OSPF の認証のための設定例

目次

概要

この文書では、OSPF 隣接ルータを柔軟に認証できる Open Shortest Path First（OSPF）認証の設定例を説明します。 安全な方法でルーティング アップデート情報を交換するために、OSPF で認証をイネーブルにすることができます。 OSPF 認証は、None（またはヌル）、Simple、または MD5 のいずれかです。 認証方式「None」は、OSPF で認証が使用されないことを意味します。これがデフォルトの方式です。 Simple 認証では、パスワードはクリアテキストでネットワークを通過します。 MD5 認証では、パスワードはネットワークを通過しません。 MD5 は RFC 1321 で規定されたメッセージ ダイジェスト アルゴリズムです。 MD5 は最も安全な OSPF 認証のモードと見なされます。 認証を設定する際には、エリア全体を同じタイプの認証で設定する必要があります。 Cisco IOS® ソフトウェア リリース 12.0(8) 以降、認証はインターフェイス単位でサポートされています。 これは RFC 2328 、付録 D にも記載されています。 この機能は、Cisco Bug ID CSCdk33792（登録ユーザ専用）で追加されます。

前提条件

要件

この文書の読者は、OSPF ルーティング プロトコルの基本概念に精通している必要があります。OSPF ルーティング プロトコルの詳細については、Open Shortest Path First のマニュアルを参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 2503 ルータ
- Cisco IOS ソフトウェア リリース 12.2(27)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

次に、OSPF でサポートされている 3 種類の認証を示します。

- **ヌル認証** - タイプ 0 とも呼ばれ、パケット ヘッダーには認証情報が含まれていないことを意味します。 これがデフォルト設定です。
- **平文認証** - タイプ 1 とも呼ばれ、シンプルなクリアテキスト パスワードを使用しています。
- **MD5 認証** - タイプ 2 とも呼ばれ、MD5 暗号化パスワードを使用しています。

認証を設定する必要はありません。 しかし認証を設定した場合、同じセグメント上のすべてのピア ルータで、パスワードと認証方式が同じである必要があります。 この文書の例では、平文認証と MD5 認証の両方の設定を示します。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報について記載しています。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool を使用してください（登録ユーザ専用）。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

非暗号化テキスト認証のための設定

平文認証は、より安全度が高い MD5 認証をエリア内のデバイスがサポートできない場合に使用されます。 平文認証の場合、インターネットワークは「スニファ攻撃」に対する脆弱性が残されたままです。この場合、プロトコル アナライザによってパケットが捕捉され、パスワードが読み取られる可能性があります。 しかし平文認証は、セキュリティのためよりもむしろ、OSPF の再設定を実行している場合に有効です。 たとえば、共通のブロードキャスト ネットワークを共有している古い OSPF ルータと新しい OSPF ルータで、別のパスワードを使用して、それらの相互の会話を防止できます。 平文認証パスワードはエリア全体で同一である必要はありませんが、隣接

ルータ間では同じである必要があります。

- 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.
```

注: 設定内の area authentication コマンドによって、特定エリア内のルータのすべてのインターフェイスに対し、認証がイネーブルになります。 インターフェイスの基で ip ospf authentication コマンドを使用し、そのインターフェイスに対して平文認証を設定することもできます。 インターフェイスが属しているエリアで別の認証方式が使われている場合、または認証方式が使われていない場合でも、このコマンドを使用できます。 このコマンドは、その エリアに設定されている認証方式を設定し直します。 これは、同じエリアに属している別のインターフェイスで異なる認証方式を使用する必要がある場合に有効です。

MD5 認証の設定

MD5 認証では、平文認証よりも安全度が高いセキュリティが提供されます。 この方式では、MD5 アルゴリズムを使用して、OSPF パケットとパスワード（またはキー）の内容からハッシュ値を計算します。 このハッシュ値は、キー ID と減少しないシーケンス番号とともに、パケット内に置かれて送信されます。 同じパスワードを知っている受信側は、独自でハッシュ値を計算します。 メッセージの内容が変更されていない場合、受信側のハッシュ値は、メッセージと一緒に送信された送信側のハッシュ値と一致します。

キー ID により、ルータは複数のパスワードを参照できます。 このため、パスワードのマイグレーションが簡単になり、安全度も高くなります。 たとえば、あるパスワードから別のパスワードにマイグレーションする場合には、別のキー ID でパスワードを設定した後で、最初のキーを削除します。 シーケンス番号は、リプレイ攻撃を防止します。この攻撃では OSPF パケットの捕捉と変更が行われた後、ルータに再送信されます。 平文認証と同様、MD5 認証パスワードはエリア

全体で同じである必要はありません。 しかし、隣接ルータ間では同じである必要があります。

注: すべてのルータ上で service password-encryption コマンドを設定することをお勧めします。これにより、設定ファイルが表示される場合、ルータによってパスワードが暗号化され、ルータの設定のテキスト コピーを見ることによってパスワードを知られることを防ぎます。

- 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.
```

