Note en tech d'emballage OSPF, de MTU et LSA

Contenu

[Introduction](#)
[Longueur de paquet OSPF](#)
[MTU en paquet DBD](#)
[LSAs de comportement et d'emballage OSPF dans un paquet de mise à jour LS](#)
[Avant l'ID de bogue Cisco CSCse01519](#)
[Après l'ID de bogue Cisco CSCse01519](#)
[ID de bogue Cisco CSCse01519](#)
[Aperçu](#)
[Scénario](#)

Introduction

Ce document décrit l'interaction des paquets de Protocole OSPF (Open Shortest Path First), de l'unité maximum de transition (MTU), des annonces d'État de lien (LSAs), et des paquets de mise à jour de l'État de lien (LS) dans le cadre de l'ID de bogue Cisco CSCse01519.

Longueur de paquet OSPF

Les liens sur des Routeurs ont un MTU. Les paquets sortants, tels que des paquets OSPF, ne peuvent pas être plus grands que l'interface MTU.

Request For Comments (RFC) version 2 de 2328 documents du protocole OSPF. L'annexe A.1 de RFC 2328 décrit l'encapsulation des paquets OSPF de cette manière :

L'OSPF fonctionne directement au-dessus de la couche réseau de l'Internet Protocol. Des paquets OSPF sont donc encapsulés seulement par des en-têtes IP et de liaison de données locale.

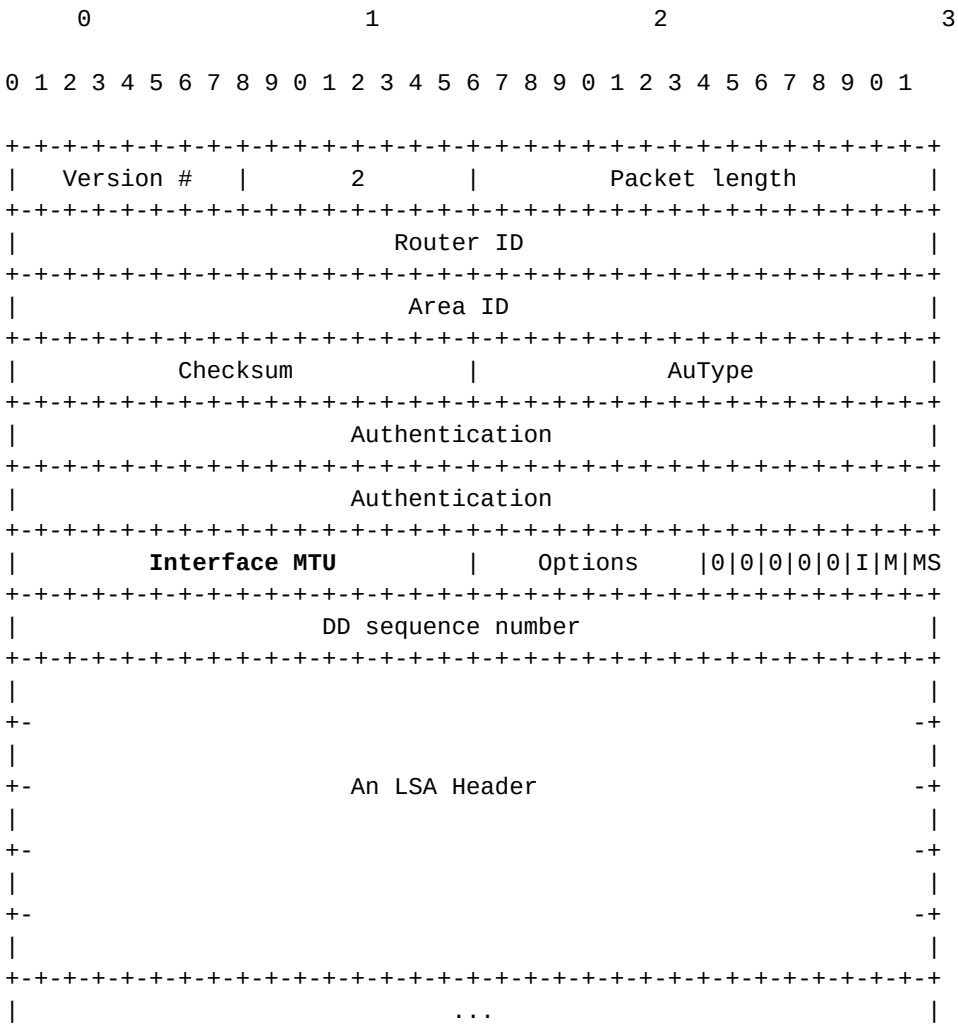
L'OSPF ne définit pas une manière de fragmenter ses paquets de protocole, et dépend de la fragmentation IP en transmettant des paquets plus grands que le MTU de réseau. S'il y a lieu, la longueur de paquets OSPF peut être jusqu'à 65,535 octets (en-tête IP y compris). Les types de paquet OSPF qui sont susceptibles d'être grands (des paquets de description de base de données, demande d'État de lien, mise à jour d'État de lien, et des paquets d'accusé de réception d'État de lien) peuvent habituellement être coupés en plusieurs paquets distincts de protocole, sans perte de fonctionnalité. Ceci est recommandé ; La fragmentation IP devrait être évitée autant que possible.

