

MTU-tuning voor L2TP

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Fragmentatievoorbeeld](#)

[De kwesties](#)

[MTU-tuningmethoden](#)

[Een lagere IP-MTU handmatig configureren](#)

[PMTU's op Windows-pc's aanpassen](#)

[De IP-MTU automatisch aanpassen](#)

[TCP MSS aanpassen](#)

[Een lagere MTU configureren](#)

[Conclusie](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft fragmentatie en hermontage van L2TP-koppelingen en legt uit hoe een afstemming van de maximale transmissieeenheid (MTU) kan helpen om een aantal van de hiermee samenhangende problemen op te lossen.

Voorwaarden

Vereisten

Lezers van dit document zouden kennis moeten hebben van:

- Configuratieopdrachten van General Virtual Private Dialup Network (VPDN)
- Algemene IP-onderwerpen zoals fragmentatie, opnieuw samenvoegen, MTU, insluiting, kopregels enzovoort.

Gebruikte componenten

De meeste configuratie- en functieverbeteringen die hier worden besproken, zijn beschikbaar in Cisco IOS® software releases 12.1T of 12.2T en hoger. Zie de afzonderlijke rubrieken hieronder voor meer informatie.

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Conventies

Raadpleeg [Cisco Technical Tips Conventions](#) (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

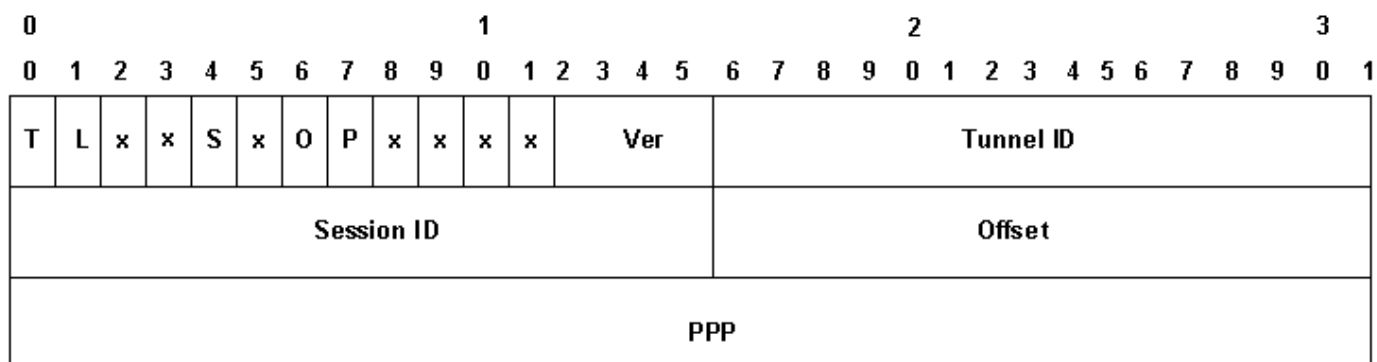
Fragmentatievoorbeeld

Soms moet je tunnelingekapselde pakketten fragmenteren om ze op de draad te kunnen verzenden. Hier is een voorbeeld van.

In het geval van L2TP over UDP, omvat de overhead van alle protocollen een extra set IP-, UDP- en L2TP-headers. De IP header is 20 bytes, de UDP-header is 8 bytes en de L2TP-header is meestal 12 bytes. De 12 bytes van de L2TP-header zijn:

- de versie- en vlaggenvelden (2 bytes)
- de velden tunnelid en sessieid (2 bytes elk)
- 2 bytes van padding-offset
- 4 bytes van Point-to-Point Protocol (PPP)-insluiting

In dit schema zijn meer details te zien:



Als u gegevenssequencing inschakelen (dit wordt standaard uitgeschakeld op Cisco-apparaten), moet u een extra 4 bytes voor de NS- en NR-velden toevoegen. Voeg de IP-, UDP- en L2TP-headers toe om te zien dat L2TP via UDP 40 bytes van protocol insluiting aan het pakket toevoegt.

Wanneer u een IP-pakket van 1500 bytes in L2TP inneemt, wordt het ingekapselde pakket 1540 bytes (1500 + 40 bytes van IP, UDP en L2TP-headers). U moet het pakket fragmenteren om het via een standaard Ethernet-type interface te verzenden (die een MTU van 1500 bytes) heeft. Het ingekapselde pakje is in twee gefragmenteerd. Het eerste fragment bestaat uit 1500 bytes (1460 bytes van het oorspronkelijke IP-pakket + 40 bytes van L2TP-insluiting). Het tweede fragment bestaat uit 60 bytes (laatste 40 bytes van het oorspronkelijke IP-pakket + 20 bytes van IP-overhead).

Opmerking: Alleen het eerste fragment bevat de L2TP-header. het tweede fragment bevat alleen een IP-header. Dit laat de L2TP-peer, of het nu een LAC of LNS is, toe om de twee fragmenten

opnieuw te monteren in het oorspronkelijke pakket met 1540 bytes tunnel ingekapselde pakketjes.

De kwesties

Een van de problemen die Layer 2 Tunneling Protocol (L2TP) via User Datagram Protocol (UDP) en andere Layer 2 en Layer 3 IP-gebaseerde tunneling-protocollen tegenkomen, is dat de overhead van het tunneling-protocol de grootte van het tunnelingekapselde pakket vergroot. Wanneer het oorspronkelijke pakket al groot is, moet u het tunnelingekapselde pakket fragmenteren om het op de draad te verzenden.

Een van de problemen die het fragmenteren en opnieuw assembleren van het L2TP-pakket op de L2TP Access Concentrator (LAC) en L2TP Network Server (LNS) veroorzaakt is dat de fragmentatie en herassemblage op procesniveau in Cisco IOS-software wordt uitgevoerd. Wanneer u grote aantallen L2TP-sessies en verkeersstromen op een LNS aggregereert, kan de processwitching drastisch dalen naar de prestaties. Om deze reden is het zeer wenselijk de behoefte aan fragmentatie en herassemblage in het L2TP-switchingpad te verminderen of te elimineren.

Gebruik een van de in dit document beschreven methoden om de maximale transmissieeenheid (MTU) aan te passen om deze op te lossen.

MTU-tuningmethoden

Een verscheidenheid aan configuraties en functies in Cisco IOS software is ontworpen om fragmentatie en herassemblage in het L2TP-switchpad te voorkomen door de MTU aan te passen.

Een lagere IP-MTU handmatig configureren

Het configureren van een lagere IP MTU op de virtuele sjabloon interface met de **ip mtu** opdracht. Het configureren van een lagere IP MTU dwingt de router om IP-pakketten die de IP MTU overschrijden en het DF- (Don't Fragment)-bit in de IP-header te laten plaatsen. De router genereert dan een Internet Control Message Protocol (ICMP) type 3 Host Unbereikbaar, code 4 fragmentatie nodig bericht naar de bron van het pakket (de oorspronkelijke host). Dit bericht verwijst naar de IP MTU van de interface, zodat de bron de pakketgrootte kan beperken om door de interface te passen. Dit proces wordt ook bekend als Pad MTU Detection (PMTUD). Raadpleeg voor meer informatie [RFC 1191](#) . Configureer de IP-MTU met de grootste IP-pakketgrootte die niet groter is dan de PMTU tussen de LAC en de LNS wanneer de volledige L2TP-header wordt toegevoegd. Stel de IP MTU in op 1460 (1500-40 bytes) voor een PMTU van 1500 bytes en een L2TP-header van 40 bytes.

Als de PMTU onbekend is (of verandert) tussen de LAC en de LNS, kunt u de opdracht **ip pmtu** configureren onder de **vpdn-groep**. De **ip pmtu**-opdracht werd toegevoegd in Cisco IOS-software release 12.2(4)T met behulp van Bug ID CSCds72714 (niet zichtbaar voor externe gebruikers). De functie **ip pmtu** kopieert het DF-bit van het binnenpakket naar de buiten L2TP-header en zet PMTUD aan tussen de router en het L2TP-tunneleindpunt.

PMTU's op Windows-pc's aanpassen

Microsoft Windows heeft een registratieset waarmee u een backhaff-functie voor hun PMTU-ondekking kunt inschakelen. Raadpleeg het volgende artikel op de Microsoft website voor

informatie over Windows NT: [Verandering van het algoritme van het PMTU van het alfabet voor Windows NT 3.51 \(Q136970\)](#) .

Voor Windows 2000/XP beschrijft het Microsoft artikel [How to Troubleshoot Black Hole Router Issues \(Q314825\)](#) verschillende methoden in Windows om dit probleem te voorkomen. Dit artikel definieert het begrip "zwarte gat" router, beschrijft een methode om routers voor zwart gat te lokaliseren en stelt drie manieren voor om het gegevensverlies te voorkomen dat kan optreden vanwege een router voor zwart gat.

