Exemple de configuration de l'authentification en OSPF

Contenu

Introduction

Ce document montre des exemples de configuration de l'authentification Open Shortest Path First (OSPF) dont la flexibilité permet d'authentifier des voisins OSPF. Vous pouvez activer l'authentification OSPF afin d'échanger des informations de mise à niveau de routage d'une manière sécurisée. L'authentification OSPF peut être de type « none » (ou null), « simple » ou « MD5 ». La méthode d'authentification « none » signifie qu'aucune authentification n'est utilisée pour l'OSPF. Il s'agit de la méthode par défaut. Avec l'authentification simple, le mot de passe est transmis en texte clair sur le réseau. Avec l'authentification MD5, le mot de passe n'est pas transmis sur le réseau. MD5 est un algorithme Message-Digest spécifié dans la RFC 1321. MD5 est considéré comme le mode d'authentification OSPF le plus sécurisé. Quand vous configurez l'authentification, vous devez configurer une zone entière avec le même type d'authentification. À partir de la version de logiciel 12.0(8) de Cisco IOS®, l'authentification est prise en charge sur base d'interface. Ce point est également mentionné dans la RFC 2328 , annexe D. Cette fonctionnalité figure dans l'ID de bogue Cisco CSCdk33792 (clients enregistrés uniquement).

Conditions préalables

Conditions requises

Les lecteurs de ce document doivent connaître les concepts de base du protocole de routage OSPF. Consultez la documentation Open Shortest Path First pour obtenir des informations sur le protocole de routage OSPF.

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- Routeurs Cisco 2503
- Logiciel Cisco IOS Version 12.2(27)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Voici les trois types d'authentifications pris en charge par OSPF.

- **Authentification nulle** : également appelée Type 0, cette authentification signifie qu'aucune information d'authentification n'est incluse dans l'en-tête de paquet. Il s'agit de la valeur par défaut.
- **Authentification en texte brut** : également appelée Type 1, cette authentification utilise des mots de passe simples en texte brut.
- **Authentification MD5** : également appelée Type 2, cette authentification utilise des mots de passe MD5 chiffrés.

L'authentification n'a pas besoin d'être définie. Cependant, si elle est définie, tous les routeurs homologues du même segment doivent avoir le même mot de passe et la même méthode d'authentification. Les exemples de ce document illustrent les configurations d'une authentification en texte brut et d'une authentification MD5.

Configurer

Cette section vous présente les informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'outil de recherche de commande (clients enregistrés uniquement).

Diagramme du réseau

Ce document utilise cette configuration du réseau.

Configurations pour l'authentification en texte brut

L'authentification en texte brut est utilisée quand les périphériques d'une zone ne prennent pas en charge l'authentification MD5 plus sécurisée. L'authentification en texte brut rend l'interréseau vulnérable à une « attaque de renifleur » (sniffer attack) dans laquelle les paquets sont capturés par un analyseur de protocole qui permet de lire les mots de passe. Cette authentification est toutefois utile lorsque vous effectuez une reconfiguration OSPF, et non pour des raisons de sécurité. Par exemple, des mots de passe distincts peuvent être utilisés sur des routeurs OSPF plus anciens et plus récents qui partagent un réseau de diffusion commun afin de les empêcher de parler entre eux. Les mots de passe d'authentification en texte brut n'ont pas besoin d'être identiques au sein d'une zone, mais ils doivent l'être entre voisins.

- 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.
```

Remarque: La commande area authentication de la configuration active l'authentification pour toutes les interfaces du routeur dans une zone particulière. Vous pouvez également utiliser la commande ip ospf authentication sous l'interface afin de configurer l'authentification en texte brut pour l'interface. Cette commande peut être utilisée si une méthode d'authentification différente ou aucune méthode d'authentification n'est configurée sous la zone à laquelle l'interface appartient. Elle remplace la méthode d'authentification configurée pour la zone. Cela est utile si diverses

interfaces appartenant à la même zone ont besoin d'utiliser des méthodes d'authentification différentes.

Configurations pour l'authentification MD5

L'authentification MD5 offre une plus grande sécurité que l'authentification en texte brut. Cette méthode utilise l'algorithme MD5 pour calculer une valeur de hachage à partir du contenu du paquet OSPF, ainsi qu'un mot de passe (ou clé). Cette valeur de hachage est transmise dans le paquet, avec un ID de clé et un numéro de séquence non décroissant. Le récepteur, qui connaît le même mot de passe, calcule sa propre valeur de hachage. Si rien ne change dans le message, la valeur de hachage du récepteur doit correspondre à la valeur de hachage de l'expéditeur qui est transmise avec le message.

L'ID de clé permet aux routeurs de référencer plusieurs mots de passe. Ceci facilite la migration des mot de passe et la rend plus sécurisée. Par exemple, pour migrer d'un mot de passe à un autre, configurez un mot de passe sous un ID de clé différent, puis supprimez la première clé. Le numéro de séquence empêche les attaques par relecture, dans lesquelles les paquets OSPF sont capturés, modifiés et retransmis à un routeur. Comme avec l'authentification en texte brut, il n'est pas nécessaire que les mots de passe de l'authentification MD5 soient identiques dans l'intégralité d'une zone. Cependant, ils doivent être identiques entre voisins.

Remarque: Cisco recommande que vous configuriez la commande service password-encryption sur tous les routeurs. Le routeur chiffre ainsi les mots de passe dans n'importe quelle affichage du fichier de configuration et empêche qu'ils soient appris grâce à l'observation de la copie du texte de la configuration du routeur.

- 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.
```

Remarque: La commande area authentication message-digest dans cette configuration active l'authentification pour toutes les interfaces du routeur dans une zone spécifique. Vous pouvez également utiliser la commande ip ospf authentication message-digest sous l'interface pour configurer l'authentification MD5 pour l'interface spécifique. Cette commande peut être utilisée si une méthode d'authentification différente ou aucune méthode d'authentification n'est configurée sous la zone à laquelle l'interface appartient. Elle remplace la méthode d'authentification configurée pour la zone. Cela est utile si diverses interfaces appartenant à la même zone ont besoin d'utiliser des méthodes d'authentification différentes.

Vérifier

Ces sections fournissent des informations qui vous permettront de vérifier que vos configurations fonctionnent correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Vérifier l'authentification en texte brut

Utilisez la commande show ip ospf interface pour afficher le type d'authentification configuré pour une interface, comme le montre l'exemple suivant. Ici, l'interface Serial 0 est configurée pour l'authentification en texte brut.

```
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
```

La commande show ip ospf neighbor affiche la table de voisinage, laquelle contient des informations détaillées sur les voisins, comme le montre l'exemple suivant.

```
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
```

La commande show ip route affiche la table de routage, comme le montre l'exemple suivant.

```
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
```

Vérifier l'authentification MD5

Utilisez la commande show ip ospf interface pour afficher le type d'authentification configuré pour une interface, comme le montre l'exemple suivant. Ici, l'interface Serial 0 a été configurée pour l'authentification MD5 avec l'ID de clé « 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
```

La commande show ip ospf neighbor affiche la table de voisinage, laquelle contient des informations détaillées sur les voisins, comme le montre l'exemple suivant.

```
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#
```

La commande show ip route affiche la table de routage, comme le montre l'exemple suivant.

```
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
```

Dépanner

Ces sections fournissent des informations que vous pouvez utiliser pour dépanner vos configurations. Émettez la commande **debug ip ospf adj** afin de capturer le processus d'authentification. Cette commande **debug** doit être émise avant que la relation de voisinage ne soit établie.

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Dépanner une authentification en texte brut

Le résultat de la commande **deb ip ospf adj** pour R1-2503 indique si l'authentification en texte brut est réussie.

```
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#
```

Voici la sortie de la commande **debug ip ospf adj** lorsqu'il y a une erreur de correspondance dans le type d'authentification configuré sur les routeurs. Cette sortie montre que le routeur R1-2503 utilise l'authentification de type 1 tandis que le routeur R2-2503 est configuré pour l'authentification de type 0. Cela signifie que le routeur R1-2503 est configuré pour l'authentification en texte brut (type 1) tandis que le routeur R2-2503 est configuré pour l'authentification nulle (type 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.
```

Voici la sortie de la commande **debug ip ospf adj** lorsque la valeur des clés d'authentification (mots de passe) ne correspond pas. Dans le cas présent, les deux routeurs sont configurés pour l'authentification en texte brut (type 1) mais il y a une erreur de correspondance dans la valeur des clés (mots de passe).

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

Dépanner une authentification MD5

Voici le résultat de la commande **debug ip ospf adj** pour R1-2503 lorsque l'authentification MD5 est réussie.

```
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#
```

Voici la sortie de la commande **debug ip ospf adj** lorsqu'il y a une erreur de correspondance dans le type d'authentification configuré sur les routeurs. Cette sortie montre que le routeur R1-2503 utilise l'authentification de type 2 (MD5), tandis que le routeur R2-2503 utilise l'authentification de type 1 (authentification en texte brut).

```
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.
```

Voici la sortie de la commande **debug ip ospf adj** lorsqu'il y a une erreur de correspondance dans les ID de clé utilisés pour l'authentification. Cette sortie montre que le routeur R1-2503 utilise l'authentification MD5 avec l'ID de clé 1, tandis que le routeur R2-2503 utilise l'authentification MD5 avec l'ID de clé 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
```

Le résultat de cette commande **debug ip ospf adj** pour R1-2503 montre quand la clé 1 et la clé 2 pour l'authentification MD5 sont configurées en tant qu'élément de la migration.

```
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#
```

Informations connexes

- Configuration de l'authentification OSPF sur une liaison virtuelle
- Pourquoi la commande show ip ospf neighbor révèle-t-elle les voisins en état d'initialisation ?
- Commandes OSPF
- Exemples de configuration OSPF
- Page d'assistance technologique OSPF

- Support et documentation techniques - Cisco Systems