

Réglage MTU pour L2TP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Exemple de fragmentation](#)

[Les questions](#)

[Méthodes de accord de MTU](#)

[Configurer manuellement un IP MTU inférieur](#)

[Ajuster PMTU sur des PC de Windows](#)

[Ajuster automatiquement l'IP MTU](#)

[Ajuster le TCP MSS](#)

[Configurer un MTU inférieur](#)

[Conclusion](#)

[Informations connexes](#)

Introduction

Ce document décrit la fragmentation et le réassemblage de liens L2TP et explique comment le réglage de Maximum Transmission Unit (MTU) peut aider à atténuer certains des problèmes qui y sont liés.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir la connaissance de :

- Commandes de configuration générales de Réseau privé virtuel à accès commuté (VPDN)
- Thèmes de général IP tels que la fragmentation, remontage, MTU, encapsulation, en-têtes, et ainsi de suite.

Composants utilisés

La plupart des améliorations de configuration et de caractéristique discutées ici sont disponibles dans des versions de logiciel 12.1T ou 12.2T de Cisco IOS® et plus tard. Cependant, référez-vous aux différentes sections au-dessous du pour en savoir plus.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

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

Exemple de fragmentation

Vous parfois devez fragmenter les paquets tunnel-encapsulés afin d'être les transmettez sur le fil. Voici un exemple de ceci.

Dans le cas de L2TP au-dessus d'UDP, le temps système de tous les protocoles inclut un ensemble supplémentaire d'en-têtes IP, d'UDP et L2TP. L'en-tête IP est de 20 octets, l'en-tête d'UDP est de 8 octets, et l'en-tête L2TP est généralement de 12 octets. Les 12 octets de l'en-tête L2TP incluent :

- la version et les champs d'indicateur (2 octets)
- l'id de tunnel et l'id de session met en place (2 octets chacun)
- 2 octets de décalage de remplissage
- 4 octets d'encapsulation de Protocole point à point (PPP)

Ce diagramme affiche plus de détails :

Si vous activez le séquençage de données (il est désactivé par défaut sur des périphériques de Cisco), vous devez ajouter les 4 octets supplémentaires pour les champs NS et de Nr. Ajoutez les en-têtes IP, d'UDP et L2TP pour voir que L2TP au-dessus d'UDP ajoute 40 octets d'encapsulation de protocole au paquet.

Quand vous encapsulez des 1500 paquets IP d'octet dans L2TP, le paquet encapsulé devient de 1540 octets (1500 + 40 octets d'en-têtes IP, d'UDP et L2TP). Vous devez fragmenter le paquet afin de le transmettre au-dessus d'une interface standard d'Ethernet-type (qui a un MTU de 1500 octets). Le paquet encapsulé est fragmenté dans deux. Le premier fragment se compose de 1500 octets (1460 octets du paquet IP d'origine + 40 octets d'encapsulation L2TP). Le deuxième fragment se compose de 60 octets (40 derniers octets du paquet IP d'origine + 20 octets de temps système IP).

Remarque: Seulement le premier fragment contient l'en-tête L2TP ; le deuxième fragment contient seulement une en-tête IP. Ceci permet au pair L2TP, que ce soit un LAC ou un LNS, pour rassembler les deux fragments dans l'original paquet tunnel-encapsulé 1540 par octets.

Les questions

Un des problèmes que le Layer 2 Tunneling Protocol (L2TP) au-dessus du Protocole UDP (User Datagram Protocol) et de la face basée sur IP de protocoles de l'autre Tunnellisation de la couche 2 et de la couche 3 est que le temps système du protocole de Tunnellisation augmente la taille du paquet tunnel-encapsulé. Quand le paquet d'origine est déjà normal, vous devez fragmenter le

paquet tunnel-encapsulé afin de le transmettre sur le fil.