[De IP-MTU automatisch aanpassen](#)

U kunt ook automatische aanpassing van de IP MTU inschakelen. Deze functie stelt de router in staat om automatisch de IP MTU aan te passen op de virtuele toegangsinterface om te compenseren voor de grootte van de L2TP-header en de MTU van de noodopdracht. Deze optie is in Cisco IOS-software-release 12.1(5)T toegevoegd met behulp van Bug ID [CSCdr01713](#) (alleen [geregistreerde](#) klanten).

N.B.: De IP-MTU wordt alleen automatisch aangepast als er geen IP-MTU handmatig wordt ingesteld op de virtuele-sjabloon-interface (met behulp van de optie in de vorige sectie).

Eerst werd deze optie standaard ingeschakeld zonder methode om deze uit te schakelen. Bug ID [CSC67753](#) (alleen [geregistreerde](#) klanten) in Cisco IOS-software-releases 12.2(3) en 12.2(4)T voegde later de opdracht **[no] ip mtu** bij de **VPN-groep** aan om deze optie in te schakelen en uit te schakelen. Deze optie moest standaard zijn ingeschakeld. Deze optie heeft geen Opdracht Line Interface (CLI) om de standaardinstelling alleen voor L2X-verbindingen te wijzigen, die niet binden aan een **VPDN-groep** (zoals een door SGBP geïnitieerde L2F of L2TP-tunnel). Het onvermogen om het uit te schakelen voor Multichassis Multilink PPP (MPPPP)-topologieën, in combinatie met de hierna beschreven PMTUD-problemen, heeft veel gebruikersklachten veroorzaakt. Om deze reden werd de standaardinstelling gewijzigd om de automatische aanpassingsfunctie van de IP-MTU te laten uitgeschakeld vanaf Cisco IOS-software-releases 12.2(6) en 12.2(8)T en later met Bug ID [CSCdu 69834](#) (alleen [geregistreerde](#) klanten).

Zowel de handmatige als de automatische aanpassing van de MTU zijn gebaseerd op de PMTUD tussen de eindhosts. PMTUD werkt in theorie niet goed op het internet, maar wel op het internet. Zie [RFC 2923](#) voor een gedetailleerde beschrijving van hoe PMTUD op internet breekt. Het grootste probleem is de aanwezigheid van "zwarte gaten", die ervoor zorgen dat de downloads van webpagina's halverwege de stroom lijken te hangen. Deze zwarte gaten worden in het algemeen veroorzaakt door firewalls of routers die zijn ingesteld om ICMP-berichten te filteren. Wanneer de bron van de grote pakketten niet in staat is om het "ICMP Host Onbereikbaar"bericht van de router te ontvangen, erop wijzend dat de MTU is overschreden, kan zij de pakketgrootte niet verminderen. In plaats daarvan blijft het proberen om hetzelfde pakket steeds opnieuw uit te zenden met de PDF-bit-set. Deze pakketten worden door LNS gedropt aangezien ze PMTU overschrijden en de verbinding stopt met reageren.

Wegens problemen die op PMTUD vertrouwen om te ontdekken dat de IP MTU kleiner is via een L2TP-tunnel, heeft Cisco de TCP Maximum Segment Size (MSS) optie in Cisco IOS-software-release 12.2(4)T toegevoegd.

[TCP MSS aanpassen](#)

De optie Maximum aantal segmentgrootte van TCP - toegevoegd door Bug ID [CSCds6957](#) (alleen [geregistreerde](#) klanten) beschikbaar in Cisco IOS-software-release 12.2(4)T en staat de router later

toe om de geadverteerde MSS in inkomende en uitgaande TCP-pakketten (SYN) die door de end-hosts worden verzonden aan te passen. Door de TCP MSS in een lagere waarde te veranderen dan de gebruikelijke standaard van 1460, kunt u TCP als een bron van pakketten met volledige grootte elimineren. De TCP MSS moet aan een waarde worden aangepast zodat een TCP-segment met een TCP/IP-header en ingekapseld in L2TP via UDP niet hoger is dan de IP MTU van de IP-interface. Een TCP/IP-header is over het algemeen 40 bytes en de L2TP-over-UDP-header is een extra 40 bytes. Daarom moet de TCP MSS in het algemeen worden aangepast aan 1420 (1500 - 40 bytes TCP/IP-header - 40 bytes L2TP via UDP-header).

