MTU-Tuning für L2TP

Inhalt

Einführung

In diesem Dokument wird die Fragmentierung und Reassemblierung auf L2TP-Verbindungen beschrieben. Außerdem wird erläutert, wie die MTU-Optimierung (Maximum Transmission Unit) bei der Behebung einiger der damit verbundenen Probleme helfen kann.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten über Folgendes verfügen:

- Allgemeine VPDN-Konfigurationsbefehle (Virtual Private Dialup Network)
- Allgemeine IP-Themen wie Fragmentierung, Reassemblierung, MTU, Kapselung, Header usw.

Verwendete Komponenten

Die meisten der hier besprochenen Konfigurations- und Funktionsverbesserungen sind in den Cisco IOS® Software Releases 12.1T oder 12.2T und höher enthalten. Weitere Informationen finden Sie jedoch in den einzelnen Abschnitten weiter unten.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

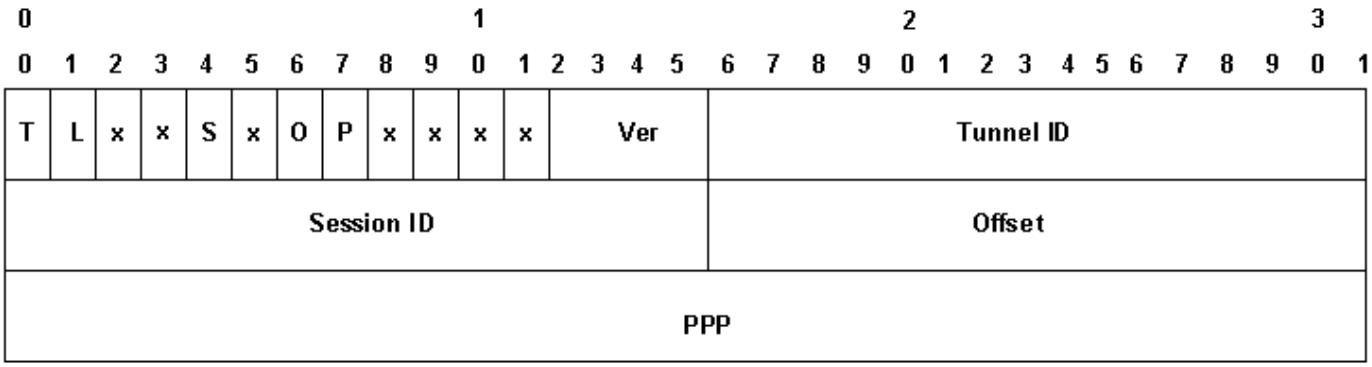
Fragmentierungsbeispiel

Manchmal müssen Sie Pakete mit Tunnelkapselung fragmentieren, um sie über die Leitung zu übertragen. Hier ein Beispiel dafür.

Bei L2TP über UDP umfasst der Overhead aller Protokolle einen zusätzlichen Satz von IP-, UDP- und L2TP-Headern. Der IP-Header hat 20 Byte, der UDP-Header 8 Byte und der L2TP-Header 12 Byte. Die 12 Byte des L2TP-Headers sind:

- die Versionsnummer und die Flagfelder (2 Byte)
- die Felder Tunnel-ID und Session-ID (je 2 Byte)
- 2 Byte Padding-Offset
- 4 Byte Point-to-Point Protocol (PPP)-Kapselung

Dieses Diagramm zeigt weitere Details:



Wenn Sie die Datensequenzierung aktivieren (diese ist auf Cisco Geräten standardmäßig deaktiviert), müssen Sie zusätzliche 4 Byte für die Felder Ns und Nr hinzufügen. Addieren Sie die IP-, UDP- und L2TP-Header, um zu sehen, dass L2TP über UDP dem Paket 40 Byte Protokollkapselung hinzufügt.

Wenn Sie ein 1500-Byte-IP-Paket in L2TP einkapseln, wird das gekapselte Paket zu 1540 Byte (1500 + 40 Byte IP-, UDP- und L2TP-Header). Sie müssen das Paket fragmentieren, um es über eine standardmäßige Ethernet-Schnittstelle (mit einer MTU von 1.500 Byte) zu übertragen. Das gekapselte Paket ist in zwei Teile fragmentiert. Das erste Fragment besteht aus 1.500 Byte (1.460 Byte des ursprünglichen IP-Pakets + 40 Byte L2TP-Kapselung). Das zweite Fragment besteht aus 60 Byte (die letzten 40 Byte des ursprünglichen IP-Pakets + 20 Byte IP-Overhead).

