Contenu

Introduction

Ce document décrit comment le Layer 2 Tunneling Protocol (L2TP) dans StarOS est mis en application sur l'ASR5k et dépanne L2TP scrutant - L2TPTunnelDownPeerUnreachable.

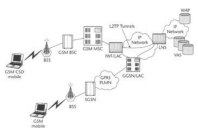
Quel est L2TP ?

L2TP étend la nature point par point du PPP. L2TP fournit une méthode d'encapsulation pour la transmission des trames PPP percées un tunnel, qui permet les points finaux de PPP à percer un tunnel au-dessus d'un réseau de commutation de paquets. L2TP le plus généralement est déployé dans les scénarios de distant-Access-type qui emploient l'Internet pour offrir des services d'intranet-type. Le concept est celui d'un réseau privé virtuel (VPN).

Les deux éléments physiques primaires de L2TP sont le concentrateur L2TP Access (LAC) et le serveur de réseau L2TP (LNS) :

- LAC : Le LAC est un pair au LNS qui agit en tant qu'un côté du périphérique du tunnel. Le LAC termine la connexion PPP distante et se repose entre le distant et le LNS. Des paquets sont expédiés à et de la connexion distante au-dessus de la connexion PPP. Des paquets à et du LNS sont expédiés au-dessus du tunnel L2TP.
- LNS : Le LNS est un pair au LAC qui agit en tant qu'un côté du périphérique du tunnel. Le LNS est le point d'arrêt pour les sessions percées un tunnel par PPP de LAC. Ceci est utilisé pour agréger les sessions PPP et le d'entrée LAC-percés un tunnel par multiple dans le réseau privé.

L2TP simplifié a installé dans le réseau mobile, suivant les indications de cette image.



Il y a deux types de message différents que L2TP utilise :

- Messages de contrôle : L2TP passe des messages de contrôle et de données au-dessus du contrôle et des voies de transmission de données distincts. Le canal de contrôle d'intrabande passe la Gestion ordonnancée de connexion de contrôle, le programme de maintenance, le rapport d'erreurs, et les messages de Contrôle de session. L'initiation de la connexion de contrôle n'est pas spécifique au LAC ou au LNS mais, plutôt, au créateur de tunnel et au récepteur qui a la pertinence dans l'établissement de la connexion de contrôle. Une méthode d'authentification de défi de partager-secret est utilisée entre les périphériques du tunnel.
- Messages de données : Des messages de données sont utilisés pour encapsuler les trames PPP qui sont envoyées dans le tunnel L2TP.

L'écoulement d'appel détaillé et l'établissement de tunnel est expliqué ici :

http://www.cisco.com/c/en/us/support/docs/dial-access/virtual-private-dialup-network-vpdn/23980-l2tp-23980.html

Où l'utilisons-nous dans la mobilité ?

Le déploiement typique est pour des utilisateurs en entreprise où le GGSN agit en tant que LAC et établit sécurise des tunnels vers le LNS qui est actionné dans le réseau d'entreprise. Les écoulements d'appel détaillé sont disponibles dans l'annexe du guide de configuration GGSN qui peut être trouvée, par version de logiciel spécifique, ici :

http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html

Quel est ASR5x00 dans cette installation ?

ASR5k peut prendre en charge la fonctionnalité de LAC et LNS.

Support de LAC L2TP

L2TP établit des tunnels de contrôle L2TP entre le LAC et le LNS avant de percer un tunnel les connexions PPP d'abonné comme sessions L2TP. Le service de LAC est basé sur la même architecture que le GGSN et les avantages de l'allocation de ressources dynamique et le message et le traitement de données distribués. Cette conception permet au service de LAC pour la prendre en charge plus de 4000 installations par seconde ou maximum de 3G fini de débit. Il peut y avoir un maximum supérieur à 65535 sessions dans un tunnel simple et autant d'en tant que 500,000 sessions L2TP utilisant 32,000 tunnels par système.

Support L2TP LNS

Le système configuré comme serveur de réseau de Layer 2 Tunneling Protocol (LNS) prend en charge les tunnels sécurisés du réseau privé virtuel d'arrêt (VPN) entre des concentrateurs L2TP Access (LACS).

L2TP établit des tunnels de contrôle L2TP entre le LAC et le LNS avant de percer un tunnel les connexions PPP d'abonné comme sessions L2TP. Il peut y a un maximum de jusqu'à 65535 sessions dans un tunnel simple et de jusqu'à 500,000 sessions par LNS.

L'architecture LNS est semblable au GGSN et utilise le concept d'un démultiplexeur pour assigner intelligemment de nouvelles sessions L2TP à travers les ressources disponibles en logiciel et en matériel sur la plate-forme sans intervention d'un opérateur.

Le pour en savoir plus se réfèrent des guides de configuration PGW/GGSN.

Configuration pour activer des services sur les périphériques de Cisco

Exemple de configuration pour le LAC sur ASR5k

Exemple de configuration pour le LNS sur ASR5k

> Remarque: Des plusieurs adresses sur la même interface IP peuvent être liées à différents services LNS. Cependant, chaque adresse peut être liée à seulement un service LNS. En outre, le service LNS ne peut pas être lié à la même interface que d'autres services tels qu'un service de LAC.

Exemple de configuration pour le LNS sur le périphérique de Cisco IOS

Ceci peut être utilisé comme exemple de configuration le prenant en charge pour la configuration Cisco IOS et n'est pas sujet à cet article.

Configuration LNS

Dépannez l'événement inaccessible de pair

Cette section donnera quelques instructions sur la façon dont dépanner l'événement L2TPTunnelDownPeerUnreachable dans le réseau. Il est expliqué ici concernant le RP clôturé par PDSN mais les étapes de dépannage sont le même pour le dépannage avec GGSN/PGW.

Comme rappel, un LAC au tunnel LNS est créé afin de contenir des sessions d'abonné tandis qu'il étend la connexion d'abonné d'un PDSN/HA/GGSN/PGW au LNS où il est terminé et où une adresse IP est fournie. Si sur un châssis de StarOS, le LNS obtiendra une adresse IP d'un pool d'IP configuré. Si sur un autre LNS, par exemple aux sites du client, l'adresse IP est fournie par le LNS là. Dans le dernier scénario, ceci a pu efficacement tenir compte pour que les utilisateurs se connectent à leur réseau domestique par une exécution de LAC sur un partenaire d'itinérance.

Un tunnel du LAC LNS est d'abord créé pendant que la première session d'abonné est tentée pour être installée, et restera tant que il y a des sessions dans le tunnel.

Quand la dernière session finit pour un tunnel donné, ce tunnel est fermé ou arrêté. Plus d'un

tunnel peut être établi entre les mêmes pairs LAC-LNS.

Voici un extrait de sortie du **show l2tp de** commande **perce un tunnel tout** ce qui affiche que ceci dans ce cas le châssis héberge des services de LAC et LNS (TestLAC et TestLNS). Notez que TOUS le LAC et le LNS perce un tunnel ont des sessions, alors que quelques tunnels fermés RP n'ont aucune session.

La configuration de services peut être visualisée avec

Voici un exemple du déroutement L2TPTunnelDownPeerUnreachable avec le service 1.1.1.2 de LAC et le service LNS (pair) 1.1.1.1

Obtenez un compte de combien de fois ce déroutement a été déclenchées (puisque recharge ou dernière remise des statistiques) utilisant les **statistiques de show snmp trap de** commande

Le déroutement L2TPTunnelDownPeerUnreachable est déclenché pour L2TP quand un délai d'attente d'installation de tunnel se produit OU des paquets de keep-alive (bonjour) ne sont pas répondues à. La cause est habituellement due au pair LNS ne répondant pas aux demandes des questions de LAC ou de transport dans l'un ou l'autre de direction.

Il n'y a aucun déroutement pour indiquer que le pair devient accessible, qui, si on ne le comprend pas comment étudier plus plus loin, peut mener à la confusion de savoir si il y a toujours une question ou pas au moment d'enquête (demande de caractéristique).

Pour poursuivre, la plupart de partie importante que nous avons besoin est l'adresse IP de pair. La première étape est de s'assurer qu'il y a de la connectivité IP qui peut être vérifiée avec le PING. S'il y a de Connectivité vous pouvez poursuivre met au point

Notes :

l2tpmgr dépiste l'installation spécifique de session d'abonné

l2tp-control dépiste l'établissement de tunnel :

Voici l'échantillon mettent au point de cette sortie

Cas d'utilisation : Le tunnel initial a installé la panne devant relancer des délais d'attente

Voici le déroutement résultant SNMP déclenché pour apparier les logs ci-dessus pour le moment que le système a déterminé la panne

Cas d'utilisation : Le tunnel initial a installé la panne devant relancer des délais d'attente - analyse

Ce que nous voyons est ce tunnel monte à 16:34 et il tente d'envoyer le défi pendant cinq fois. Apparemment, il n'y a aucune réponse et par la suite les débranchements de tunnel.