注: 設定内の area authentication message-digest コマンドによって、特定エリア内のルータのすべてのインターフェイスに対し、認証がイネーブルになります。 インターフェイスで ip ospf authentication message-digest コマンドを使用し、その特定のインターフェイスに対して MD5 認証を設定することもできます。 インターフェイスが属しているエリアで別の認証方式が使われている場合、または認証方式が使われていない場合でも、このコマンドを使用できます。 このコマンドは、そのエリアに設定されている認証方式を設定し直します。 これは、同じエリアに属している別のインターフェイスで異なる認証方式を使用する必要がある場合に有効です。

確認

このセクションでは、設定が正しく動作することを確認するための情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

平文認証の確認

次の出力に示すように、show ip ospf interface コマンドを使用して、インターフェイスに設定さ

れた認証タイプを表示します。 ここでは、シリアル 0 インターフェイスは平文認証用に設定されています。

```
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 コマンドは、次の出力に示すように、隣接ルータの詳細情報から構成されている隣接ルータ テーブルを表示します。

```
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 コマンドは、次の出力に示すように、ルーティング テーブルを表示します。

```
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
```

MD5 認証の確認

次の出力に示すように、show ip ospf interface コマンドを使用して、インターフェイスに設定された認証タイプを表示します。 この場合、シリアル 0 インターフェイスは、キー ID「1」を使った MD5 認証が設定されています。

```
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 コマンドは、次の出力に示すように、隣接ルータの詳細情報から構成されている隣接ルータ テーブルを表示します。

```
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 コマンドは、次の出力に示すように、ルーティング テーブルを表示します。

```
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
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。 認証プロセスを取り込むには、**debug ip ospf adj コマンド**を発行します。 この debug コマンドは、隣接ルータ

との関係を確立する前に実行する必要があります。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

平文認証のトラブルシューティング

R1-2503 に対するこの **debug ip ospf adj** 出力は、平文認証が成功した場合を示しています。

```
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#
```

これは、ルータに設定されている認証タイプが不一致である場合の、**debug ip ospf adj** コマンドの出力です。 この出力は、ルータ R1-2503 がタイプ 1 の認証を使用し、ルータ R2-2503 がタイプ 0 の認証用に設定されていることを示しています。 つまり、ルータ R1-2503 に平文認証（タイプ 1）が設定されており、ルータ R2-2503 にヌル認証（タイプ 0）が設定されています。

```
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.
```

これは、認証キー（パスワード）値が不一致である場合の、 **debug ip ospf adj** コマンドの出力です。 この場合、両方のルータにプレーン テキスト認証（タイプ 1）が設定されていますが、キー（パスワード）の値が一致していません。

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

MD5 認証のトラブルシューティング

これは MD5 認証が成功したときの、R1-2503 の **debug ip ospf adj** コマンドの出力です。

```
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#
```

これは、ルータに設定されている認証タイプが不一致である場合の、**debug ip ospf adj** コマンドの出力です。 この出力は、ルータ R1-2503 がタイプ 2 (MD5) 認証を使用し、ルータ R2-2503 がタイプ 1 の認証 (平文認証) を使用していることを示しています。

```
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.
```

これは、認証に使用するキー ID の不一致がある場合の、**debug ip ospf adj** コマンドの出力です。 この出力は、ルータ R1-2503 がキー ID 1 で MD5 認証を使用し、ルータ R2-2503 がキー ID 2 で MD5 認証を使用することを示しています。

```
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
```

R1-2503 用のこの **debug ip ospf adj コマンド**の出力は、MD5 認証のキー 1 とキー 2 が、マイグレーションの一部として設定されていることを示しています。

```
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#
```

関連情報

- 仮想リンクでの OSPF 認証設定
- show ip ospf neighbor コマンドが初期状態のネイバーを表示する理由
- OSPF コマンド
- OSPF 設定例
- OSPF テクノロジーに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems