

# Nota Técnica da embalagem OSPF, MTU e LSA

## Índice

[Introdução](#)

[Tamanho de pacote de OSPF](#)

[MTU no pacote DBD](#)

[LSA do comportamento e da embalagem OSPF em um pacote de atualização LS](#)

[Antes da identificação de bug Cisco CSCse01519](#)

[Após a identificação de bug Cisco CSCse01519](#)

[Identificação de bug Cisco CSCse01519](#)

[Visão geral](#)

[Cenário](#)

## Introdução

Este documento descreve a interação de pacotes do Open Shortest Path First (OSPF), da unidade máxima da transição (MTU), das propagandas do estado do link (LSA), e do estado do link pacotes de atualização (LS) no contexto da identificação de bug Cisco [CSCse01519](#).

## Tamanho de pacote de OSPF

Os links no Roteadores têm um MTU. Os pacotes de saída, tais como pacotes de OSPF, não podem ser maiores do que a interface MTU.

Versão 2 dos documentos da [solicitação para comentários \(RFC\) 2328 do](#) protocolo de OSPF. O apêndice A.1 do RFC 2328 descreve o encapsulamento dos pacotes de OSPF desse modo:

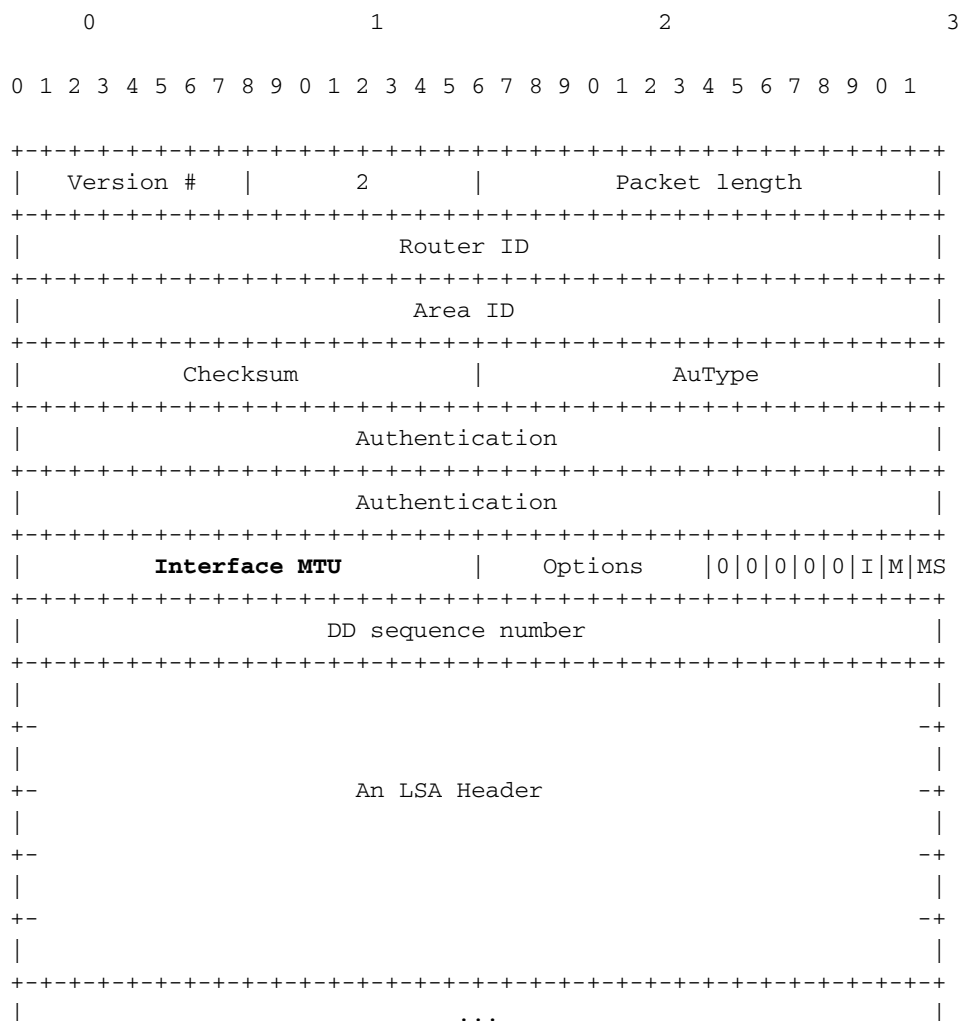
O OSPF é executado diretamente sobre a camada de rede do protocolo de internet. Os pacotes de OSPF são encapsulados consequentemente unicamente por encabeçamentos IP e de link de dados local.

