

Exemple de configuration de la liaison virtuelle OSPFv3

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit un exemple sur configurer les liaisons virtuelles dans la version 3 (OSPFv3) de protocole OSPF. OSPFv3 examine la version 2 OSPF pour fournir le support pour l'IPv6 conduisant des préfixes et le plus de grande taille des adresses d'IPv6.

Pour chaque liaison virtuelle, un datablock principal des informations relatives à la sécurité est créé pour la liaison virtuelle. Puisqu'un socket sécurisé doit être ouvert sur chaque interface, il y aura un datablock correspondant des informations relatives à la sécurité pour chaque interface dans la zone de transit. L'état sécurisé de socket est maintenu dans le datablock des informations relatives à la sécurité de l'interface. Le champ d'état dans le datablock principal des informations relatives à la sécurité reflète l'état du tout les sécurisent des sockets ouverts pour la liaison virtuelle. Si tout les sécurisez les sockets sont EN HAUSSE, alors l'état de Sécurité pour la liaison virtuelle sera placé à.

Les paquets ont envoyé en fonction une liaison virtuelle avec IPsec doivent utiliser la source et les adresses de destination prédéterminées. La première adresse locale trouvée dans le LSA du l'intra-zone-préfixe du routeur pour la zone est utilisée comme adresse source. Cette adresse source est enregistrée dans la structure de données de zone et utilisé quand sécurisez les sockets sont ouverts et des paquets envoyé au-dessus de la liaison virtuelle. La liaison virtuelle pas transition à l'état point par point jusqu'à ce qu'une adresse source soit sélectionnée. En outre, quand l'adresse source ou de destination change, les précédents sécurisent des sockets doivent être fermés et nouveau sécurisez les sockets ouverts.

Cet exemple de configuration utilise la commande d'[area virtual-link](#) de définir une liaison virtuelle OSPF dans le mode de configuration du routeur.

Remarque: Chaque voisin de liaison virtuelle doit inclure l'ID de zone de transit et l'ID de routeur voisin correspondant de liaison virtuelle pour qu'une liaison virtuelle soit correctement configurée. Utilisez la commande EXEC de [show ip ospf](#) de voir l'ID de routeur.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Terminez-vous la stratégie et la planification de réseau OSPF pour votre réseau d'IPv6.
- Routage d'unicast d'IPv6 d'enable.
- IPv6 d'enable sur l'interface.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les configurations dans ce document est basées sur le routeur de gamme Cisco 3700 sur le logiciel 12.4 (15)T 13 de version logicielle de Cisco IOS®.

Conventions

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

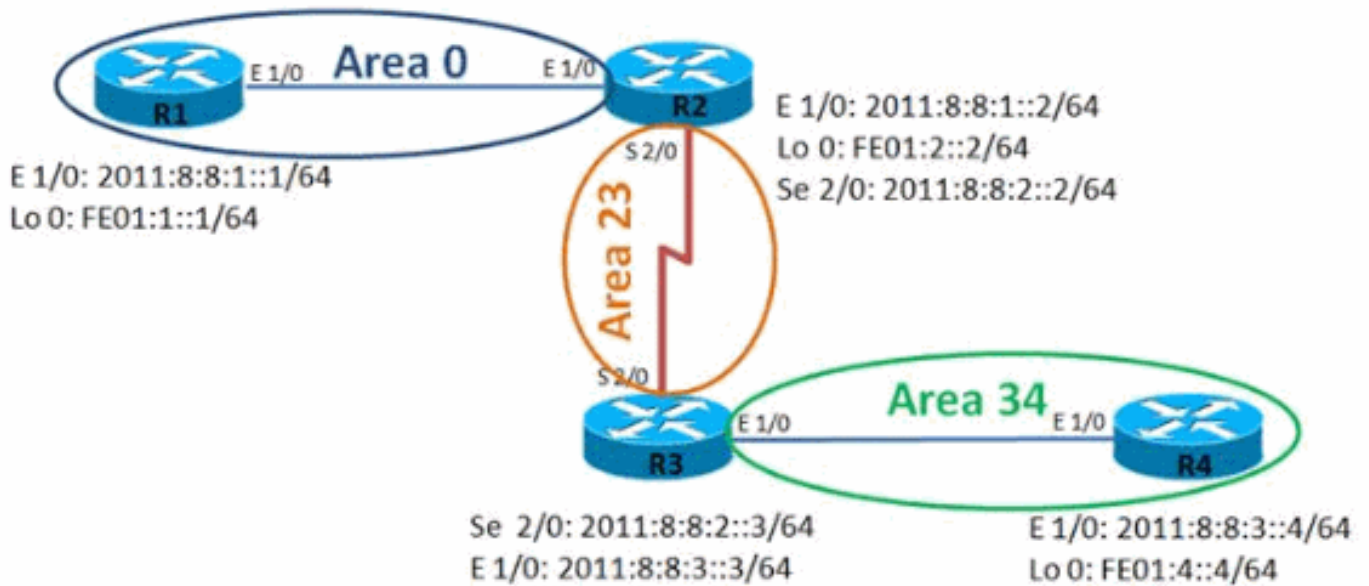
Configurez

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

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- Routeur R1
- Routeur R2
- Routeur R3
- Routeur R4