Il peut y avoir un ou plusieurs LSAs dans un paquet de mise à jour LS. Beaucoup LSAs en un paquet de mise à jour LS est connu en tant qu'emballage de LSAs dans un paquet de mise à jour

LS.

MTU en paquet DBD

Le paquet de la description de base de données (DBD), également spécifié dans RFC 2328, décrit le contenu de la base de données d'état de lien OSPF :



L'annexe A.3.3 de RFC 2328 décrit l'interface MTU en tant que :

La taille dans les octets du plus grand datagramme IP qui peut être envoyé l'interface associée, sans fragmentation.

Routeurs qui sont reliés à un échange de lien leur valeur d'interface MTU en paquets DBD quand la contiguïté OSPF est initialisée.

Section 10.6 d'états RFC 2328 :

Si le champ de MTU d'interface dans le paquet de description de base de données indique une taille de datagramme IP qui est plus grande que le routeur peut recevoir sur l'interface de réception sans fragmentation, le paquet de description de base de données est rejeté.

Quand la commande de **debug ip ospf adj** est utilisée, vous pouvez voir l'arrivée de ces paquets DBD.

Dans cet exemple, il y a une non-concordance en valeurs de MTU entre deux voisins OSPF. Ce

routeur a le MTU 1600 :

```
OSPF: Rcv DBD from 10.100.1.2 on GigabitEthernet0/1 seq 0x2124 opt 0x52 flag 0x2
len 1452 mtu 2000 state EXSTART
OSPF: Nbr 10.100.1.2 has larger interface MTU
```

L'autre routeur OSPF a l'interface MTU 2000 :

```
OSPF: Rcv DBD from 10.100.100.1 on GigabitEthernet0/1 seq 0x89E opt 0x52 flag 0x7
len 32 mtu 1600 state EXCHANGE
OSPF: Nbr 10.100.100.1 has smaller interface MTU
```

Les paquets DBD sont retransmis continuellement jusqu'à ce que la contiguïté OSPF soit par la suite démolie.

```
OSPF: Send DBD to 10.100.1.2 on GigabitEthernet0/1 seq 0x9E6 opt 0x52 flag 0x7
len 32
OSPF: Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1 [10]
OSPF: Send DBD to 10.100.1.2 on GigabitEthernet0/1 seq 0x9E6 opt 0x52 flag 0x7
len 32
OSPF: Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1 [11]
%OSPF-5-ADJCHG: Process 1, Nbr 10.100.1.2 on GigabitEthernet0/1 from EXSTART to
DOWN, Neighbor Down: Too many retransmissions
```

LSAs de comportement et d'emballage OSPF dans un paquet de mise à jour LS

Avant l'ID de bogue Cisco CSCse01519

Avant l'ID de bogue Cisco CSCse01519, l'OSPF en logiciel de Cisco IOS® a construit des paquets OSPF aucun plus grands octets than1500, indépendamment de l'interface MTU. Ainsi, si l'interface MTU était plus grande que 1500 octets, l'OSPF emballait toujours seulement jusqu'à 1500 octets dans un paquet OSPF. C'était quelque peu inefficace parce que l'OSPF pourrait envoyer de plus grands paquets sur le lien et réaliser un plus grand débit.

