Konfigurieren Sie zuerst die Authentifizierung in "Open Shortest Path".

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die OSPF-Authentifizierung (Open Shortest Path First) konfiguriert wird und wie OSPF-Nachbarn flexibel authentifiziert werden können.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments müssen mit den grundlegenden Konzepten des OSPF-Routing-Protokolls vertraut sein. Weitere Informationen zum OSPF-Routing-Protokoll finden Sie unter oder.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen.

- Cisco 2503 Router
- Cisco IOS®-Softwareversion 12.2(27)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Dieses Dokument zeigt Beispielkonfigurationen für die OSPF-Authentifizierung (Open Shortest Path First), die eine flexible Authentifizierung von OSPF-Nachbarn ermöglicht. Sie können die Authentifizierung in OSPF aktivieren, um Routing-Aktualisierungsinformationen sicher auszutauschen. Die OSPF-Authentifizierung kann none (oder null), simple (Einfach) oder MD5 sein. Die Authentifizierungsmethode none (Keine) bedeutet, dass keine Authentifizierung für OSPF verwendet wird und es sich um die Standardmethode handelt. Bei der einfachen Authentifizierung wird das Passwort im Klartext über das Netzwerk übertragen. Bei MD5-Authentifizierung wird das Kennwort nicht über das Netzwerk weitergeleitet. MD5 ist ein in RFC 1321 definierter Message-Digest-Algorithmus. MD5 gilt als der sicherste OSPF-Authentifizierungsmodus. Wenn Sie die Authentifizierung konfigurieren, müssen Sie einen gesamten Bereich mit demselben Authentifizierungstyp konfigurieren. Mit Cisco IOS® Software, Version 12.0(8), wird die Authentifizierung schnittstellenweise unterstützt. Dies wird auch in RFC 2328, Anhang D erwähnt. Diese Funktion wurde in "Cisco Bug ID CSCdk33792" hinzugefügt.

> **Anmerkung:** Nur registrierte Cisco Kunden können auf diese Websites und Tools zugreifen.

Dies sind die drei verschiedenen Authentifizierungstypen, die von OSPF unterstützt werden.

- **Null Authentication (**Authentifizierung Null) - Dies wird auch als Typ 0 bezeichnet und bedeutet, dass im Paket-Header keine Authentifizierungsinformationen enthalten sind. Dies ist die Standardeinstellung.
- **Plain Text Authentication** - Dies wird auch als Typ 1 bezeichnet und verwendet einfache Klartext-Passwörter.
- **MD5-Authentifizierung** - Dies wird auch als Typ 2 bezeichnet und verwendet kryptografische MD5-Kennwörter.

Die Authentifizierung muss nicht festgelegt werden. Wenn sie jedoch festgelegt ist, müssen alle Peer-Router im gleichen Segment über dasselbe Kennwort und dieselbe Authentifizierungsmethode verfügen. Die Beispiele in diesem Dokument zeigen Konfigurationen für die Nur-Text- und MD5-Authentifizierung.

Konfigurieren

In diesem Abschnitt finden Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet.

Netzwerkdiagramm

Konfigurationen für die Nur-Text-Authentifizierung

Die Klartextauthentifizierung wird verwendet, wenn Geräte in einem Bereich die sicherere MD5-Authentifizierung nicht unterstützen. Bei der Nur-Text-Authentifizierung ist das Internetwork anfällig für einen "Sniffer-Angriff", bei dem Pakete von einem Protokollanalysator erfasst und die Passwörter gelesen werden können. Sie ist jedoch bei der OSPF-Neukonfiguration nützlich, anstatt für die Sicherheit. Beispielsweise können auf älteren und neueren OSPF-Routern, die ein gemeinsames Broadcast-Netzwerk nutzen, separate Kennwörter verwendet werden, um die Kommunikation zwischen Routern zu verhindern. Authentifizierungskennwörter im Klartext müssen in einem Bereich nicht identisch sein, sondern zwischen Nachbarn identisch sein.