Examinez les par défaut de configuration ou les valeurs configurées et voyez

Cette configuration doit interpeted comme les retransmettent d'abord après 1 seconde, puis augmentation exponentielle - doublant chaque fois : 1, 2, 4, 8, 8.

Notez les maximum-retransmissions de terme (cinq) inclut le premier essai/transmission.
retransmission-délai d'attente-maximum est la durée maximale entre les transmissions après (si) cette limite est atteinte
le retransmission-délai d'attente-premier est le point commençant de combien de temps attendre avant la première retransmission.

Ainsi, faisant le calcul, dans le cas des paramètres par défaut, une panne se produirait après 1+ 2 + 4 + 8 + 8 secondes = 23 secondes, qui est vu exactement comme dans la sortie ci-dessous.

Cas d'utilisation : Panne initiale d'installation de tunnel due au Keepalives

L'autre raison pour le déroutement L2TPTunnelDownPeerUnreachable n'est aucune réponse aux messages de keepalive-intervalle. Ceux-ci sont utilisés au cours des périodes où il n'y a aucun message ou donnée de contrôle étant envoyée au-dessus du tunnel, pour s'assurer que l'autre extrémité est encore active. S'il y a des sessions dans le tunnel, mais ils ne font rien, cette commande s'assure que le tunnel fonctionne toujours correctement, parce qu'en l'activant, des messages de keepalive sont envoyés après que la période configurée sans échange de paquet (c.-à-d. 60 secondes), et des réponses soient prévues. La fréquence d'envoyer la keepalive après avoir envoyé le premier et ne pas avoir obtenu une réponse est identique comme décrit ci-dessus pour l'installation de tunnel. Ainsi, après 23 secondes de ne pas recevoir une réponse bonjour aux messages (de keepalive), le tunnel sera démoli. Voir le keepalive-intervalle configurable (par défaut = 60s).

Voici les exemples de l'échange réussi de keep-alive, les deux de l'abonné de moniteur et de se connecter. Notez l'intervalle d'une minute entre les ensembles de messages en raison d'aucune données d'utilisateur étant transmises pour une minute. Dans cet exemple, les services du LAC et LNS se trouvent dans le même châssis, dans les contextes nommés **destination** et **lns** respectivement.

En conclusion, voici un exemple à où, pour un tunnel existant, des messages Hello ne sont pas répondus, et l'appel et le tunnel sont démolis. Surveillez l'abonné sorti :

Voici les logs respectifs.

Notez le délai d'attente de tunnel de contrôle de sortie - cinq relance-tentés, ms du dernier-intervalle 8000 pour les essais ratés.

Et déroutement correspondant SNMP

Affichez les considérations de sortie

Exécuter la commande suivante indiquera s'il y a eu les questions d'accessibilité de pair avec un pair spécifique (ou pour tous les tunnels dans un service particulier de LAC/lns)

Les connexions actives contre- apparie le nombre de tunnels existants pour ce pair là peuvent être plus d'un, comme vu dans pour sortir du show l2tp perce un tunnel tous de plus tôt.

Pour connecter le compteur indiquera combien de pannes d'installation de tunnel se sont produites.
Le compteur dépassé par relance maximum est probablement le compteur le plus important, car il indique le manque de connecter en raison d'un délai d'attente (chaque relance dépassée a comme conséquence un déroutement L2TPTunnelDownPeerUnreachable). Ces informations

vous indiquent seulement que la fréquence du problème pour un pair indiqué, il ne t'indique pas pourquoi le délai d'attente s'est produit. Mais connaître la fréquence peut être utile en remontant les parties dans le processus de dépannage global.

La section de sessions fournit le détail au niveau de session d'abonné (contre le niveau de tunnel) Les sessions actives parent des correspondances que la somme (si plus d'un tunnel pour un pair) de la colonne active de Sess sortie du show l2tp perce un tunnel pour le pair particulier.
Pour connecter le compteur indique combien de sessions ne se sont pas connectées. Notez que les installations défectueuses de session ne déclenchent pas le déroutement L2TPTunnelDownPeerUnreachable, seulement les installations défectueuses de tunnel font.

Il y a également des compteurs que la version des tunnels de show l2tp commandent qui peuvent être utiles.

En conclusion, au niveau de session, tous les abonnés pour un pair donné peuvent être visualisés.

Le nombre d'abonnés trouvés devrait apparier le nombre de sessions actives comme discuté.