> Remarque: Il y avait une exception à ce scénario. Si un LSA tenait plus de 1500 octets, l'OSPF a construit ce paquet, aucune matière la taille, parce que l'OSPF ne peut pas fragmenter un LSA. La pile IP du routeur a alors fragmenté le paquet afin d'adapter le MTU de l'interface sortante. Ceci s'est typiquement produit quand un routeur OSPF a eu beaucoup de liens, et le LSA du routeur est devenu plus grand que le MTU de lien.

De même, si le MTU de l'interface sortante était plus petit que 1500 octets, le processus OSPF a toujours construit ou a emballé des paquets OSPF vers le haut de 1500 octets, et la pile IP du routeur a fragmenté le paquet dans de plus petits paquets IP afin d'adapter le MTU du lien sortant. Ceci s'est typiquement produit avec un tunnel d'IPSec entre deux Routeurs qui exécutaient l'OSPF. Le temps système ajouté des octets d'encapsulation du tunnel a mené à un MTU qui était plus petit que 1500 octets. L'OSPF a construit des paquets OSPF jusqu'à 1500 octets et les paquets ont été alors fragmentés avant que le routeur les ait transmis. C'était une inefficacité supplémentaire.

Après l'ID de bogue Cisco CSCse01519

Après l'ID de bogue Cisco CSCse01519, l'OSPF dans l'IOS peut emballer des paquets OSPF pour être plus grand que 1500 octets. Ceci se produit si le MTU de l'interface sortante est plus grand que 1500 octets. Les transmissions sont plus efficaces parce que plus d'informations peuvent être emballées dans un plus grand paquet. En d'autres termes, si un routeur OSPF doit communiquer beaucoup LSAs externe à un voisin OSPF, il peut emballer LSAs plus externe dans un paquet de mise à jour LS si ce routeur exécute l'IOS avec l'ID de bogue Cisco CSCse01519 mis en application.

L'ID de bogue Cisco CSCse01519 permet également à l'OSPF pour établir de plus petits que 1500 octets de paquets. Dans quelques scénarios, le MTU entre deux voisins OSPF est plus petit que 1500 octets. Dans l'exemple précédent avec un tunnel d'IPSec, l'OSPF transmet les paquets OSPF qui sont plus petits que 1500 octets et évite la fragmentation IP ; de nouveau, l'exception est le cas d'un LSA qui est plus grand que l'interface MTU.

ID de bogue Cisco CSCse01519

Quand vous promouvez un routeur OSPF, vous pouvez découvrir une question de MTU OSPF provoquée par l'ID de bogue Cisco CSCse01519.

Aperçu

Beaucoup de réseaux ont des voisins OSPF qui sont connectés par un réseau commuté de la couche 2 (L2), ou le réseau de transport, consisté en le service de L2VPN ou une Hiérarchie Numérique Synchrone/réseau synchrone du réseau optique (SDH/SONET). Ces réseaux de transport peuvent avoir différentes configurations de MTU que les Routeurs qui exécutent l'OSPF.

Bien que la configuration de MTU devrait être correcte sur tous les Routeurs et devrait refléter le MTU vrai, il y a souvent des erreurs qui passent inapperçues.

C'est un réseau d'exemple avec deux Routeurs qui exécutent l'OSPF. Le routeur 1 (R1) et le routeur 2 (R2) sont connectés par un commutateur L2.

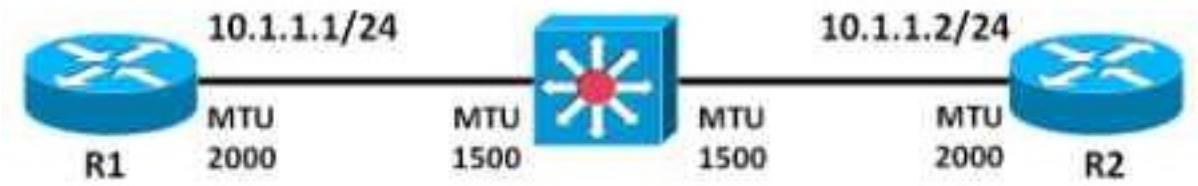


Figure 1 : Example network

Dans cet exemple, les Routeurs ont des interfaces de GigabitEthernets avec un MTU réglé à 2000. Le MTU du commutateur L2 est seulement 1500 octets.

