

Open Shortest Path First에서 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[일반 텍스트 인증을 위한 컨피그레이션](#)

[MD5 인증 컨피그레이션](#)

[다음을 확인합니다.](#)

[일반 텍스트 인증 확인](#)

[MD5 인증 확인](#)

[문제 해결](#)

[일반 텍스트 인증 문제 해결](#)

[MD5 인증 문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 OSPF(Open Shortest Path First) 인증을 구성하고 OSPF 인접 디바이스를 유연하게 인증할 수 있도록 하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서의 독자는 OSPF 라우팅 프로토콜의 기본 개념을 잘 알고 있어야 합니다. 또는 OSPF 라우팅 프로토콜에 대한 정보를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 2503 라우터
- Cisco IOS® Software 릴리스 12.2(27)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

배경 정보

이 문서에서는 OSPF(Open Shortest Path First) 인증에 대한 샘플 컨피그레이션을 보여 줍니다. 이 컨피그레이션을 통해 OSPF 인접 디바이스를 유연하게 인증할 수 있습니다. 라우팅 업데이트 정보를 안전하게 교환하기 위해 OSPF에서 인증을 활성화할 수 있습니다. OSPF 인증은 none(또는 null), simple 또는 MD5일 수 있습니다. 인증 방법 "없음"은 OSPF에 대해 어떤 인증도 사용되지 않으며 기본 방법입니다. 간단한 인증으로 비밀번호는 네트워크를 통해 일반 텍스트로 전달됩니다. MD5 인증에서는 암호가 네트워크를 통과하지 않습니다. MD5는 RFC 1321에 지정된 메시지 다이제스트 알고리즘입니다. MD5는 가장 안전한 OSPF 인증 모드로 간주됩니다. 인증을 구성할 때 동일한 인증 유형으로 전체 영역을 구성해야 합니다. Cisco IOS Software Release 12.0(8)에서는 인터페이스별로 인증이 지원됩니다. 이는 RFC [2328](#), [부록 D](#)에서도 언급됩니다.

 참고: 등록된 Cisco 클라이언트만 이러한 사이트와 톨에 액세스할 수 있습니다.

다음은 OSPF에서 지원되는 세 가지 인증 유형입니다.

- Null Authentication(Null 인증) - Type 0이라고도 하며, 패킷 헤더에 인증 정보가 포함되어 있지 않음을 의미합니다. 기본값입니다.
- 일반 텍스트 인증 — 유형 1이라고도 하며 간단한 일반 텍스트 비밀번호를 사용합니다.
- MD5 인증 - 유형 2라고도 하며 MD5 암호화 비밀번호를 사용합니다.

인증 설정할 필요가 없습니다. 그러나 이 설정이 적용되면 동일한 세그먼트의 모든 피어 라우터에는 동일한 비밀번호와 인증 방법이 있어야 합니다. 이 문서의 예는 일반 텍스트 및 MD5 인증에 대한 컨피그레이션을 보여줍니다.

구성

이 섹션에서는 이 문서에서 설명하는 기능을 구성하는 데 필요한 정보를 제공합니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



일반 텍스트 인증을 위한 컨피그레이션

일반 텍스트 인증은 영역 내의 디바이스가 더 안전한 MD5 인증을 지원할 수 없는 경우 사용됩니다. 일반 텍스트 인증은 프로토콜 분석기가 패킷을 캡처하고 비밀번호를 읽을 수 있는 "스니퍼 공격"에 취약하도록 인터넷워크를 방치합니다. 그러나 보안을 위해서가 아니라 OSPF 재구성을 수행할 때 유용합니다. 예를 들어, 라우터 간의 통신을 방지하기 위해 공통 브로드캐스트 네트워크를 공유하는 이전 및 최신 OSPF 라우터에서 별도의 비밀번호를 사용할 수 있습니다. 일반 텍스트 인증 비밀번호는 영역 전체에서 동일해야 할 필요는 없지만 네이버 사이에서는 동일해야 합니다.

- R2-2503
- R1-2503

R2-2503
<pre>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.</pre>
R1-2503
<pre>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.</pre>

 참고: 컨피그레이션의 [area authentication](#) 명령은 특정 영역에 있는 라우터의 모든 인터페이스에 대한 인증을 활성화합니다. 또한 인터페이스 아래의 ip ospf authentication 명령을 사용하여 인터페이스에 대한 일반 텍스트 인증을 구성할 수 있습니다. 인터페이스가 속한 영역 아래에 다른 인증 방법이 구성되어 있거나 인증 방법이 구성되어 있지 않은 경우 이 명령을 사용할 수 있습니다. 영역에 대해 구성된 인증 방법을 재정의합니다. 이는 동일한 영역에 속하는 서로 다른 인터페이스에서 서로 다른 인증 방법을 사용해야 하는 경우에 유용합니다

MD5 인증 컨피그레이션

MD5 인증은 일반 텍스트 인증보다 높은 보안을 제공합니다. 이 방법은 MD5 알고리즘을 사용하여 OSPF 패킷의 내용 및 비밀번호(또는 키)에서 해시 값을 계산합니다. 이 해시 값은 키 ID 및 비감소 시퀀스 번호와 함께 패킷에서 전송됩니다. 동일한 비밀번호를 알고 있는 수신자는 자신의 해시 값을 계산합니다. 만약 메시지의 어떤 것도 변하지 않는다면, 수신자의 해시 값은 메시지와 함께 전송되는 송신자의 해시 값과 일치해야 한다.