- 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. ! route
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
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. ! route
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.
```

Anmerkung: Der Befehl area authentication in der Konfiguration ermöglicht die Authentifizierung aller Schnittstellen des Routers in einem bestimmten Bereich. Sie können auch den Befehl **ip ospf authentication** unter der Schnittstelle verwenden, um die Nur-Text-Authentifizierung für die Schnittstelle zu konfigurieren. Dieser Befehl kann verwendet werden, wenn in dem Bereich, zu dem die Schnittstelle gehört, eine andere Authentifizierungsmethode oder keine Authentifizierungsmethode konfiguriert ist. Die für den Bereich konfigurierte Authentifizierungsmethode wird überschrieben. Dies ist nützlich, wenn verschiedene Schnittstellen, die zum gleichen Bereich gehören, unterschiedliche Authentifizierungsmethoden verwenden müssen

Konfigurationen für MD5-Authentifizierung

Die MD5-Authentifizierung bietet eine höhere Sicherheit als die Nur-Text-Authentifizierung. Diese Methode verwendet den MD5-Algorithmus, um einen Hash-Wert aus dem Inhalt des OSPF-Pakets und einem Kennwort (oder Schlüssel) zu berechnen. Dieser Hashwert wird zusammen mit einer Schlüssel-ID und einer nicht abnehmenden Sequenznummer im Paket übertragen. Der Empfänger, der dasselbe Passwort kennt, berechnet seinen eigenen Hash-Wert. Wenn sich nichts in der Nachricht ändert, muss der Hashwert des Empfängers mit dem Hashwert des Senders übereinstimmen, der mit der Nachricht übertragen wird.

Mit der Schlüssel-ID können die Router auf mehrere Passwörter verweisen. Dadurch wird die Passwortmigration einfacher und sicherer. Um beispielsweise von einem Kennwort zu einem anderen zu migrieren, konfigurieren Sie ein Kennwort unter einer anderen Schlüssel-ID, und entfernen Sie den ersten Schlüssel. Die Sequenznummer verhindert Replay-Angriffe, bei denen OSPF-Pakete erfasst, geändert und erneut an einen Router übertragen werden. Wie bei der Nur-Text-Authentifizierung müssen MD5-Authentifizierungskennwörter in einem Bereich nicht identisch

sein. Sie müssen jedoch zwischen den Nachbarn identisch sein.

> **Anmerkung:** Cisco empfiehlt, den Befehl service password-encryption auf allen Routern zu konfigurieren. Dadurch verschlüsselt der Router die Kennwörter in jeder Anzeige der Konfigurationsdatei und schützt die Textkopie der Router-Konfiguration vor Beobachtung.

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

> **Anmerkung:** Der Befehl area authentication message-digest in dieser Konfiguration ermöglicht die Authentifizierung aller Router-Schnittstellen in einem bestimmten Bereich. Sie können auch den Befehl ip ospf authentication message-digest unter der Schnittstelle verwenden, um die MD5-Authentifizierung für die jeweilige Schnittstelle zu konfigurieren. Dieser Befehl kann verwendet werden, wenn in dem Bereich, zu dem die Schnittstelle gehört, eine andere Authentifizierungsmethode oder keine Authentifizierungsmethode

konfiguriert ist. Die für den Bereich konfigurierte Authentifizierungsmethode wird überschrieben. Dies ist nützlich, wenn verschiedene Schnittstellen, die zum gleichen Bereich gehören, unterschiedliche Authentifizierungsmethoden verwenden müssen.

Überprüfung

In diesen Abschnitten finden Sie Informationen zur Überprüfung der ordnungsgemäßen Konfiguration.

Nur-Text-Authentifizierung überprüfen

Verwenden Sie den Befehl **show ip ospf interface**, um den für eine Schnittstelle konfigurierten Authentifizierungstyp anzuzeigen, wie diese Ausgabe zeigt. Hier ist die serielle 0-Schnittstelle für die Nur-Text-Authentifizierung konfiguriert.

```
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
```

Der Befehl **show ip ospf neighbor** zeigt die Nachbartabelle an, die aus den Nachbardetails besteht, wie diese Ausgabe zeigt.

```
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
```

Der Befehl **show ip route** zeigt die Routing-Tabelle an, wie in dieser Ausgabe dargestellt.