Si la taille du trafic de données n'est jamais plus grande que 1500 octets, vous pouvez utiliser l'IOS sans ID de bogue Cisco CSCse01519 parce que les paquets OSPF ne sont jamais plus grands que 1500 octets. Cependant, s'il y a un LSA qui est de 1800 octets, par exemple, le processus OSPF sur R1 ou R2 établit octets d'un paquet de mise à jour LS de plus grands que 1500 et les transmet, mais le paquet est lâché par le commutateur L2 entre les Routeurs.

Si la base de données OSPF sur R2 a assez de réseaux, le LSAs localement lancé sont si grand qu'un paquet de mise à jour LS pourrait être plus grand que l'interface MTU.

- Si ces réseaux sont lancés par la commande réseau de bâche, les réseaux apparaissent dans le LSA du routeur de R2. R2 construit un LSA du routeur qui est plus grand que 2000 octets et le transmet, mais l'IP le fragmente à 2000 octets, l'interface MTU. Le commutateur L2 cependant relâche ces paquets. L'OSPF retransmet alors ce paquet sans fin, et l'état de contiguïté OSPF n'est jamais plein. Ainsi, la question est immédiatement découverte, même lorsque vous exécutez l'IOS sans ID de bogue Cisco CSCse01519.
- Si ces réseaux sont lancés par la commande **connectée par redistribuer**, les réseaux apparaissent dans LSAs externe. Essais OSPF pour emballer LSAs externe dans un paquet de mise à jour LS qui est jusqu'à 1500 octets dans la taille. Dans ce cas, parce que l'interface MTU est de 2000 octets, la contiguïté OSPF atteint le « PLEIN » état. La question d'un MTU sous-jacent insuffisant n'est pas immédiatement découverte. La question sera découverte quand un routeur est mis à jour à l'IOS avec l'ID de bogue Cisco CSCse01519.

Scénario

Supposez que les deux Routeurs exécutent une version IOS sans ID de bogue Cisco CSCse01519.

Quand les constructions de contiguïté OSFP, notent que R1 ne reçoit jamais octets d'un paquet OSPF de plus grands que 1500, bien que le MTU des interfaces soit 2000.

Activez la commande de **paquets OSPF d'IP de débogage**.

```
OSPF: rcv. v:2 t:1 l:48 rid:10.100.1.2
     aid:0.0.0.0 chk:72CF aut:0 auk: from GigabitEthernet0/1
...
OSPF: rcv. v:2 t:4 l:1468 rid:10.100.1.2
     aid:0.0.0.0 chk:8389 aut:0 auk: from GigabitEthernet0/1
OSPF: rcv. v:2 t:4 l:136 rid:10.100.1.2
...
```

Dans cette sortie de débogage, 'l:1468 est la longueur du paquet OSPF, ainsi vous pouvez voir que le plus grand paquet OSPF était de 1468 octets. 't:4 indique que le paquet OSPF est le type 4, qui est un paquet de mise à jour d'État de lien. Cette table de la section 4.3 de RFC 2328 définit les différents types de paquet OSPF :

Type	Nom de paquet	Fonction de Protocol
1	Bonjour	Découvrez/mettez à jour les voisins
2	Description de base de données	Récapitulez le contenu de base de données
3	Demande d'État de lien	Téléchargement de base de données
4	Mise à jour d'État de lien	Mise à jour de base de données
5	État de lien ACK	Inondation de l'accusé de réception

La contiguïté OSPF atteint le « PLEIN » état.

```
R1#show ip ospf neighbor gigabitEthernet 0/1

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.100.1.2        0   FULL/  -        00:00:34    10.1.1.2        GigabitEthernet0/1

R2#show ip ospf neighbor gigabitEthernet 0/1

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.100.100.1      0   FULL/  -        00:00:34    10.1.1.1        GigabitEthernet0/1
```

