

L2TP용 MTU 튜닝

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[조각화 예](#)

[문제](#)

[MTU 튜닝 방법](#)

[하위 IP MTU 수동 구성](#)

[Windows PC에서 PMTU 조정](#)

[IP MTU 자동 조정](#)

[TCP MSS 조정](#)

[하위 MTU 구성](#)

[결론](#)

[관련 정보](#)

소개

이 문서에서는 L2TP 링크에서 프래그먼트화 및 재어셈블리에 대해 설명하고 MTU(Maximum Transmission Unit) 튜닝을 통해 관련 문제의 일부를 완화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서의 독자는 다음에 대해 알고 있어야 합니다.

- 일반 VPDN(Virtual Private Dialup Network) 구성 명령
- 조각화, 재어셈블리, MTU, 캡슐화, 헤더 등의 일반적인 IP 항목

사용되는 구성 요소

여기에서 설명하는 대부분의 컨피그레이션 및 기능 개선 사항은 Cisco IOS® Software 릴리스 12.1T 또는 12.2T 이상에서 제공됩니다. 그러나 자세한 내용은 아래의 개별 섹션을 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

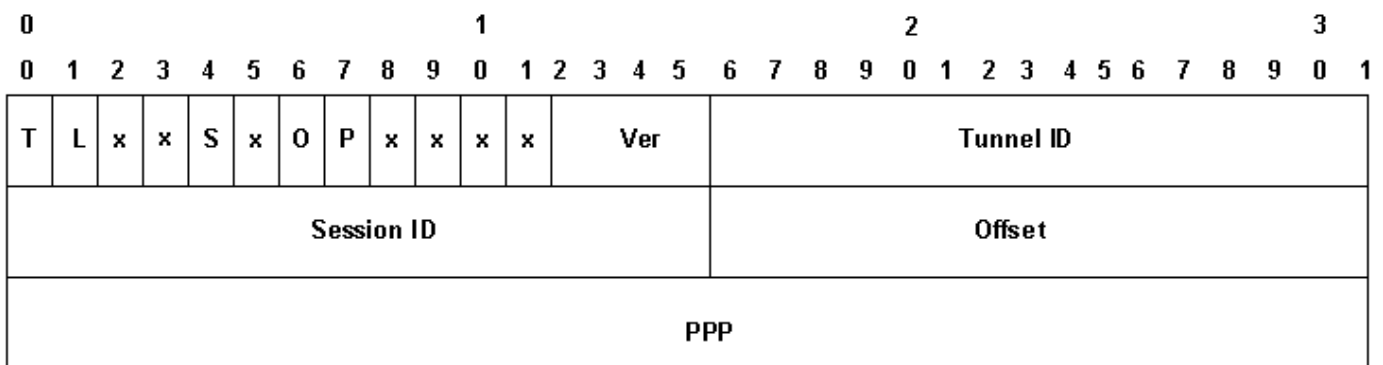
조각화 예

회선에서 전송하려면 터널 캡슐화된 패킷을 조각화해야 하는 경우가 있습니다. 여기 이것의 예가 있습니다.

L2TP over UDP의 경우, 모든 프로토콜의 오버헤드는 추가 IP, UDP 및 L2TP 헤더 집합을 포함합니다. IP 헤더는 20바이트, UDP 헤더는 8바이트, L2TP 헤더는 일반적으로 12바이트입니다. L2TP 헤더의 12바이트는 다음과 같습니다.

- version 및 flag 필드(2바이트)
- 터널 id 및 세션 id 필드(각각 2바이트)
- 패딩 오프셋 2바이트
- PPP(Point-to-Point Protocol) 캡슐화의 4바이트

이 다이어그램에서는 자세한 내용을 보여 줍니다.



데이터 시퀀스를 활성화한 경우(Cisco 디바이스에서 기본적으로 비활성화됨), Ns 및 Nr 필드에 4바이트를 추가해야 합니다. IP, UDP 및 L2TP 헤더를 추가하여 L2TP over UDP가 패킷에 프로토콜 캡슐화의 40바이트를 추가하는지 확인합니다.

1500바이트 IP 패킷을 L2TP로 캡슐화할 경우 캡슐화된 패킷은 1540바이트(IP, UDP 및 L2TP 헤더의 1500 + 40바이트)가 됩니다. 표준 이더넷 유형 인터페이스(MTU 1500바이트)를 통해 전송하려면 패킷을 프래그먼트화해야 합니다. 캡슐화된 패킷은 두 개로 분할됩니다. 첫 번째 프래그먼트는 1500바이트(원래 IP 패킷의 1460바이트 + L2TP 캡슐화의 40바이트)로 구성됩니다. 두 번째 프래그먼트는 60바이트(원래 IP 패킷의 마지막 40바이트 + 20바이트의 IP 오버헤드)로 구성됩니다.