Routeur R1

```
hostname R1
!
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
 no ip address
 ipv6 address FE01:1::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface Ethernet1/0
 no ip address
 ipv6 address 2011:8:8:1::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
ipv6 router ospf 10
 router-id 1.1.1.1
 log-adjacency-changes
```

Routeur R2

```
hostname R2
!
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
 no ip address
 ipv6 address FE01:2::2/64
 ipv6 enable
```

```
ipv6 ospf 10 area 0
!
interface Ethernet1/0
no ip address
ipv6 address 2011:8:8:1::2/64
ipv6 enable
ipv6 ospf 10 area 0
!
interface Serial2/0
no ip address
ipv6 address 2011:8:8:2::2/64
ipv6 enable
ipv6 ospf 10 area 23
serial restart-delay 0
clock rate 64000
!
ipv6 router ospf 10
router-id 2.2.2.2
log-adjacency-changes
area 23 virtual-link 3.3.3.3
!
```

Routeur R3

```
hostname R3
!
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
no ip address
ipv6 address FE01:3::3/64
ipv6 enable
ipv6 ospf 10 area 23
!

interface Ethernet1/0
no ip address
ipv6 address 2011:8:8:3::3/64
ipv6 enable
ipv6 ospf 10 area 34
!
interface Serial2/0
no ip address
ipv6 address 2011:8:8:2::3/64
ipv6 enable
ipv6 ospf 10 area 23
serial restart-delay 0
!
ipv6 router ospf 10
router-id 3.3.3.3
log-adjacency-changes
area 23 virtual-link 2.2.2.2
!
```

Routeur R4

```
hostname R4
!
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
no ip address
ipv6 address FE01:4::4/64
ipv6 enable
```

```
ipv6 ospf 10 area 34
!
interface Ethernet1/0
no ip address
ipv6 address 2011:8:8:3::4/64
ipv6 enable
ipv6 ospf 10 area 34
!
ipv6 router ospf 10
router-id 4.4.4.4
log-adjacency-changes
!
```

Vérifiez

Utilisez ces commandes de vérifier la configuration :

Dans le routeur R1

La sortie prouve clairement que le routeur R1 peut cingler avec succès l'adresse de bouclage du routeur R4.

ping ipv6

```
R1#ping ipv6
Target IPv6 address: fe01:4::4
Ping Loopback 0 interface of R4 Repeat count [5]:
Datagram size [100]: Timeout in seconds [2]: Extended
commands? [no]: Type escape sequence to abort. Sending
5, 100-byte ICMP Echos to FE01:4::4, timeout is 2
seconds: !!!!! Success rate is 100 percent (5/5), round-
trip min/avg/max = 48/72/96 ms
```

Dans le routeur R2

La commande de [show ipv6 ospf neighbor](#) fournit les informations sur les voisins sur a par base d'interface.

show ipv6 ospf neighbor

```
R2# show ipv6 ospf neighbor

Neighbor ID      Pri   State           Dead Time
Interface ID     Interface
3.3.3.3          0    FULL/ -         -
22              OSPFv3_VL0
Virtual Link Between R2 & R3 1.1.1.1 1 FULL/DR 00:00:35
4 Ethernet1/0 3.3.3.3 0 FULL/ - 00:00:31 12 Serial2/0
```

Dans le routeur R4

La sortie prouve clairement que le routeur R4 peut cingler avec succès l'interface de réalimentation du routeur R1.

ping ipv6

```
R4#ping ipv6
Target IPv6 address: fe01:1::1
Ping Loopback 0 interface of R1 Repeat count [5]:
```

```
Datagram size [100]: Timeout in seconds [2]: Extended
commands? [no]: Type escape sequence to abort. Sending
5, 100-byte ICMP Echos to FE01:1::1, timeout is 2
seconds: !!!!! Success rate is 100 percent (5/5), round-
trip min/avg/max = 56/100/224 ms
```

[Dépannez](#)

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

[Informations connexes](#)

- [Support technique d'IPv6](#)
- [Support technique de Protocole OSPF \(Open Shortest Path First\)](#)
- [Mise en oeuvre de l'OSPF pour l'IPv6](#)
- [Configuration d'échantillon pour OSPFv3](#)
- [Support et documentation techniques - Cisco Systems](#)