Ensuite, IOS de mise à jour sur R2 à une version IOS avec l'ID de bogue Cisco CSCse01519.

```
R2#show ip ospf neighbor gigabitEthernet 0/1

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.100.100.1      0   LOADING/  -     00:00:33    10.1.1.1        GigabitEthernet0/1

R2#show ip ospf neighbor gigabitEthernet 0/1 detail
Neighbor 10.100.100.1, interface address 10.1.1.1
   In the area 0 via interface GigabitEthernet0/1
   Neighbor priority is 0, State is LOADING, 5 state changes
   DR is 0.0.0.0 BDR is 0.0.0.0
   Options is 0x12 in Hello (E-bit L-bit )
   Options is 0x52 in DBD (E-bit L-bit O-bit)
   LLS Options is 0x1 (LR)
   Dead timer due in 00:00:39
   Neighbor is up for 00:00:49
   Index 1/1, retransmission queue length 0, number of retransmission 0
   First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
   Last retransmission scan length is 0, maximum is 0
   Last retransmission scan time is 0 msec, maximum is 0 msec
   Number of retransmissions for last link state request packet 9
   Poll due in 00:00:00

R2#show ip ospf neighbor gigabitEthernet 0/1 detail
Neighbor 10.100.100.1, interface address 10.1.1.1
   In the area 0 via interface GigabitEthernet0/1
   Neighbor priority is 0, State is LOADING, 5 state changes
   DR is 0.0.0.0 BDR is 0.0.0.0
   Options is 0x12 in Hello (E-bit L-bit )
   Options is 0x52 in DBD (E-bit L-bit O-bit)
   LLS Options is 0x1 (LR)
   Dead timer due in 00:00:33
   Neighbor is up for 00:02:06
   Index 1/1, retransmission queue length 0, number of retransmission 0
   First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
   Last retransmission scan length is 0, maximum is 0
   Last retransmission scan time is 0 msec, maximum is 0 msec
   Number of retransmissions for last link state request packet 25
   Poll due in 00:00:03

%OSPF-5-ADJCHG: Process 1, Nbr 10.100.100.1 on GigabitEthernet0/1 from LOADING
to DOWN, Neighbor Down: Too many retransmissions
```

La contiguïté OSPF est coincée dans l'état de « CHARGEMENT » et n'atteint pas le « PLEIN » état. Les retransmissions se produisent jusqu'à ce que l'OSPF atteigne sa limite de 25 retransmissions. Les essais OSPF pour établir la contiguïté de nouveau, la même question se reproduit, et la boucle continue sans fin.

Ainsi, la mise à jour sur R2 découvre une question précédemment masquée : le MTU sous-jacent est plus petit que celui utilisé par les Routeurs OSPF.

Quand le commutateur change le MTU à 2000, octets d'un paquet OSPF de plus grands que 1500

('l:1980) est transmis sans le problème.

```
R1#
OSPF: rcv. v:2 t:3 l:1980 rid:10.100.1.2
     aid:0.0.0.0 chk:AC5B aut:0 auk: from GigabitEthernet0/1
```

Afin de vérifier les questions sous-jacentes de MTU, cinglez toujours l'adresse IP voisine OSPF avec une taille égale au MTU et au bit DF (ne font pas le fragment) pour placer.

Afin de découvrir la valeur du MTU sous-jacent, exécutez un ping, et balayez la taille. Comptez le nombre de points d'exclamation (!) dans la sortie afin de déterminer le MTU correct. Dans cet exemple, la dernière réponse d'écho de la **commande ping** a la taille 1500 octets.

```
R2#ping
Protocol [ip]:
Target IP address: 10.1.1.1
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: yes
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]: yes
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]: yes
Sweep min size [36]: 1460
Sweep max size [18024]: 1540
Sweep interval [1]:
Type escape sequence to abort.
Sending 81, [1460..1540]-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.............................
...........
Success rate is 49 percent (40/81), round-trip min/avg/max = 1/1/4 ms
```