

OSPF-, MTU- en LSA-pakkettechnische opmerking

Inhoud

[Inleiding](#)

[OSPF-pakketgrootte](#)

[MTU in DBD-pakket](#)

[OSPF-gedrag en het verpakken van LSA's in een LS-update](#)

[Vóór Cisco Bug ID CSCse01519](#)

[Na Cisco plug-in CSCse01519](#)

[Cisco plug-in CSCse01519](#)

[Overzicht](#)

[Scenario](#)

Inleiding

Dit document beschrijft de interactie van de pakketten Open Shortest Path First (OSPF), maximum transitie-eenheid (MTU), Link State Advertisements (LSA's) en Link State (LS) Update-pakketten in de context van Cisco bug ID [CSCse01519](#).

OSPF-pakketgrootte

Links op routers hebben een MTU. Uitgaande pakketten, zoals OSPF-pakketten, kunnen niet groter zijn dan de interface-MTU.

[Verzoek om Comments \(RFC\) 2328](#) documenten versie 2 van het OSPF-protocol. Bijlage A.1 van RFC 2328 beschrijft de insluiting van OSPF-pakketten op deze manier:

OSPF voert rechtstreeks via de netwerklaag van het Internet Protocol uit. OSPF-pakketten zijn daarom alleen ingesloten door IP- en lokale datalink-headers.

OSPF definieert geen manier om zijn protocolpakketten te fragmenteren, en is afhankelijk van IP-fragmentatie bij het verzenden van pakketten die groter zijn dan de netwerk MTU. Indien nodig, kan de lengte van OSPF-pakketten tot 65.535 bytes (inclusief de IP-header) zijn. De OSPF-pakkettypen die waarschijnlijk groot zijn (Databaseverschrijving pakketten, Link State Application, Link State Update, en Link State Recognition pakketten) kunnen doorgaans in verschillende afzonderlijke protocolpakketten worden gesplitst zonder dat de functionaliteit verloren gaat. Dit wordt aanbevolen; IP-fragmentatie moet zoveel mogelijk worden vermeden.

Er kan een of meer LSA's zijn in een LS Update pakket. Vele LSA's in één pakket LS Update is bekend als het inpakken van LSA's in een pakket LS Update.


```
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
```

De andere router OSPF heeft 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
```

De DBD-pakketten worden ononderbroken opnieuw verzonden tot de OSPF-nabijheid uiteindelijk wordt afgebroken.