Un des problèmes que fragmenter et rassembler le paquet L2TP les causes sur L2TP Access concentrateur (LAC) et de serveur de réseau L2TP (LNS) est que la fragmentation et le remontage est faite au niveau de processus en logiciel de Cisco IOS. En agrégeant un grand nombre de sessions L2TP et de circulation sur un LNS, la commutation de processus peut excessivement réduire la représentation. Pour cette raison, il est fortement désirable de réduire ou éliminer le besoin de fragmentation et de remontage dans le chemin de commutation L2TP.

Utilisez une des méthodes décrites dans ce document pour ajuster le Maximum Transmission Unit (MTU) afin de résoudre ceci.

[Méthodes de accord de MTU](#)

Un grand choix de configurations et de caractéristiques en logiciel de Cisco IOS ont été conçues pour éviter la fragmentation et le remontage dans le chemin de commutation L2TP en ajustant le MTU.

[Configurer manuellement un IP MTU inférieur](#)

Configurez un IP MTU inférieur sur l'interface de modèle virtuel utilisant la commande d'**ip mtu**. Configurer un IP MTU inférieur force le routeur pour relâcher tous les paquets IP qui dépassent l'IP MTU et ont le bit DF (Don't Fragment) réglé dans l'en-tête IP. Le routeur génère alors un inaccessible d'hôte du type 3 de Protocole ICMP (Internet Control Message Protocol), codent le message 4 nécessaire par fragmentation vers la source du paquet (l'hôte d'origine). Ce message indique l'IP MTU de l'interface, de sorte que la source puisse réduire la longueur de paquet pour s'adapter par l'interface. Ce processus est également connu en tant que détection de MTU de chemin (PMTUD). Le pour en savoir plus, se rapportent à [RFC 1191](#) . [Configurez l'IP MTU à la plus grande taille de paquets IP qui ne dépassera pas le PMTU entre le LAC et le LNS quand la pleine en-tête L2TP est ajoutée. Pour 1500 un octet PMTU et une en-tête de l'octet L2TP de la norme 40, placez l'IP MTU à 1460 \(en-tête d'octet 1500-40\).](#)

Si le PMTU est inconnu (ou des modifications) entre le LAC et le LNS, vous pouvez configurer l'**ip pmtu** de commande sous le vpdn-groupe. La commande d'**ip pmtu** a été ajoutée dans le Logiciel Cisco IOS version 12.2(4)T utilisant l'ID CSCds72714 de bogue (non visualisable aux utilisateurs externes). La caractéristique d'**ip pmtu** copie le bit DF du paquet intérieur sur l'en-tête extérieure L2TP et active PMTUD entre le routeur et son point final de tunnel L2TP.

[Ajuster PMTU sur des PC de Windows](#)

Microsoft Windows a des paramètres de registre qui te permettent pour activer une caractéristique d'interruption pour leur détection PMTU. Pour les informations sur Windows NT, voyez l'article suivant sur le site Web de Microsoft : [Modification d'algorithme de détection de trou noir PMTU pour Windows NT 3.51 \(Q136970\)](#) .

Pour Windows 2000/XP, l'article de Microsoft [comment dépanner les problèmes de routeur de trou noir \(Q314825\)](#) décrit de diverses méthodes dans Windows pour éviter cette question. [Cet article définit le routeur de « trou noir » de terme, décrit une méthode de localiser des Routeurs de trou noir, et suggère trois manières d'éviter la perte de données qui peut se produire en raison d'un routeur de trou noir.](#)

Ajuster automatiquement l'IP MTU

Vous pouvez également activer le réglage automatique de l'IP MTU. Cette caractéristique permet au routeur pour ajuster automatiquement l'IP MTU sur l'interface d'accès virtuel pour compenser la taille de l'en-tête L2TP et le MTU de l'interface de sortie. Cette caractéristique a été ajoutée dans le Logiciel Cisco IOS version 12.1(5)T utilisant l'ID [CSCdr01713](#) (clients [enregistrés de](#) bogues seulement).