참고: 첫 번째 프래그먼트에만 L2TP 헤더가 포함됩니다. 두 번째 프래그먼트는 IP 헤더만 포함합니다. 이를 통해 LAC 또는 LNS이든 L2TP 피어는 두 프래그먼트를 원래 1540바이트 터널 캡슐화된 패킷으로 재조합할 수 있습니다.

문제

UDP(User Datagram Protocol)를 통한 L2TP(Layer 2 Tunneling Protocol)와 다른 Layer 2 및 Layer 3 IP 기반 터널링 프로토콜에서 발생하는 문제 중 하나는 터널링 프로토콜의 오버헤드가 터널 캡슐화된 패킷의 크기를 증가시킨다는 것입니다. 원래 패킷의 크기가 이미 꽉 찬 경우, 회선에서 전송하려면 터널 캡슐화된 패킷을 프래그먼트화해야 합니다.

L2TP Access Concentrator(LAC) 및 L2TP Network Server(LNS)에서 L2TP 패킷을 조각화하고 리어셈블하는 문제 중 하나는 프래그먼트화 및 재조립이 Cisco IOS 소프트웨어의 프로세스 레벨에서 이루어진다는 것입니다.LNS에서 많은 수의 L2TP 세션 및 트래픽 흐름을 집계할 때 프로세스 스위칭은 성능을 크게 줄일 수 있습니다.따라서 L2TP 스위칭 경로에서 프래그먼트화 및 재조립이 필요한 경우 줄이거나 제거하는 것이 좋습니다.

이 문제를 해결하려면 이 문서에 설명된 방법 중 하나를 사용하여 MTU(최대 전송 단위)를 조정합니다.

MTU 튜닝 방법

Cisco IOS 소프트웨어의 다양한 컨피그레이션 및 기능은 MTU를 조정하여 L2TP 스위칭 경로에서 프래그먼트화 및 재결합을 방지하기 위해 설계되었습니다.

하위 IP MTU 수동 구성

ip mtu 명령을 사용하여 가상 템플릿 인터페이스에서 하위 IP MTU를 구성합니다.낮은 IP MTU를 구성하면 라우터가 IP MTU를 초과하고 IP 헤더에 DF(Don't Fragment) 비트가 설정된 IP 패킷을 강제로 삭제합니다.그런 다음 라우터는 패킷의 소스(원래 호스트)에 대한 코드 4 프래그먼트화 필요 메시지, ICMP(Internet Control Message Protocol) 유형 3 Host Unreachable을 생성합니다. 이 메시지는 소스가 인터페이스를 통과하도록 패킷 크기를 줄일 수 있도록 인터페이스의 IP MTU를 나타냅니다.이 프로세스를 PMTUD(Path MTU Detection)라고도 합니다. 자세한 내용은 [RFC 1191](#)을 참조하십시오.전체 L2TP 헤더가 추가될 때 LAC와 LNS 간의 PMTU를 초과하지 않는 최대 IP 패킷 크기에 IP MTU를 구성합니다.1500바이트 PMTU 및 표준 40바이트 L2TP 헤더의 경우 IP MTU를 1460(1500-40바이트 헤더)으로 설정합니다.

LAC와 LNS 간에 PMTU를 알 수 없거나 변경할 경우 vpdn 그룹 아래에 ip pmtu 명령을 구성할 수 있습니다.ip pmtu 명령은 Bug ID CSCds72714(외부 사용자가 볼 수 없음)를 사용하여 Cisco IOS Software Release 12.2(4)T에 추가되었습니다. ip pmtu 기능은 내부 패킷에서 외부 L2TP 헤더로 DF 비트를 복사하고 라우터와 L2TP 터널 엔드포인트 간에 PMTUD를 활성화합니다.

Windows PC에서 PMTU 조정

Microsoft Windows에는 PMTU 검색에 대한 백오프 기능을 사용하도록 설정하는 레지스트리 설정이 있습니다.Windows NT에 대한 자세한 내용은 Microsoft 웹 사이트에서 다음 문서를 참조하십시오.[Windows NT 3.51\(Q136970\)용 PMTU 블랙홀 탐지 알고리즘 변경](#)

Windows 2000/XP의 경우 Microsoft 문서 [How to Troubleshoot Black Hole Router Issues \(Q314825\)](#) 에서 이 문제를 방지하기 위한 Windows의 다양한 방법에 대해 설명합니다.이 문서에서는 "블랙홀" 라우터라는 용어를 정의하고, 블랙홀 라우터를 찾는 방법을 설명하고, 블랙홀 라우터로 인해 발생할 수 있는 데이터 손실을 방지하는 세 가지 방법을 제안합니다.