Hinweis: Nur das erste Fragment enthält den L2TP-Header. Das zweite Fragment enthält nur einen IP-Header. Auf diese Weise kann der L2TP-Peer, sei es eine LAC oder ein LNS, die beiden Fragmente wieder in das Tunnelgekapselte ursprüngliche 1540-Byte-Paket einbauen.

Die Probleme

Eines der Probleme, mit denen das Layer 2 Tunneling Protocol (L2TP) über das User Datagram Protocol (UDP) und andere IP-basierte Layer-2- und Layer-3-Tunneling-Protokolle konfrontiert ist, besteht darin, dass der Overhead des Tunneling-Protokolls die Größe des durch Tunnel gekapselten Pakets erhöht. Wenn das ursprüngliche Paket bereits in voller Größe ist, müssen Sie das Paket mit Tunnelkapselung fragmentieren, um es über die Leitung zu übertragen.

Eines der Probleme bei der Fragmentierung und erneuten Zusammenstellung des L2TP-Pakets auf dem L2TP Access Concentrator (LAC) und dem L2TP Network Server (LNS) besteht darin, dass die Fragmentierung und Neuassemblierung in der Cisco IOS-Software auf Prozessebene erfolgt. Wenn eine große Anzahl von L2TP-Sitzungen und Datenverkehrsflüssen in einem LNS zusammengefasst wird, kann Prozess-Switching die Leistung erheblich reduzieren. Aus diesem Grund ist es äußerst wünschenswert, die Notwendigkeit einer Fragmentierung und Reassemblierung im L2TP-Switching-Pfad zu reduzieren oder zu eliminieren.

Verwenden Sie eine der in diesem Dokument beschriebenen Methoden, um die Maximum Transmission Unit (MTU) anzupassen, um dies zu beheben.

MTU-Optimierungsmethoden

Die Cisco IOS-Software bietet eine Vielzahl von Konfigurationen und Funktionen, um eine Fragmentierung und Reassemblierung im L2TP-Switching-Pfad durch Anpassung der MTU zu vermeiden.

Manuelle Konfiguration einer niedrigeren IP-MTU

Konfigurieren Sie mithilfe des Befehls **ip mtu** eine niedrigere IP-MTU auf der Virtual-Template-Schnittstelle. Durch die Konfiguration einer niedrigeren IP-MTU muss der Router alle IP-Pakete verwerfen, die die IP-MTU überschreiten, und das DF-Bit (Don't Fragment) im IP-Header festlegen. Der Router generiert dann eine Internet Control Message Protocol (ICMP)-Nachricht vom Typ 3 Host Unreachable, Code-4-Fragmentierung erforderlich, die an die Quelle des Pakets (den ursprünglichen Host) gesendet wird. Diese Meldung gibt die IP-MTU der Schnittstelle an, sodass die Quelle die Paketgröße so reduzieren kann, dass sie in die Schnittstelle passt. Dieser Prozess wird auch als Path MTU Detection (PMTUD) bezeichnet. Weitere Informationen finden Sie in RFC 1191 . Konfigurieren Sie die IP-MTU auf die größte IP-Paketgröße, die die PMTU zwischen der LAC und dem LNS nicht überschreitet, wenn der vollständige L2TP-Header hinzugefügt wird. Legen Sie für einen 1500-Byte-PMTU und einen standardmäßigen 40-Byte-L2TP-Header die IP-MTU auf 1460 (1500-40-Byte-Header) fest.

Wenn die PMTU nicht bekannt ist (oder Änderungen vornimmt), können Sie den Befehl **ip pmtu** unter der **vpdn-Gruppe** konfigurieren. Der Befehl **ip pmtu** wurde in Version 12.2(4)T der Cisco IOS-Software mit der Bug-ID CSCds72714 (für externe Benutzer nicht sichtbar) hinzugefügt. Die **ip pmtu-**Funktion kopiert das DF-Bit aus dem internen Paket in den externen L2TP-Header und aktiviert die PMTUD zwischen dem Router und seinem L2TP-Tunnel-Endpunkt.

PMTU auf Windows-PCs anpassen

Microsoft Windows verfügt über eine Registrierungseinstellung, mit der Sie eine Backoff-Funktion für die PMTU-Erkennung aktivieren können. Weitere Informationen zu Windows NT finden Sie im

folgenden Artikel auf der Microsoft-Website: PMTU Black Hole Detection Algorithm Change für Windows NT 3.51 (Q136970) .

Für Windows 2000/XP beschreibt der Microsoft-Artikel How to Troubleshoot Black Hole Router Issues (Q314825)verschiedene Methoden in Windows zur Vermeidung dieses Problems. Dieser Artikel definiert den Begriff "Black Hole"-Router, beschreibt eine Methode zum Auffinden von Routern mit schwarzen Löchern und schlägt drei Möglichkeiten vor, um Datenverluste zu vermeiden, die durch einen Black Hole Router auftreten können.

Automatische Anpassung der IP-MTU

Sie können auch die automatische Anpassung der IP-MTU aktivieren. Diese Funktion ermöglicht dem Router die automatische Anpassung der IP-MTU auf der Virtual-Access-Schnittstelle, um die Größe des L2TP-Headers und die MTU der Ausgangsschnittstelle auszugleichen. Diese Funktion wurde in der Cisco IOS Software-Version 12.1(5)T mit der Bug-ID CSCdr01713 hinzugefügt (nur registrierte Kunden).

Hinweis: Die IP-MTU wird nur automatisch angepasst, wenn auf der Virtual-Template-Schnittstelle keine IP-MTU manuell konfiguriert wurde (unter Verwendung der Option im vorherigen Abschnitt).

Zunächst wurde diese Funktion standardmäßig aktiviert, ohne dass sie deaktiviert werden kann. Die Bug-ID CSCdt67753 (nur registrierte Kunden) in den Cisco IOS Software-Versionen 12.2(3) und 12.2(4)T hat später den Befehl **[no] ip mtu adjust** unter der **vpdn-Gruppe** hinzugefügt, um die Funktion zu aktivieren und zu deaktivieren. Standardmäßig sollte die Funktion aktiviert sein. Diese Funktion verfügt nicht über eine CLI (Command Line Interface), um die Standardeinstellung nur für L2X-Verbindungen zu ändern, die nicht an eine **vpdn-Gruppe** gebunden sind (z. B. an einen L2F- oder L2TP-Tunnel, der von SGBP initiiert wurde). Die Unfähigkeit, diese Funktion für Multichassis Multilink PPP (MMPPP)-Topologien zu deaktivieren, führte in Verbindung mit den unten beschriebenen PMTUD-Problemen zu zahlreichen Benutzerbeschwerden. Aus diesem Grund wurde die Standardeinstellung so geändert, dass die Funktion zur automatischen IP-MTU-Anpassung ab den Cisco IOS Software-Versionen 12.2(6) und 12.2(8)T und später mithilfe der Bug-ID CSCdu69834 deaktiviert wird (nur registrierte Kunden).

Sowohl die manuelle als auch die automatische Einstellung der MTU-Größe basiert auf der PMTUD zwischen den End-Hosts. Theoretisch ist die PMTUD im Internet zwar nicht gut genug. Eine detaillierte Beschreibung der Pausen der PMTUD im Internet finden Sie in RFC 2923 . Das größte Problem ist das Vorhandensein von "schwarzen Löchern", die dazu führen, dass die Downloads von Webseiten in der Mitte des Streams hängen. Diese schwarzen Löcher werden im Allgemeinen durch Firewalls oder Router verursacht, die zum Herausfiltern von ICMP-Nachrichten konfiguriert sind. Wenn die Quelle der großen Pakete die Meldung "ICMP Host Unreachable" (ICMP-Host nicht erreichbar) vom Router nicht erhalten kann, die anzeigt, dass die MTU überschritten wurde, kann die Paketgröße nicht reduziert werden. Stattdessen wird weiterhin versucht, dasselbe Paket mit festgelegtem DF-Bit immer wieder neu zu übertragen. Diese Pakete werden vom LNS verworfen, da sie PMTU überschreiten und die Verbindung nicht mehr reagiert.

Aufgrund von Problemen, bei denen die PMTUD erkennt, dass die IP-MTU über einen L2TP-Tunnel kleiner ist, hat Cisco in Version 12.2(4)T der Cisco IOS-Software die Funktion zur Einstellung der maximalen TCP-Segmentgröße (MSS) hinzugefügt.

Anpassen der TCP-MSS

Die Funktion zur Einstellung der maximalen TCP-Segmentgröße wird durch die Bug-ID

CSCds69577 (nur registrierte Kunden) in Version 12.2(4)T der Cisco IOS-Software hinzugefügt und ermöglicht dem Router, die angekündigte TCP-MSS in SYN-Paketen zu ändern, die von den End-Hosts gesendet werden. Wenn Sie die TCP-MSS auf einen niedrigeren Wert als den üblichen Standardwert von 1460 ändern, können Sie TCP als Quelle von Paketen voller Größe eliminieren. Die TCP-MSS sollte so angepasst werden, dass ein TCP-Segment mit einem TCP/IP-Header, das in L2TP über UDP gekapselt ist, die IP-MTU der Ausgangsschnittstelle nicht überschreitet. Ein TCP/IP-Header hat im Allgemeinen 40 Byte und der L2TP-over-UDP-Header 40 Byte. Daher sollte die TCP-MSS im Allgemeinen auf 1420 (1500 - 40 Byte TCP/IP-Header - 40 Byte L2TP über UDP-Header) eingestellt werden.

Der hierfür verwendete Befehl ist **ip tcp adjust-mss <*mss*>** ein Befehl auf Schnittstellenebene.

Die letzte Option zur Reduzierung der Fragmentierung in einem L2TP-Netzwerk erfordert die Unterstützung der MRU-Aushandlung (Maximum Receive Unit) auf dem Point-to-Point Protocol-Client. Die MRU-Option in PPP ermöglicht es einem Peer, anzukündigen, was seine maximale Empfangseinheit ist. Wenn beispielsweise ein Peer eine MRU von 1460 ankündigt, verarbeitet dieser Peer keinen PPP-Frame mit einer Nutzlast von mehr als 1460 Byte. Bei der Cisco PPP-Implementierung wird die MTU der Schnittstelle als MRU-Wert verwendet, der bei der PPP-Aushandlung angekündigt wurde. Wenn die MTU als Standardwert von 1500 Byte festgelegt ist, wird keine MRU angekündigt, da dies der Standardstandard für PPP ist. Wenn die MTU jedoch auf 1460 festgelegt ist, wird eine PPP-MRU von 1460 angekündigt. Wenn der PPP-Peer die während der PPP-Aushandlung angekündigte MRU abhört und seine MTU (und indirekt die IP-MTU) für diese PPP-Verbindung anpasst, können wir eine Fragmentierung vermeiden. Bei einer angekündigten PPP-MRU von 1460 muss der Peer die IP-MTU auf 1460 einstellen. Dies wiederum ändert die TCP-MSS, die der Peer beim Öffnen von TCP-Verbindungen ankündigt, und verhindert eine Fragmentierung über das L2TP-Netzwerk.

Konfigurieren einer niedrigeren MTU

Verwenden Sie den Befehl **mtu <*bytes*>**, um eine niedrigere MTU für die Virtual-Template-Schnittstelle zu konfigurieren. Dies erfordert wiederum Unterstützung auf dem PPP-Client, um die angekündigte MRU während der PPP-Aushandlung anzuhören. Ein bekannter Client, der die MRU-Option abhört, ist der PPP-Client von Windows XP. Leider halten sich andere häufig bereitgestellte PPP-Clients nicht an die angekündigte PPP-MRU. In der PPP-Client-Dokumentation finden Sie, ob die angekündigte PPP-MRU ordnungsgemäß verwendet wird. Wenn L2TP mit Proxy-LCP ausgeführt wird, muss die Neuverhandlung des LCP erfolgen, da die MRU-Option während der LCP-Phase ausgehandelt wird. Um die Neuverhandlung des LCP zu aktivieren, konfigurieren Sie **immer** unter der **vpdn-Gruppe die Neuverhandlung** des **lcp bei Nichtübereinstimmung** oder **die Neuverhandlung** des **LCP**.

Ein Problem bei der Senkung der MTU besteht darin, dass auch die IP-MTU automatisch verringert wird. Es ist derzeit nicht möglich, eine IP-MTU, die größer als die MTU ist, auf einer Virtual-Template-Schnittstelle zu konfigurieren. Diese wird über die Bug-ID CSCdx39828 als Anfrage für Funktionen/Erweiterungen verfolgt (für externe Benutzer nicht sichtbar).

Bei dieser Methode müssen die Clients die MRU-Option während der LCP-Aushandlung abhören. Häufig gibt es verschiedene Clients: Einige hören MRU, andere nicht. Die Clients, die die MRU ignorieren, führen die im Abschnitt Automatische Anpassung der IP-MTU beschriebenen PMTUD-Probleme aus. Für diese Clients können Sie eine andere Problemumgehung einsetzen, indem Sie die PMTUD effektiv ausschalten, indem Sie das DF-Bit auf dem internen IP-Paket löschen. Sie können dies mit der folgenden Konfiguration tun:

```
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
```

Schlussfolgerung

Die Cisco IOS-Software bietet eine Vielzahl von Möglichkeiten zur Maximierung der L2TP-Switching-Leistung. Die PMTUD ist eine ideale Lösung. Aufgrund von Problemen im Internet ist es jedoch nicht immer zuverlässig. Die Cisco IOS-Software bietet einige alternative Mechanismen, um die L2TP-Switching-Leistung hoch zu halten und die Benutzerkonnektivität zu maximieren.

Zugehörige Informationen

- RFC 2923: TCP-Probleme mit MTU-Pfaderkennung
- Anpassen von IP-MTU, TCP-MSS und PMTUD auf Windows- und Sun-Systemen
- Wählen - Zugriff auf Technologie-Support
- Technischer Support und Dokumentation - Cisco Systems