```
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-Authentifizierung überprüfen

Verwenden Sie den Befehl **show ip ospf interface**, um den für eine Schnittstelle konfigurierten Authentifizierungstyp anzuzeigen, wie diese Ausgabe zeigt. Hier wurde die Schnittstelle "Serial 0" für die MD5-Authentifizierung mit der Schlüssel-ID "1" konfiguriert.

```
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
```

Der Befehl **show ip ospf neighbor** zeigt die Nachbartabelle an, die aus den Nachbardetails besteht, wie diese Ausgabe zeigt.

```
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#
```

Der Befehl **show ip route** zeigt die Routing-Tabelle an, wie in dieser Ausgabe dargestellt.

```
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
```

Fehlerbehebung

In diesen Abschnitten finden Sie Informationen zur Fehlerbehebung bei Ihren Konfigurationen.

Führen Sie den Befehl **debug ip ospf adj** aus, um den Authentifizierungsprozess zu erfassen. Dieser **Debug**-Befehl muss ausgegeben werden, bevor die Nachbarbeziehung hergestellt wird.

> **Anmerkung:** Weitere Informationen zu Debug-Befehlen finden Sie vor der Verwendung der **Debug-**Befehle unter Wichtige Informationen.

Problembehandlung bei der unverschlüsselten Authentifizierung

Die **deb ip ospf adj-**Ausgabe für R1-2503 zeigt an, wenn die Nur-Text-Authentifizierung erfolgreich ist.

```
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#
```

Dies ist die Ausgabe des Befehls **debug ip ospf adj**, wenn der auf den Routern konfigurierte Authentifizierungstyp nicht übereinstimmt. Diese Ausgabe zeigt, dass der Router R1-2503 die

Typ-1-Authentifizierung verwendet, während der Router R2-2503 für die Typ-0-Authentifizierung konfiguriert ist. Das bedeutet, dass der Router R1-2503 für die Nur-Text-Authentifizierung (Typ 1) konfiguriert ist, während der Router R2-2503 für die Null-Authentifizierung (Typ 0) konfiguriert ist.

```
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.
```

Dies ist die Ausgabe des Befehls **debug ip ospf adj**, wenn die Authentifizierungsschlüsselwerte (Kennwort) nicht übereinstimmen. In diesem Fall sind beide Router für die Nur-Text-Authentifizierung (Typ 1) konfiguriert, die Schlüssel-(Kennwort-)Werte stimmen jedoch nicht überein.

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

Fehlerbehebung bei MD5-Authentifizierung

Dies ist die Ausgabe des Befehls **debug ip ospf adj** für R1-2503, wenn die MD5-Authentifizierung erfolgreich war.

```
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#
```

Dies ist die Ausgabe des Befehls **debug ip ospf adj**, wenn der auf den Routern konfigurierte Authentifizierungstyp nicht übereinstimmt. Diese Ausgabe zeigt, dass der Router R1-2503 die Typ-2-Authentifizierung (MD5) verwendet, während der Router R2-2503 die Typ-1-Authentifizierung (Klartext-Authentifizierung) verwendet.

```
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.
```

Dies ist die Ausgabe des Befehls **debug ip ospf adj**, wenn die Schlüssel-IDs für die Authentifizierung nicht übereinstimmen. Diese Ausgabe zeigt, dass der Router R1-2503 MD5-Authentifizierung mit Schlüssel-ID 1 verwendet, während der Router R2-2503 MD5-Authentifizierung mit Schlüssel-ID 2 verwendet.

```
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
```

Die Ausgabe des Befehls **debug ip ospf adj** für R1-2503 zeigt, wenn sowohl Key 1 als auch Key 2 für die MD5-Authentifizierung als Teil der Migration konfiguriert wurden.

```
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#
```

Zugehörige Informationen

- Konfigurieren der OSPF-Authentifizierung auf einem virtuellen Link
- Warum zeigt der show ip ospf neighbor-Befehl offenbart Nachbarn im Init-Zustand?
- OSPF-Befehle
- OSPF-Konfigurationsbeispiele
- IP Routing-Support-Seite
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.