키 ID를 사용하면 라우터가 여러 비밀번호를 참조할 수 있습니다. 이렇게 하면 비밀번호 마이그레이션이 더욱 쉽고 안전해집니다. 예를 들어 한 비밀번호에서 다른 비밀번호로 마이그레이션하려면 다른 키 ID로 비밀번호를 구성하고 첫 번째 키를 제거합니다. 시퀀스 번호는 OSPF 패킷이 캡처, 수정 및 라우터로 재전송되는 반복 공격을 방지합니다. 일반 텍스트 인증과 마찬가지로, MD5 인증 비밀번호는 영역 전체에서 동일해야 합니다. 그러나, 그들은 이웃들 사이에서 똑같은 필요가 있다.

 참고: 모든 라우터에서 [service password-encryption](#) 명령을 구성하는 것이 좋습니다. 이로 인해 라우터는 구성 파일의 모든 표시에서 비밀번호를 암호화하고 라우터 구성의 텍스트 복사본을 관찰로부터 보호합니다.

- 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.
```

 참고: 이 컨피그레이션의 [area authentication message-digest](#) 명령은 특정 영역의 모든 라우터 인터페이스에 대한 인증을 활성화합니다. 인터페이스 아래에서 [ip ospf authentication message-digest](#) 명령을 사용하여 특정 인터페이스에 대한 MD5 인증을 구성할 수도 있습니다. 인터페이스가 속한 영역 아래에 다른 인증 방법이 구성되어 있거나 인증 방법이 구성되어 있지 않은 경우 이 명령을 사용할 수 있습니다. 영역에 대해 구성된 인증 방법을 재정의합니다. 이는 동일한 영역에 속하는 서로 다른 인터페이스에서 서로 다른 인증 방법을 사용해야 하는 경우에 유용합니다.

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일반 텍스트 인증 확인

이 출력에 표시된 것처럼 인터페이스에 대해 구성된 인증 유형을 보려면 `show ip ospf interface` 명령을 사용합니다. 여기서 Serial 0 인터페이스는 일반 텍스트 인증을 위해 구성됩니다.

```
<#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` 명령은 이 출력에 표시된 대로 네이버 세부 정보로 구성된 네이버 테이블을 표시합니다.

```
<#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

이 출력에 표시된 것처럼 `show ip route` 명령은 라우팅 테이블을 표시합니다.

```
<#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
```

MD5 인증 확인

이 출력에 표시된 것처럼 인터페이스에 대해 구성된 인증 유형을 보려면 `show ip ospf interface` 명령을 사용합니다. 여기서 Serial 0 인터페이스는 키 ID가 "1"인 MD5 인증을 위해 구성되었습니다.

<#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` 명령은 이 출력에 표시된 대로 네이버 세부 정보로 구성된 네이버 테이블을 표시합니다.

<#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#

이 출력에 표시된 것처럼 show ip route 명령은 라우팅 테이블을 표시합니다.

```
<#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
```

문제 해결

이 섹션에서는 컨피그레이션 트러블슈팅에 사용할 수 있는 정보를 제공합니다. 인증 프로세스를 캡처하기 위해 debug ip ospf adj 명령을 실행합니다. 이 디버그 명령은 네이버 관계를 설정하기 전에 실행해야 합니다.



참고: [debug 명령을 사용하기 전에 Debug 명령](#)에 대한 중요 정보를 참조하십시오.

일반 텍스트 인증 문제 해결

R1-2503에 대한 deb ip ospf adj 출력은 일반 텍스트 인증이 성공한 경우를 보여줍니다.

```
<#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#

```

라우터에 구성된 인증 유형이 일치하지 않을 때 debug ip ospf adj 명령의 출력입니다. 이 출력은 라우터 R1-2503이 유형 1 인증을 사용하는 반면 라우터 R2-2503은 유형 0 인증을 위해 구성되었음을 보여줍니다. 즉, 라우터 R1-2503은 일반 텍스트 인증(유형 1)으로 구성된 반면 라우터 R2-2503은 null 인증(유형 0)으로 구성됩니다.

```
<#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.
```

인증 키(비밀번호) 값이 일치하지 않을 때 debug ip ospf adj 명령의 출력입니다. 이 경우 두 라우터 모두 일반 텍스트 인증(Type 1)으로 구성되지만 키(비밀번호) 값이 일치하지 않습니다.

```
<#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 인증 문제 해결

MD5 인증에 성공한 경우 R1-2503에 대한 debug ip ospf adj 명령 출력입니다.

```
<#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#

```

라우터에 구성된 인증 유형이 일치하지 않을 때 debug ip ospf adj 명령의 출력입니다. 이 출력은 라우터 R1-2503이 유형 2(MD5) 인증을 사용하는 반면 라우터 R2-2503은 유형 1 인증(일반 텍스트 인증)을 사용함을 보여줍니다.

```
<#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.
```

인증에 사용되는 키 ID가 일치하지 않을 때 debug ip ospf adj 명령의 출력입니다. 이 출력은 라우터 R1-2503이 키 ID 1의 MD5 인증을 사용하는 반면 라우터 R2-2503은 키 ID 2의 MD5 인증을 사용함을 보여줍니다.

<#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
```

R1-2503에 대한 이 debug ip ospf adj 명령 출력은 MD5 인증을 위한 키 1과 키 2가 모두 마이그레이션의 일부로 구성된 경우를 보여줍니다.

<#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#
```

관련 정보

- [가상 링크에서 OSPF 인증 구성](#)
- [show ip ospf neighbor 명령이 초기화 상태의 인접 디바이스를 표시하는 이유는 무엇입니까?](#)
- [OSPF 명령](#)
- [OSPF 컨피그레이션 예](#)
- [IP 라우팅 지원 페이지](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.