De hiervoor gebruikte opdracht is **IP TCP-instelling, bijv. mss <mss>**, wat een opdracht op interfaceniveau is.

De laatste optie voor het verminderen van fragmentatie in een L2TP-netwerk vereist ondersteuning voor Maximaal ontvangen (MRU) onderhandeling op de Point-to-Point Protocol-client. De MRU optie in PPP staat een peer toe om te adverteren wat zijn maximum ontvangstenheid is. Bijvoorbeeld, als een peer adverteert een MRU van 1460, zal die peer geen PPP frame verwerken met een lading groter dan 1460 bytes lang. Cisco PPP-implementatie gebruikt de MTU van de interface als de MRU-waarde die tijdens PPP-onderhandeling wordt geadverteerd. Als MTU is ingesteld als de standaardinstelling van 1500 bytes, wordt er geen MRU geadverteerd, omdat dit de standaardwaarde is voor PPP. Indien de MTU echter op 1460 is ingesteld, wordt een PPP MRU van 1460 geadverteerd. Als de PPP peer luistert naar de MRU die tijdens PPP onderhandeling wordt geadverteerd en zijn MTU (en indirect de IP MTU) voor die PPP verbinding aanpast, kunnen we fragmentatie vermijden. Met een geadverteerde PPP MRU van 1460 moet de peer de IP MTU op 1460 instellen. Dit wijzigt op zijn beurt de TCP MSS dat de peer adverteert wanneer hij TCP verbindingen opent en fragmentatie via het L2TP-netwerk vermijdt.

Een lagere MTU configureren

Gebruik de **opdracht <bytes>** om een lagere MTU te configureren op de virtuele-sjabloon-interface. Nogmaals, dit vereist steun aan de PPP cliënt om aan de geadverteerde MRU tijdens PPP onderhandeling te luisteren. Eén bekende client die luistert naar de MRU-optie is de Windows XP PPP-client. Helaas houden andere veelgebruikte PPP-klienten zich niet aan de geadverteerde PPP-MRU zoals zij zouden moeten doen. Raadpleeg de PPP-clientdocumentatie om te bepalen of de geadverteerde PPP-MRU correct wordt gebruikt. Wanneer L2TP met proxy-LCP wordt uitgevoerd, moet de LCP-heronderhandeling plaatsvinden, aangezien de MRU-optie tijdens de LCP-fase wordt onderhandeld. Om LCP-heronderhandeling mogelijk te maken, moet u **lcp-heronderhandeling configureren op een niet-match** of **lcp-heronderhandeling altijd** onder de **vpdn-groep**.

Eén kwestie van het verlagen van de MTU is dat de MTU van de IP ook automatisch wordt verlaagd. Het is momenteel niet mogelijk om een IP MTU groter te configureren dan de MTU op een virtuele sjabloon-interface. Dit wordt gevolgd door Bug ID CSCdx39828 als een eigenschap/verbeteringsverzoek (niet zichtbaar voor externe gebruikers).

Voor deze methode moeten klanten tijdens de LCP-onderhandelingen naar de MRU-optie luisteren. Er is vaak een mix van klanten: Sommigen luisteren naar MRU, sommigen niet. De klanten die MRU negeren, lopen de PMTUD-problemen op die in de sectie worden beschreven. [Automatisch de IP-MTU aanpassen](#). Voor deze klanten kunt u een andere workround gebruiken door PMTUD effectief uit te schakelen door het DF-bit op het binnen IP-pakket vrij te maken. U kunt dit doen met de volgende configuratie:

```
interface virtual-template1
```

```
ip policy route-map clear-df
!  
route-map clear-df permit 10  
  match ip address 101  
  set ip df 0  
!  
access-list 101 permit tcp any any
```

Conclusie

Cisco IOS-software biedt veel manieren om L2TP-switchingprestaties te maximaliseren. PMTUD is een ideale oplossing. Als gevolg van problemen op het internet is het echter niet altijd betrouwbaar. Cisco IOS-software biedt een aantal alternatieve mechanismen om L2TP-switchingprestaties hoog te houden en de gebruikersconnectiviteit te maximaliseren.

Gerelateerde informatie

- [RFC2923: TCP-problemen met detectie van padMTU](#)
- [IP MTU, TCP MSS en PMTUD op Windows- en Sun-systemen aanpassen](#)
- [Kiezen - Ondersteuning voor toegangstechnologie](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)