IP MTU 자동 조정

IP MTU의 자동 조정을 활성화할 수도 있습니다.이 기능을 사용하면 라우터가 가상 액세스 인터페이스에서 IP MTU를 자동으로 조정하여 이그레스 인터페이스의 L2TP 헤더 및 MTU의 크기를 보완할 수 있습니다.이 기능은 버그 ID CSCdr01713을 사용하여 Cisco IOS Software 릴리스 12.1(5)T에 추가되었습니다([등록된](#) 고객만 해당).

참고: IP MTU는 가상 템플릿 인터페이스에 수동으로 구성된 IP MTU가 없는 경우에만 자동으로 조

정됩니다(이전 섹션의 옵션 사용).

처음에는 이 기능을 비활성화하는 방법 없이 기본적으로 활성화했습니다. Cisco IOS Software 릴리스 12.2(3) 및 12.2(4)T의 버그 ID [CSCdt67753\(등록된 고객만 해당\)](#)에서 나중에 이 기능을 활성화하거나 비활성화하기 위해 vpdn 그룹에서 **[no] ip mtu adjust** 명령을 추가했습니다. 기본적으로 이 기능이 활성화되어 있어야 합니다. 이 기능에는 L2X 연결에 대해서만 기본값을 변경할 수 있는 CLI(Command Line Interface)가 없으며, vpdn 그룹(예: SGBP 시작 L2F 또는 L2TP 터널)에 바인딩되지 않습니다. MPPPP(Multichassis Multilink PPP) 토폴로지에 대해 이 옵션을 비활성화할 수 없어 아래에 설명된 PMTUD 문제와 함께 많은 사용자 불만이 발생했습니다. 따라서 Cisco IOS Software Release 12.2(6) 및 12.2(8)T 이상에서 Bug ID [CSCdu69834\(등록된 고객만\)](#)를 사용하여 IP MTU 자동 조정 기능을 비활성화하도록 기본값이 변경되었습니다.

MTU의 수동 및 자동 조정 모두 최종 호스트 간의 PMTUD에 의존합니다. 이론적으로는 괜찮지만, PMTUD는 인터넷에서 잘 작동하지 않습니다. 인터넷에서 PMTUD가 어떻게 중단되는지에 대한 자세한 설명은 RFC 2923 을 참조하십시오. 가장 큰 문제는 웹 페이지 다운로드가 스트림 중간에 멈춘 것처럼 보이는 "블랙홀"이 있다는 것입니다. 이러한 블랙홀은 일반적으로 ICMP 메시지를 필터링하도록 구성된 방화벽 또는 라우터에 의해 발생합니다. 큰 패킷의 소스가 라우터에서 "ICMP Host Unreachable" 메시지를 수신할 수 없는 경우, MTU가 초과되었음을 나타내는 경우 패킷 크기를 줄일 수 없습니다. 대신 DF 비트 세트를 사용하여 동일한 패킷을 반복해서 재전송하려고 시도합니다. 이러한 패킷은 PMTUD를 초과하고 연결이 응답하지 않으므로 LNS에서 삭제됩니다.

PMTUD를 사용하여 L2TP 터널을 통해 IP MTU가 더 작음을 감지하는 데 문제가 있기 때문에 Cisco는 Cisco IOS Software Release 12.2(4)T에서 TCP MSS(Maximum Segment Size) 조정 기능을 추가했습니다.

[TCP MSS 조정](#)

TCP Maximum Segment Size 조정 기능 - Cisco IOS Software Release 12.2(4)T 이상에서는 Bug ID [CSCds69577\(등록된 고객만 해당\)](#)에 추가됨을 사용하면 라우터가 엔드 호스트에서 보낸 수신 및 발신 동기화(SYN) 패킷에서 알려진 TCP MSS를 수정할 수 있습니다. TCP MSS를 일반적인 기본값인 1460보다 낮은 값으로 수정하면 TCP를 전체 크기의 패킷의 소스로 제거할 수 있습니다. TCP MSS는 TCP/IP 헤더가 있고 L2TP over UDP에 캡슐화된 TCP 세그먼트가 이그레스 인터페이스의 IP MTU를 초과하지 않도록 값으로 조정해야 합니다. TCP/IP 헤더는 일반적으로 40바이트이며 L2TP over UDP 헤더는 추가 40바이트입니다. 따라서 일반적으로 TCP MSS는 1420(1500 - 40바이트 TCP/IP 헤더 - 40바이트 L2TP over UDP 헤더)으로 조정되어야 합니다.

이 명령에 사용되는 명령은 **ip tcp adjust-mss <mss>**이며, 이는 인터페이스 레벨 명령입니다.

L2TP 네트워크에서 단편화를 줄이기 위한 마지막 옵션은 Point-to-Point 프로토콜 클라이언트에서 MRU(Maximum Receive Unit) 협상을 지원해야 합니다. PPP의 MRU 옵션을 사용하면 피어가 최대 수신 유닛을 알릴 수 있습니다. 예를 들어 피어가 1460의 MRU를 광고하는 경우 해당 피어는 1460바이트보다 큰 페이로드를 가진 PPP 프레임을 처리하지 않습니다. Cisco PPP 구현에서는 인터페이스의 MTU를 PPP 협상 중에 광고한 MRU 값으로 사용합니다. MTU가 기본값인 1500바이트로 설정된 경우 PPP의 표준 기본값이므로 MRU가 광고되지 않습니다. 그러나 MTU를 1460으로 설정하면 PPP MRU 1460이 광고됩니다. PPP 피어가 PPP 협상 중에 광고된 MRU를 듣고 해당 PPP 링크에 대한 MTU(그리고 간접적으로 IP MTU)를 조정하는 경우 프래그먼트화를 방지할 수 있습니다. 알려진 PPP MRU가 1460인 경우 피어는 IP MTU를 1460으로 설정해야 합니다. 그러면 피어가 TCP 연결을 열 때 광고하는 TCP MSS를 수정하고 L2TP 네트워크를 통해 프래그먼트화를 방지합니다.

[하위 MTU 구성](#)

mtu <bytes> 명령을 사용하여 가상 템플릿 인터페이스에서 낮은 MTU를 구성합니다.다시 한 번, PPP 협상 중에 광고된 MRU를 들으려면 PPP 클라이언트에 대한 지원이 필요합니다.MRU 옵션을 수신하는 알려진 클라이언트 중 하나는 Windows XP PPP 클라이언트입니다.그러나 일반적으로 구축된 다른 PPP 클라이언트는 광고된 PPP MRU를 제대로 따르지 않습니다.PPP 클라이언트 설명서를 참조하여 광고된 PPP MRU를 올바르게 사용하는지 확인합니다.proxy-LCP를 사용하여 L2TP를 실행하는 경우 LCP 단계 중에 MRU 옵션이 협상되므로 LCP 재협상이 이루어져야 합니다.LCP 재협상을 활성화하려면 lcp 재협상 on-mismatch 또는 lcp 재협상이 항상 vpdn-group에서 구성합니다.

MTU를 낮추는 데 있어 한 가지 문제는 IP MTU도 자동으로 낮아진다는 것입니다.현재 가상 템플릿 인터페이스에서 MTU보다 큰 IP MTU를 구성할 수 없습니다.이는 Bug ID CSCdx39828을 기능/개선 요청으로 추적됩니다(외부 사용자가 볼 수 없음).

이 방법을 사용하려면 클라이언트가 LCP 협상 중에 MRU 옵션을 수신해야 합니다.다음과 같은 여러 클라이언트가 혼합되어 있습니다.MRU를 듣는 사람들, 그렇지 않은 사람들MRU를 무시하는 클라이언트는 Automatically Adjusting the IP MTU([IP MTU 자동 조정](#)) 섹션에 설명된 PMTUD 문제 [에](#) 실행됩니다.이러한 클라이언트의 경우 내부 IP 패킷에서 DF 비트를 지워 PMTUD를 효과적으로 해제하여 다른 해결 방법을 사용할 수 있습니다.다음 컨피그레이션으로 이 작업을 수행할 수 있습니다.

```
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
```

결론

Cisco IOS 소프트웨어는 L2TP 스위칭 성능을 최대화하는 다양한 방법을 제공합니다.PMTUD는 이상적인 솔루션입니다.그러나, 인터넷의 문제로 인해, 항상 믿을 수 있는 것은 아니다.Cisco IOS 소프트웨어는 L2TP 스위칭 성능을 높이고 사용자 연결을 극대화하는 몇 가지 대체 메커니즘을 제공합니다.

관련 정보

- [RFC2923:경로 MTU 검색의 TCP 문제](#)
- [Windows 및 Sun 시스템에서 IP MTU, TCP MSS 및 PMTUD 조정](#)
- [다이얼 - 액세스 기술 지원](#)
- [기술 지원 및 문서 - Cisco Systems](#)