验证，具体如下：

- **无身份验证** - 也称为类型 0，意味着数据包报头中不包含身份验证信息。这是默认类型。
- **明文身份验证** - 也称为类型 1，使用简单的明文密码。
- **MD5 身份验证** - 也称为类型 2，使用 MD5 加密密码。

身份验证不需要设置。但是如果设置身份验证，同一网段上的所有对等路由器都必须具有相同的密码和身份验证方式。本文档示例演示的是明文身份验证和 MD5 身份验证的配置。

Configure

本部分提供了用于配置本文档所述功能的信息。

Note: 要查找本文档所用命令的更多信息，请使用命令查找工具（仅注册客户可访问）。

Network Diagram

本文档使用此网络设置。

明文身份验证配置

某个区域内的设备在不支持更安全的 MD5 身份验证时使用明文身份验证。明文身份验证让网际网络易受“嗅探器攻击”；在攻击过程中，协议分析工具会捕获数据包，读取其中的密码。但是，除了安全外，执行 OSPF 重新配置时，明文身份验证非常有用。例如，共享通用广播网络的新旧 OSPF 路由器可以使用单独的密码，以防止它们相互对话。明文身份验证密码没必要在整个区域内保持一致，但在邻居之间必须保持一致。

- R2-2503
- R1-2503

R2-2503

```
interface Loopback0
  ip address 70.70.70.70 255.255.255.255
 !
 interface Serial0
  ip address 192.16.64.2 255.255.255.0
  ip ospf authentication-key c1$c0
!--- The Key value is set as "c1$c0 ". !--- It is the
password that is sent across the network. clockrate
64000 ! router ospf 10 log-adjacency-changes network
70.0.0.0 0.255.255.255 area 0 network 192.16.64.0
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 192.16.64.1 255.255.255.0
 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
192.16.64.0 0.0.0.255 area 0 area 0 authentication !---
Plain text authentication is enabled !--- for all
interfaces in Area 0.
```

Note: 配置中的 area authentication 命令为特定区域路由器的所有接口启用身份验证。还可以在接口下使用 ip ospf authentication 命令为接口配置明文身份验证。如果在接口所属区域下配置了不同的身份验证方式或未配置身份验证方式，则可以使用此命令。该命令会覆盖为此区域配置的身份验证方式。同属一个区域的不同接口需要使用不同的身份验证方式时，该命令会非常有用。

MD5 身份验证配置

MD5 身份验证具有比明文身份验证更高的安全性。此方式使用 MD5 算法计算出 OSPF 数据包和密码（或密钥）内容的散列值 。该散列值连同密钥 ID 和非递减的序列号在数据包中一起传输。知晓相同密码的接收端计算自身的散列值。如果消息中的内容未更改，则接收端收到的散列值应匹配消息中传输的发送端的散列值。

密钥 ID 使路由器可以引用多个密码。这让密码迁移更简单、更安全。例如，要从一个密码迁移到另一个密码，在另一个不同的密钥 ID 下配置密码，然后删除第一个密钥。序列号可防止重播攻击；在攻击过程中，OSPF 数据包会被捕获和修改，然后重新传输到路由器。与明文身份验证相同，MD5 身份验证密码没必要在整个区域内保持一致。但是，它们在邻居之间必须相同。

Note: 思科建议在所有路由器上配置 service password-encryption 命令。这样，不管配置文件如何显示，路由器都会加密其中的密码，防止他人通过观察路由器的配置文本而获知密码。

- R2-2503
- R1-2503

R2-2503

```
```

```
interface Loopback0
  ip address 70.70.70.70 255.255.255.255
 !
 interface Serial0
  ip address 192.16.64.2 255.255.255.0
  ip ospf message-digest-key 1 md5 c1$c0
!--- Message digest key with ID "1" and !--- Key value
(password) is set as "c1$c0 ". clockrate 64000 ! router
ospf 10 network 192.16.64.0 0.0.0.255 area 0 network
70.0.0.0 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 192.16.64.1 255.255.255.0
 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
192.16.64.0 0.0.0.255 area 0 area 0 authentication
message-digest !--- MD5 authentication is enabled for !-
-- all interfaces in Area 0.
```