```
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
```

OSPF-gedrag en het verpakken van LSA's in een LS-update

Vóór Cisco Bug ID CSCse01519

Voordat Cisco bug ID [CSCse01519](#), OSPF in de Cisco IOS[®] software die OSPF-pakketten met niet meer dan 1500 bytes heeft gebouwd, ongeacht de interface-MTU. Dus als de interface-MTU groter was dan 1500 bytes, OSPF heeft alleen tot 1500 bytes in een OSPF-pakket ingepakt. Dit was ietwat inefficiënt omdat OSPF grotere pakketten op de link kon verzenden en grotere doorvoersnelheid kon bereiken.

Opmerking: Er was één uitzondering op dit scenario. Als één LSA meer dan 1500 bytes heeft bewaard, bouwde OSPF dat pakket, ongeacht de grootte, omdat OSPF geen één LSA kan fragmenteren. De IP stapel van de router fragmenteerde het pakket om de MTU van de uitgaande interface te passen. Dit kwam typisch voor toen een router OSPF veel verbindingen had, en de router LSA groter werd dan de verbinding MTU.

Op dezelfde manier als MTU van de uitgaande interface kleiner was dan 1500 bytes, is het OSPF-proces nog steeds gebouwd of ingepakt OSPF-pakketten tot 1500 bytes. De IP-stapel van de router heeft het pakket gefragmenteerd in kleinere IP-pakketten om te passen in de MTU van de uitgaande link. Dit kwam typisch voor met een IPSec-tunnel tussen twee routers die OSPF in werking hadden. De toegevoegde overhead van de insluitingsbytes van de tunnel leidde tot een MTU die kleiner was dan 1500 bytes. OSPF-gebouwde OSPF-pakketten tot 1500 bytes en de pakketten zijn vervolgens gefragmenteerd voordat de router ze heeft verzonden. Dit was een extra inefficiëntie.

Na Cisco plug-in CSCse01519

Na Cisco bug-ID [CSCse01519](#) kan OSPF-pakketten in IOS-pakketten zijn die groter zijn dan 1500 bytes. Dit gebeurt als de MTU van de uitgaande interface groter is dan 1500 bytes. Transmissies zijn efficiënter omdat meer informatie in één groter pakket kan worden ingepakt. Met andere woorden, als één OSPF-router veel externe LSA's naar een OSPF-buurman moet verzenden, kan deze meer externe LSA's in één LS-update-pakket verpakken als die router IOS met Cisco bug ID CSCse01519 geïmplementeerd heeft.

Met Cisco bug-ID CSCse01519 kan ook OSPF-pakketten bouwen die kleiner zijn dan 1500 bytes. In sommige scenario's, is MTU tussen twee OSPF burens kleiner dan 1500 bytes. In het vorige voorbeeld met een IPSec-tunnel, brengt OSPF pakketten over die kleiner zijn dan 1500 bytes en IP fragmentatie vermijdt; Ook in dit geval is de uitzondering het geval van een LSA die groter is dan de interface MTU.

Cisco plug-in CSCse01519

Wanneer u een OSPF-router verbetert, kunt u een OSPF-MTU-probleem ontdekken dat door Cisco bug-ID [CSCse01519](#) is veroorzaakt.

Overzicht

Veel netwerken hebben OSPF-buren die aangesloten zijn door een Layer 2 (L2) switched netwerk of transportnetwerk dat bestaat uit L2 VPN-service of een synchroon digitaal Hierarchy/Synchronous Optical Network (SDH/SONET) netwerk. Deze transportnetwerken kunnen verschillende MTU-instellingen hebben dan de routers die OSPF-ondersteuning uitvoeren.

Hoewel de instelling van de MTU op alle routers zou moeten gelden en de echte MTU zou moeten weerspiegelen, zijn er vaak fouten die onopgemerkt blijven.

Dit is een voorbeeldnetwerk met twee routers die OSPF uitvoeren. Router 1 (R1) en router 2 (R2) worden aangesloten door een L2 switch.

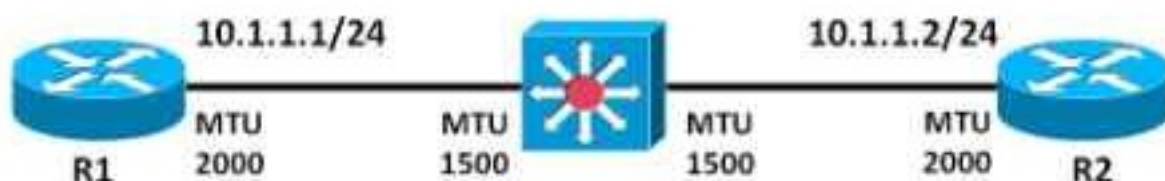


Figure 1 : Example network

In dit voorbeeld hebben de routers Gigabit Ethernet interfaces met een MTU die op 2000 is ingesteld. De MTU van de L2 switch is slechts 1500 bytes.

Als de grootte van het gegevensverkeer nooit groter is dan 1500 bytes, kunt u IOS zonder Cisco bug ID [CSCse01519](#) gebruiken omdat de OSPF-pakketten nooit groter zijn dan 1500 bytes. Als er echter een LSA is dat 1800 bytes is, bijvoorbeeld, bouwt het OSPF-proces op R1 of R2 een LS Update-pakket dat groter is dan 1500 bytes en geeft het door, maar het pakket wordt door de L2-switch tussen de routers gedropt.

Als de OSPF-database op R2 genoeg netwerken heeft, zijn de lokaal geïnitieerde LSA's zo groot dat een LS-update-pakket groter kan zijn dan de interface-MTU.

- Als deze netwerken hun oorsprong vinden in het opvallende netwerkopdracht, verschijnen de netwerken in de router LSA van R2. R2 bouwt een router LSA die groter is dan 2000 bytes en geeft het door, maar IP fragmenten het aan 2000 bytes, de interface MTU. De L2 switch laat deze pakketten echter vallen. OSPF zendt dit pakket vervolgens eindeloos opnieuw uit en de OSPF-nabijheidsstaat is nooit vol. Dus wordt de kwestie onmiddellijk ontdekt, zelfs wanneer u IOS zonder Cisco bug-ID CSCse01519 draait.
- Als deze netwerken van de **herverdelingsverbonden** opdracht afkomstig zijn, verschijnen de netwerken in externe LSAs. OSPF probeert externe LSA's in één LS-bijwerken pakket te verpakken dat tot 1500 bytes in grootte heeft. In dit geval, omdat de interface MTU 2000 bytes is, bereikt de OSPF nabijheid de 'FULL' staat. De kwestie van een ontoereikende onderliggende MTU wordt niet onmiddellijk ontdekt. De kwestie zal worden ontdekt wanneer één router aan IOS met Cisco bug ID CSCse01519 wordt bijgewerkt.

Scenario

Stel dat beide routers een IOS-versie zonder Cisco bug-ID [CSCse01519](#) uitvoeren.

Wanneer de OSFP nabijheid bouwt, merk op dat R1 nooit een OSPF pakket groter dan 1500 bytes ontvangt, alhoewel MTU van de interfaces 2000 is.

Schakel de opdracht **ip-pakketten automatisch** op.