O OSPF não definir uma maneira de fragmentar seus pacotes de protocolo, e depender da fragmentação de IP quando os pacotes de transmissão maiores do que a rede MTU. Caso necessário, o comprimento dos pacotes de OSPF pode ser até 65,535 bytes (que incluem o cabeçalho IP). Os tipos do pacote de OSPF que são prováveis ser grandes (o Database Description Packets, liga a requisição de estado, liga a atualização do estado, e os pacotes de reconhecimento do estado do link) podem geralmente ser rachados em diversos pacotes de protocolo separados, sem perda de funcionalidade. Isto é recomendado; A fragmentação de IP deve ser evitada sempre que possível.

Pode haver uns ou vários LSA em um pacote de atualização LS. Muitos LSA em um pacote de atualização LS são sabidos como a embalagem de LSA em um pacote de atualização LS.

# MTU no pacote DBD

O pacote da descrição de base de dados (DBD), igualmente especificado no RFC 2328, descreve os índices do base de dados de estado de link OSPF:



O apêndice A.3.3 do RFC 2328 descreve a interface MTU como:

O tamanho nos bytes do IP datagram o maior que pode ser mandado a relação associada, sem fragmentação.

Roteadores que está anexado a uma troca do link seu valor da interface MTU em uns pacotes DBD quando a adjacência de OSPF for inicializada.

Seção 10.6 de estados do RFC 2328:

Se o campo da interface MTU no pacote da descrição de base de dados indica um tamanho do IP datagram que seja maior do que o roteador pode aceitar na relação de recepção sem fragmentação, o pacote da descrição de base de dados está rejeitado.

Quando o comando `debug ip ospf adj` é usado, você pode ver a chegada destes pacotes DBD.

Neste exemplo, há uma má combinação em valores MTU entre dois vizinhos de OSPF. Este roteador tem 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
```

O outro OSPF Router tem a 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
```

Os pacotes DBD estão retransmitidos continuamente até que a adjacência de OSPF esteja rasgada eventualmente para baixo.

```
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
```

## LSA do comportamento e da embalagem OSPF em um pacote de atualização LS

### Antes da identificação de bug Cisco CSCse01519

Antes da identificação de bug Cisco [CSCse01519](#), o OSPF no software do <sup>®</sup> do Cisco IOS construiu pacotes de OSPF nenhuns bytes than 1500 maiores, apesar da interface MTU. Assim, se a interface MTU era maior de 1500 bytes, o OSPF ainda embalou somente até 1500 bytes em um pacote de OSPF. Isto era um tanto incapaz porque o OSPF poderia enviar pacotes maiores no link e conseguir a maior taxa de transferência.

Nota: Havia uma exceção a esta encenação. Se um LSA guardou mais de 1500 bytes, o OSPF construiu esse pacote, nenhuma matéria o tamanho, porque o OSPF não pode fragmentar um LSA. A pilha de IP do roteador fragmentou então o pacote a fim caber o MTU da interface enviada. Isto ocorreu tipicamente quando um OSPF Router teve muitos links, e o LSA de roteador tornou-se maior do que o link MTU.

Similarmente, se o MTU da interface enviada era menor de 1500 bytes, o processo de OSPF ainda construiu ou embalou pacotes de OSPF acima de 1500 bytes, e a pilha de IP do roteador fragmentou o pacote em pacotes IP menores a fim caber o MTU do link de saída. Isto ocorreu tipicamente com um túnel de IPsec entre dois Roteadores que executava o OSPF. As despesas gerais adicionadas dos bytes de encapsulamento do túnel conduziram a um MTU que fosse menor de 1500 bytes. O OSPF construiu pacotes de OSPF até 1500 bytes e os pacotes foram fragmentados então antes que o roteador os transmitiu. Esta era uma incapacidade adicional.

### Após a identificação de bug Cisco CSCse01519

Após a identificação de bug Cisco [CSCse01519](#), o OSPF nos IO pode embalar pacotes de OSPF para ser maior de 1500 bytes. Isto ocorre se o MTU da interface enviada é maior de 1500 bytes. As transmissões são mais eficiente porque mais informação pode ser embalada em um pacote maior. Ou seja se um OSPF Router precisa de transmitir muito LSAs externo a um vizinho de

OSPF, pode embalar mais LSAs externo em um pacote de atualização LS se esse roteador executa IO com a identificação de bug Cisco CSCse01519 executada.

A identificação de bug Cisco CSCse01519 igualmente permite que o OSPF construa bytes menores dos pacotes de 1500. Em algumas encenações, o MTU entre dois vizinhos de OSPF é menor de 1500 bytes. No exemplo anterior com um túnel de IPsec, o OSPF transmite os pacotes de OSPF que são menores de 1500 bytes e evita a fragmentação de IP; além disso, a exceção é o exemplo de um LSA que seja maior do que a interface MTU.

## Identificação de bug Cisco CSCse01519

Quando você promove um OSPF Router, você pode descobrir uma edição OSPF MTU causada pela identificação de bug Cisco [CSCse01519](#).