Note: 配置中的 area authentication message-digest 命令为特定区域的所有路由器接口启用身份验证。还可以在接口下使用 ip ospf authentication message-digest 命令为特定接口配置 MD5 身份验证。如果在接口所属区域下配置了不同的身份验证方式或未配置身份验证方式，则可以使用此命令。该命令会覆盖为此区域配置的身份验证方式。同属一个区域的不同接口需要使用不同的身份验证方式时，该命令会非常有用。

Verify

以下部分提供可用于确认配置正常工作的信息。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

验证明文身份验证

使用 show ip ospf interface 命令查看为接口配置的身份验证类型，如输出所示。在本示例中，为 Serial 0 接口配置了明文身份验证。

```
R1-2503# show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.16.64.1/24, 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 命令显示邻居列表，包括邻居的详细信息，如输出所示。

```
R1-2503# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
70.70.70.70       1   FULL/  -        00:00:31    192.16.64.2     Serial0
```

show ip route 命令显示路由表，如输出所示。

```
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

     70.0.0.0/32 is subnetted, 1 subnets
O       70.70.70.70 [110/65] via 192.16.64.2, 00:03:28, Serial0
     172.16.0.0/28 is subnetted, 1 subnets
C       172.16.10.32 is directly connected, Loopback0
C    192.16.64.0/24 is directly connected, Serial0
```

验证 MD5 身份验证

使用 show ip ospf interface 命令查看为接口配置的身份验证类型，如输出所示。在本示例中，为 Serial 0 接口配置了 MD5 身份验证， 密钥 ID 为“1”。

```
R1-2503# show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.16.64.1/24, 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 70.70.70.70
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

show ip ospf neighbor 命令显示邻居列表，包括邻居的详细信息，如输出所示。

```
R1-2503# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
```

```
70.70.70.70       1   FULL/  -        00:00:34    192.16.64.2     Serial0
R1-2503#
```

show ip route 命令显示路由表，如输出所示。

```
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

     70.0.0.0/32 is subnetted, 1 subnets
O       70.70.70.70 [110/65] via 192.16.64.2, 00:01:23, Serial0
     172.16.0.0/28 is subnetted, 1 subnets
C       172.16.10.32 is directly connected, Loopback0
C    192.16.64.0/24 is directly connected, Serial0
```

Troubleshoot

以下部分提供可用于对配置进行故障排除的信息。执行 **debug ip ospf adj 命令**以捕捉身份验证过程。应在邻居关系建立之前执行该 **debug 命令**。

Note: 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

R1-2503 上的 **deb ip ospf adj** 命令输出显示明文身份验证成功的时刻。

```
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 192.16.64.1 on Serial0 is dead,
  state DOWN
00:50:57: OSPF: 70.70.70.70 address 192.16.64.2 on Serial0 is dead,
  state DOWN
00:50:57: %OSPF-5-ADJCHG: Process 10, Nbr 70.70.70.70 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 70.70.70.70 on Serial0,
  state 2WAY
00:51:13: OSPF: Send DBD to 70.70.70.70 on Serial0 seq 0x2486 opt 0x42
  flag 0x7 len 32
00:51:13: OSPF: Rcv DBD from 70.70.70.70 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 70.70.70.70 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 70.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x3 len 72
00:51:13: OSPF: Database request to 70.70.70.70
00:51:13: OSPF: sent LS REQ packet to 192.16.64.2, length 12
00:51:13: OSPF: Rcv DBD from 70.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Send DBD to 70.70.70.70 on Serial0 seq 0x2488 opt 0x42
  flag 0x1 len 32
00:51:13: OSPF: Rcv DBD from 70.70.70.70 on Serial0 seq 0x2488 opt 0x42
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Exchange Done with 70.70.70.70 on Serial0
00:51:13: OSPF: Synchronized with 70.70.70.70 on Serial0, state FULL
!--- Indicates the neighbor adjacency is established. 00:51:13: %OSPF-5-ADJCHG: Process 10, Nbr
70.70.70.70 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#
```

