Configure Authentication in Open Shortest Path First

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Network Diagram
- Configurations for Plain Text Authentication
- Configurations for MD5 Authentication

Verify

- Verify Plain Text Authentication
- Verify MD5 Authentication

Troubleshoot

- Troubleshoot Plain Text Authentication
- Troubleshoot MD5 Authentication

Related Information

Introduction

This document describes how to configure Open Shortest Path First (OSPF) authentication and allow the flexibility to authenticate OSPF neighbors.

Prerequisites

Requirements

Readers of this document must be familiar with basic concepts of OSPF routing protocol. Refer to the or information on the OSPF routing protocol.

Components Used

The information in this document is based on these software and hardware versions.

- Cisco 2503 routers
- Cisco IOS® Software Release 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, ensure that you understand the potential impact of any command.

Background Information

This document shows sample configurations for Open Shortest Path First (OSPF) authentication which allows the flexibility to authenticate OSPF neighbors. You can enable authentication in OSPF in order to exchange routing update information in a secure manner. OSPF authentication can either be none (or null), simple, or MD5. In the authentication method, none" means that no authentication is used for OSPF and it is the default method. With simple authentication, the password goes in clear-text over the network. With MD5 authentication, the password does not pass over the network. MD5 is a message-digest algorithm specified in RFC 1321. MD5 is considered the most secure OSPF authentication mode. When you configure authentication, you must configure an entire area with the same type of authentication. With Cisco IOSSoftware Release 12.0(8), authentication is supported on a per-interface basis. This is also mentioned in RFC 2328, Appendix D.

Note: Only registered Cisco clients can access these sites and tools.

These are the three different types of authentication supported by OSPF:

- Null Authentication — This is also called Type 0 and it means no authentication information is included in the packet header. It is the default.
- Plain Text Authentication — This is also called Type 1 and it uses simple clear-text passwords.
- MD5 Authentication — This is also called Type 2 and it uses MD5 cryptographic passwords.

Authentication does not need to be set. However, if it is set, all peer routers on the same segment must have the same password and authentication method. The examples in this document demonstrate configurations for both plain text and MD5 authentication.

Configure

This section presents you with the information to configure the features this document describes.

Network Diagram

This document uses this network setup.



Network Diagram

Configurations for Plain Text Authentication

Plain text authentication is used when devices within an area cannot support the more secure MD5 authentication. Plain text authentication leaves the internetwork vulnerable to a sniffer attack, in which packets are captured by a protocol analyzer and the passwords can be read. However, it is useful when you perform OSPF reconfiguration, rather than for security. For example, separate passwords can be used on older and newer OSPF routers that share a common broadcast network to prevent communication between routers. Plain text authentication passwords do not have to be the same throughout an area, but they must be the same between neighbors.

- 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.
```

Note: The area authentication command in the configuration enables authentications for all the

interfaces of the router in a particular area. You can also use the **ip ospf authentication** command under the interface to configure plain text authentication for the interface. This command can be used if a different authentication method or no authentication method is configured under the area to which the interface belongs. It overrides the authentication method configured for the area. This is useful if different interfaces that belong to the same area need to use different authentication methods

Configurations for MD5 Authentication

MD5 authentication provides higher security than plain text authentication. This method uses the MD5 algorithm to compute a hash value from the contents of the OSPF packet and a password (or key). This hash value is transmitted in the packet, along with a key ID and a non-decreasing sequence number. The receiver, which knows the same password, calculates its own hash value. If nothing in the message changes, the hash value of the receiver must match the hash value of the sender which is transmitted with the message.

The key ID allows the routers to reference multiple passwords. This makes password migration easier and more secure. For example, to migrate from one password to another, configure a password under a different key ID and remove the first key. The sequence number prevents replay attacks, in which OSPF packets are captured, modified, and retransmitted to a router. As with plain text authentication, MD5 authentication passwords do not have to be the same throughout an area. However, they do need to be the same between neighbors.

Note: Cisco recommends that you configure the **service password-encryption** command on all of your routers. This causes the router to encrypt the passwords in any display of the configuration file and protect the text copy of the router configuration from observation.

- 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.
```

Note: The **area authentication message-digest** command in this configuration enables authentications for all of the router interfaces in a particular area. You can also use the **ip ospf authentication message-digest** command under the interface to configure MD5 authentication for the specific interface. This command can be used if a different authentication method or no authentication method is configured under the area to which the interface belongs. It overrides the authentication method configured for the area. This is useful if different interfaces that belong to the same area need to use different authentication methods.

Verify

These sections provide information you can use to confirm your configurations work properly.

Verify Plain Text Authentication

Use the **show ip ospf interface** command to view the authentication type configured for an interface, as this output shows. Here, the Serial 0 interface is configured for Plain text authentication.

```
<#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
```

The **show ip ospf neighbor** command displays the neighbor table that consists of the neighbor details, as this output shows.

```
<#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
```

The **show ip route** command displays the routing table, as this output shows.

```
<#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
```

Verify MD5 Authentication

Use the **show ip ospf interface** command to view the authentication type configured for an interface, as this output shows. Here, the Serial 0 interface has been configured for MD5 authentication with key ID 1.

```
<#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
```

The **show ip ospf neighbor** command displays the neighbor table that consists of the neighbor details, as this output shows.

```
<#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#
```

The **show ip route** command displays the routing table, as this output shows.

```
<#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, 00:01:23, 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
```

Troubleshoot

These sections provide information you can use to troubleshoot your configurations. Issue the **debug ip ospf adj** command in order to capture the authentication process. This **debug** command must be issued before the neighbor relationship is established.

Note: Refer to Important Information on Debug Commands before you use the **debug** commands.

Troubleshoot Plain Text Authentication

The **deb ip ospf adj** output for R1-2503 shows when plain text authentication is successful.

```
<#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#
```

This is the output of the **debug ip ospf adj** command when there is a mismatch in the type of authentication configured on the routers. This output shows that Router R1-2503 uses type 1 authentication whereas router R2-2503 is configured for type 0 authentication. This means that Router R1-2503 is configured for plain text authentication (Type 1), whereas Router R2-2503 is configured for null authentication (Type 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.
```

This is the output of the **debug ip ospf adj** command when there is a mismatch in the authentication key (password) values. In this case, both routers are configured for plain text authentication (Type 1) but there is a mismatch in the key (password) values.

```
<#root>

R1-2503#

debug ip ospf adj

00:51:33: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication Key - Clear Text
```

Troubleshoot MD5 Authentication

This is the **debug ip ospf adj** command output for R1-2503 when MD5 authentication is successful.

<#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 0x7len 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 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 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#
```

This is the output of the **debug ip ospf adj** command when there is a mismatch in the type of authentication configured on the routers. This output shows that the router R1-2503 uses type 2 (MD5) authentication, whereas Router R2-2503 uses type 1 authentication (plain text authentication).

```
<#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.
```

This is the output of the **debug ip ospf adj** command when there is a mismatch in the key IDs that are used for authentication. This output shows that the router R1-2503 uses MD5 authentication with Key ID 1, whereas the Router R2-2503 uses MD5 authentication with Key ID 2.

```
<#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
```

This **debug ip ospf adj** command output for R1-2503 shows when both Key 1 and Key 2 for MD5 authentication are configured as part of migration.

```
<#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#
```

Related Information

- Configuring OSPF Authentication on a Virtual Link
- Why Does the show ip ospf neighbor Command Reveal Neighbors in the Init State?
- OSPF Commands
- OSPF Configuration Examples
- IP Routing Support Page
- Cisco Technical Support & Downloads