### Visão geral

Muitas redes têm os vizinhos de OSPF que são conectados através de uma rede comutada da camada 2 (L2), ou a rede de transporte, compreendida do serviço L2VPN ou de uma rede /Síncrona da rede ótica da hierarquia digital síncrono (SDH/SONET). Estas redes de transporte podem ter configurações MTU diferentes do que o Roteadores que está executando o OSPF.

Embora a configuração MTU deva estar correta em todo o Roteadores e deva refletir o MTU verdadeiro, há frequentemente os erros que vão despercebidos.

Esta é uma rede de exemplo com dois Roteadores que está executando o OSPF. O roteador1 (r1) e o roteador2 (R2) são conectados através de um interruptor L2.

Neste exemplo, o Roteadores tem relações do gigabitethernet com um MTU ajustado a 2000. O MTU do interruptor L2 é somente 1500 bytes.

Se o tamanho do tráfego de dados é nunca maior de 1500 bytes, você pode usar IO sem identificação de bug Cisco [CSCse01519](#) porque os pacotes de OSPF são nunca maiores de 1500 bytes. Contudo, se há um LSA que seja 1800 bytes, por exemplo, o processo de OSPF no r1 ou no R2 constrói bytes maiores de um pacote de atualização LS de 1500 e os transmite, mas o pacote é deixado cair pelo interruptor L2 entre o Roteadores.

Se a base de dados do OSPF no R2 tem bastante redes, os LSA localmente originados são tão grandes que um pacote de atualização LS pôde ser maior do que a interface MTU.

- Se estas redes são originadas pelo comando network da cobertura, as redes aparecem no LSA de roteador do R2. O R2 constrói um LSA de roteador que seja maior de 2000 bytes e o transmite, mas o IP fragmenta-o a 2000 bytes, a interface MTU. O interruptor L2 contudo deixa cair estes pacotes. O OSPF retransmite então este pacote infinitamente, e o estado da adjacência de OSPF está nunca completo. Assim, a edição é descoberta imediatamente, mesmo quando você está executando IO sem identificação de bug Cisco CSCse01519.
- Se estas redes são originadas pelo **comando redistribute connected**, as redes aparecem no LSAs externo. O OSPF tenta embalar o LSAs externo em um pacote de atualização LS que é até 1500 bytes em tamanho. Neste caso, porque a interface MTU é 2000 bytes, a adjacência de OSPF alcança o estado "FULL". A introdução de um MTU subjacente inadequado não é

descoberta imediatamente. A edição será descoberta quando um roteador é promovido aos IO com identificação de bug Cisco CSCse01519.

## Cenário

Supõe que ambos os Roteadores executam uma Versão do IOS sem identificação de bug Cisco [CSCse01519](#).

Quando as construções da adjacência OSPF, observarem que o r1 nunca recebe bytes maiores de um pacote de OSPF de 1500, embora o MTU das relações seja 2000.

Permita o comando `packets OSPF debug IP`.

```
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
...
```

Neste resultado do debug, 'l:1468 está a um comprimento do pacote de OSPF, assim que você pode ver que o pacote de OSPF o maior era 1468 bytes. 't:4 indica que o pacote de OSPF é o tipo 4, que é um pacote de atualização de estado do link. Esta tabela da seção 4.3 do RFC 2328 define os tipos diferentes do pacote de OSPF:

Tipo	Nome do pacote	Função do protocolo
1	Saudação	Descubra/mantenha vizinhos
2	Descrição de base de dados	Resuma índices do base de dados
3	Solicitação de estado de enlace	Transferência do base de dados
4	Atualização do estado de enlace	Atualização da base de dados
5	Estado Ack do link	Inundando o reconhecimento

A adjacência de OSPF alcança o estado "FULL".

```
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
```

Em seguida, elevação IO no R2 a uma Versão do IOS com identificação de bug 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
```

A adjacência de OSPF é colada no estado da “CARGA” e não alcança o estado “FULL”. As retransmissões ocorrem até que o OSPF alcance seu limite de 25 retransmissões. O OSPF tenta estabelecer outra vez a adjacência, a mesma edição reocorre, e o laço continua infinitamente.

Assim, a elevação no R2 descobre previamente hidden uma edição: o MTU subjacente é menor do que esse usado pelos OSPF Router.

Quando o interruptor muda o MTU a 2000, bytes maiores de um pacote de OSPF os de 1500 (!:1980) estão transmitidos sem o problema.

```
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
```

A fim verificar edições sendo a base MTU, sibile sempre o endereço IP de Um ou Mais Servidores Cisco ICM NT do vizinho de OSPF com um tamanho igual ao MTU e ao jogo do bit DF (Don't Fragment).

A fim descobrir o valor do MTU subjacente, execute um sibilo, e varra o tamanho. Conte o número de pontos de exclamação (!) na saída a fim determinar o MTU correto. Neste exemplo, a última resposta de eco do comando ping tem o tamanho 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]:
```