Remarque: L'IP MTU est seulement ajusté automatiquement s'il n'y a aucun IP MTU manuellement configuré sur l'interface de modèle virtuel (utilisant l'option dans la section précédente).

Au commencement, cette caractéristique a été activée par défaut sans la méthode la désactiver. Introduisez des erreurs pour tests l'ID [CSCdt67753](#) (clients [enregistrés](#) seulement) dans des versions du logiciel Cisco IOS 12.2(3) et 12.2(4)T plus tard a ajouté l'**ip mtu adjust de** commande **[non]** sous le **vpdn-groupe** pour activer et désactiver la caractéristique. Le par défaut était d'avoir la fonction activée. Cette caractéristique n'a pas une interface de ligne de commande (CLI) pour changer le par défaut seulement pour les connexions L2X, qui ne lient pas à un **vpdn-groupe** (tel qu'un L2F ou un tunnel L2TP SGBP-initié). L'incapacité de le désactiver pour des topologies du PPP de Multichassis Multilink (MMPPP), combinées avec les problèmes PMTUD décrits ci-dessous, a entraîné beaucoup de plaintes d'utilisateur. Pour cette raison, le par défaut a été changé pour faire ajuster l'automatique d'IP MTU la caractéristique commencer désactivé dans les versions du logiciel Cisco IOS 12.2(6) et le 12.2(8)T et plus tard utilisant l'ID [CSCdu69834](#) (clients [enregistrés de](#) bogues seulement).

Le réglage manuel et automatique du MTU se fondent sur le PMTUD entre les hôtes d'extrémité. Tandis que correct dans la théorie, PMTUD ne fonctionne pas bien sur l'Internet. Voir le [RFC 2923](#) pour une description détaillée de la façon dont PMTUD se casse sur l'Internet. [Le plus grand problème est la présence des « trous noirs » qui font sembler des téléchargements de page Web s'arrêter dans le milieu du courant. Ces trous noirs sont généralement provoqués par des Pare-feu ou des Routeurs configurés pour filtrer des messages ICMP. Quand la source des grands paquets ne peut pas recevoir le message « inaccessible » d'hôte d'ICMP du routeur, indiquant que le MTU a été dépassé, elle ne peut pas réduire la longueur de paquet. Au lieu de cela, il continue à essayer et retransmettre le même paquet à plusieurs reprises avec le positionnement de bit DF. Ces paquets sont lâchés par le LNS puisqu'ils dépassent PMTU et la connexion cesse de répondre.](#)

En raison des problèmes se fondant sur PMTUD pour détecter que l'IP MTU est plus petit au-dessus d'un tunnel L2TP, Cisco a ajouté le TCP la taille que maximum de segment (MSS) ajustent la caractéristique dans le Logiciel Cisco IOS version 12.2(4)T.

Ajuster le TCP MSS

La taille maximum de segment de TCP ajustent la caractéristique - ajoutée par l'ID [CSCds69577](#) (clients [enregistrés de](#) bogues seulement) disponible dans le Logiciel Cisco IOS version 12.2(4)T et permettent plus tard au routeur pour modifier le TCP MSS annoncé dans entrant et sortant synchronisez les paquets (de SYN) envoyés vers la fin des serveurs. En modifiant le TCP MSS à une valeur inférieure que le par défaut habituel de 1460, vous pouvez éliminer le TCP comme source des paquets normaux. Le TCP MSS devrait être ajusté à une valeur tels qu'un segment de TCP avec une en-tête TCP/IP et encapsulé dans L2TP au-dessus d'UDP ne dépasse pas l'IP MTU de l'interface de sortie. Une en-tête TCP/IP est généralement de 40 octets et le L2TP au-dessus de l'en-tête d'UDP est les 40 octets supplémentaires. Par conséquent, généralement le

TCP MSS devrait être ajusté à 1420 (en-tête TCP/IP de 1500 - 40 octets - 40 octets L2TP au-dessus d'en-tête d'UDP).