```
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
...
```

In deze debug uitvoer is 'l:1468' de lengte van het OSPF-pakket, zodat u kunt zien dat het grootste OSPF-pakket 1468 bytes was. 't:4' geeft aan dat het OSPF-pakket type 4 is, dat een Link State Update-pakket is. Deze tabel in sectie 4.3 van RFC 2328 definieert de verschillende OSPF-pakkettypen:

Type	Packet-naam	Protocolfunctie
1	Hallo	buren detecteren/onderhouden
2	Beschrijving van database	Inhoud van database samenvatten
3	verzoek van de verbindingstaat	Databaseverdownload
4	Update over link	Databaseverwerking
5	Link State Ack	Overstromingsontvangstbevestiging

De OSPF nabijheid bereikt de 'FULL' staat.

```
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

Daarna, upgrade IOS op R2 naar een IOS versie met Cisco bug-ID 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
```

De OSPF-nabijheid zit vast in 'LOADING'-status en bereikt niet de 'FULL'-status. Terugzendingen komen voor tot OSPF zijn grens van 25 terugzendingen bereikt. OSPF probeert opnieuw de nabijheid te bepalen, de zelfde kwestie opnieuw voorkomt, en de lijn blijft eindeloos doorgaan.

Zo wordt in de upgrade op R2 een eerder verborgen probleem ontdekt: de onderliggende MTU is kleiner dan die gebruikt wordt door de OSPF-routers.

Wanneer de switch MTU in 2000 verandert, wordt een OSPF-pakket groter dan 1500 bytes ('!:1980') zonder probleem verzonden.

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

Om onderliggende problemen van MTU te controleren, pingel altijd het OSPF IP-adres van de buurman met een grootte gelijk aan MTU en het DF (geen fragment) bit set.

Om de waarde van de onderliggende MTU te ontdekken, voert u een ping uit en vaagt u de grootte. Tel het aantal uitroeptekens (!) in de output om de juiste MTU te bepalen. In dit voorbeeld heeft het laatste echo-antwoord van de ping opdracht een grootte van 1500 bytes.

```
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
```