以下是路由器上配置的身份验证类型不匹配时，**debug ip ospf adj 命令**的输出结果。该输出显示，R1-2503 路由器使用类型 1 身份验证，而 R2-2503 路由器被配置为类型 0 身份验证。这意味着路由器 R1-2503 被配置为明文身份验证（类型 1），而路由器 R2-2503 被配置为无身份验证（类型 0）。

```
R1-2503# debug ip ospf adj
00:51:23: OSPF: Rcv pkt from 192.16.64.2, Serial0 : Mismatch
Authentication type.
!--- Input packet specified type 0, you use type 1.
```

以下是身份验证密钥（密码）值不匹配时，**debug ip ospf adj 命令**的输出结果。在本示例中，两台路由器都被配置为明文身份验证（类型 1），但密钥（密码）值不匹配。

```
R1-2503# debug ip ospf adj
00:51:33: OSPF: Rcv pkt from 192.16.64.2, Serial0 : Mismatch
Authentication Key - Clear Text
```

MD5 身份验证故障排除

以下是 MD5 身份验证成功时，R1-2503 上的 **debug ip ospf adj 命令**输出结果。

```
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 192.16.64.1 on Serial0 is dead,
  state DOWN
00:59:17: OSPF: 70.70.70.70 address 192.16.64.2 on Serial0 is dead,
  state DOWN
00:59:17: %OSPF-5-ADJCHG: Process 10, Nbr 70.70.70.70 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 70.70.70.70 on Serial0,
  state 2WAY
!--- Both neighbors configured for Message !--- digest authentication with Key ID "1". 00:59:42:
OSPF: Send DBD to 70.70.70.70 on Serial0 seq 0x2125 opt 0x42 flag 0x7len 32 00:59:42: OSPF: Send
with youngest Key 1 00:59:42: OSPF: Rcv DBD from 70.70.70.70 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 70.70.70.70 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 70.70.70.70
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 70.70.70.70
00:59:42: OSPF: sent LS REQ packet to 192.16.64.2, length 12 00:59:42: OSPF: Rcv DBD from
70.70.70.70 on Serial0 seq 0x2126 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE 00:59:42:
OSPF: Send DBD to 70.70.70.70 on Serial0 seq 0x2127 opt 0x42 flag 0x1len 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
70.70.70.70 on Serial0 seq 0x2127 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE 00:59:42:
OSPF: Exchange Done with 70.70.70.70 on Serial0 00:59:42: OSPF: Synchronized with 70.70.70.70 on
Serial0, state FULL 00:59:42: %OSPF-5-ADJCHG: Process 10, Nbr 70.70.70.70 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#
```

以下是路由器上配置的身份验证类型不匹配时，**debug ip ospf adj 命令**的输出结果。该输出显示，R1-2503 路由器使用类型 2 (MD5) 身份验证，而 R2-2503 路由器使用类型 1 身份验证（明文身份验证）。

```
R1-2503# debug ip ospf adj
00:59:33: OSPF: Rcv pkt from 192.16.64.2, Serial0 : Mismatch
Authentication type.
!--- Input packet specified type 1, you use type 2.
```

以下是用于身份验证的密钥 ID 不匹配时，**debug ip ospf adj 命令**的输出结果。该输出显示，R1-2503 路由器使用 MD5 身份验证，密钥 ID 为 1，而 R2-2503 路由器使用 MD5 身份验证，密钥 ID 为 2。

```
R1-2503# debug ip ospf adj
00:59:33: OSPF: Send with youngest Key 1
00:59:43: OSPF: Rcv pkt from 192.16.64.2, Serial0 : Mismatch
Authentication Key - No message digest key 2 on interface
```

以下是 R1-2503 上的 **debug ip ospf adj 命令**输出结果；该输出显示 MD5 身份验证密钥 1 和密钥 2 同时配置用于迁移的时刻。

```
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 70.70.70.70 on Serial0, state 2WAY R1-2503#
```

Related Information

- 在虚拟链路上配置 OSPF 认证
- 为什么 show ip ospf neighbor 命令会显示处于 Init 状态的邻居？
- OSPF 命令

- OSPF 配置示例
- OSPF 技术支持页面
- Technical Support & Documentation - Cisco Systems