La commande utilisée pour ceci est des `<mss d'ip tcp adjust-mss >`, qui est une commande de niveau d'interface.

La dernière option pour réduire la fragmentation dans un réseau L2TP exige le support pour le maximum reçoivent la négociation de l'unité (MRU) sur le client de protocole point-à-point. L'option MRU dans le PPP permet à un pair pour annoncer ce que son maximum reçoivent l'unité est. Par exemple, si un pair annonce un MRU de 1460, ce pair ne traitera pas une trame PPP avec de plus grands que 1460 octets d'une charge utile long. L'implémentation de PPP de Cisco utilise le MTU de l'interface comme la valeur MRU qu'elle a annoncée pendant la négociation PPP. Si le MTU est placé comme par défaut de 1500 octets, aucun MRU n'est annoncé, comme c'est le par défaut standard pour le PPP. Cependant, si le MTU est placé à 1460, un PPP MRU de 1460 est annoncé. Si le pair de PPP écoute le MRU annoncé pendant la négociation PPP et ajuste son MTU (et indirectement l'IP MTU) pour ce lien de PPP, nous pouvons éviter la fragmentation. Avec un PPP annoncé MRU de 1460, le pair devrait placer l'IP MTU à 1460. Ceci, consécutivement, modifie le TCP MSS que le pair annonce en ouvrant des connexions TCP et évite la fragmentation au-dessus du réseau L2TP.

Configurer un MTU inférieur

Utilisez les `<bytes >` la commande de `mtu` de configurer un MTU inférieur sur l'interface de modèle virtuel. De nouveau, ceci exige du support sur le client de PPP d'écouter le MRU annoncé pendant la négociation PPP. Un client connu qui écoute l'option MRU est le client de PPP de Windows XP. Malheureusement, d'autres clients commun-déployés de PPP n'adhèrent pas au PPP annoncé MRU comme ils devraient. Référez-vous à la documentation de client de PPP pour déterminer si elle utilise correctement le PPP annoncé MRU. En exécutant L2TP avec le proxy-LCP, les besoins de lcp renegotiation d'avoir lieu puisque l'option MRU est négociée pendant la phase LCP. Pour activer le lcp renegotiation, configurez la **sur-non-concordance de lcp renegotiation** ou le **lcp renegotiation toujours** sous le `vpdn-groupe`.

Une question avec diminuer le MTU est que l'IP MTU automatiquement est aussi bien diminué. Il n'est actuellement pas possible de configurer un IP MTU plus grand que le MTU sur une interface de modèle virtuel. Ceci est déposé par l'ID CSCdx39828 de bogue comme caractéristique/demande d'amélioration (non visualisables aux utilisateurs externes).

Cette méthode exige des clients d'écouter l'option MRU pendant la négociation LCP. Il y a souvent un mélange de clients : certains qui écoutent MRU, certains qui ne font pas. Les clients qui ignorent le passage MRU dans les problèmes PMTUD ont décrit dans la section [ajustant automatiquement l'IP MTU](#). Pour ces clients, vous pouvez utiliser un contournement différent en arrêtant efficacement PMTUD en effaçant le bit DF sur le paquet IP intérieur. Vous pouvez faire ceci avec la configuration suivante :

```
interface virtual-templatel
  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
```

Conclusion

Le logiciel de Cisco IOS fournit beaucoup de manières de maximiser la performance de commutation L2TP. PMTUD est une solution idéale. Cependant, en raison des problèmes sur l'Internet, il n'est pas toujours fiable. Le logiciel de Cisco IOS fournit quelques mécanismes alternatifs pour garder la haute de performance de commutation L2TP et pour maximiser la Connectivité d'utilisateur.

[Informations connexes](#)

- [RFC2923 : Problèmes de TCP avec la découverte de MTU de la voie d'accès](#)
- [Réglage de IP MTU, TCP MSS et PMTUD sur Windows et Sun Systems](#)
- [Support technique d'accès commuté](#)
- [Support et documentation techniques - Cisco Systems](#)