VPDN 이해

목차

소개

VPDN(Virtual Private Dial-Up Network)을 사용하면 프라이빗 네트워크 다이얼인 서비스가 원격 액세스 서버(LAC[L2TP Access Concentrator])로 정의됩니다.

PPP(Point-to-Point Protocol) 클라이언트가 LAC로 전화를 걸 때 LAC는 해당 PPP 세션을 해당 클라이언트의 L2TP 네트워크 서버(LNS)로 전달해야 한다고 결정합니다.그런 다음 LNS가 사용자를 인증하고 PPP 협상을 시작합니다.PPP 설정이 완료되면 모든 프레임이 LAC를 통해 클라이언트와 LNS로 전송됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

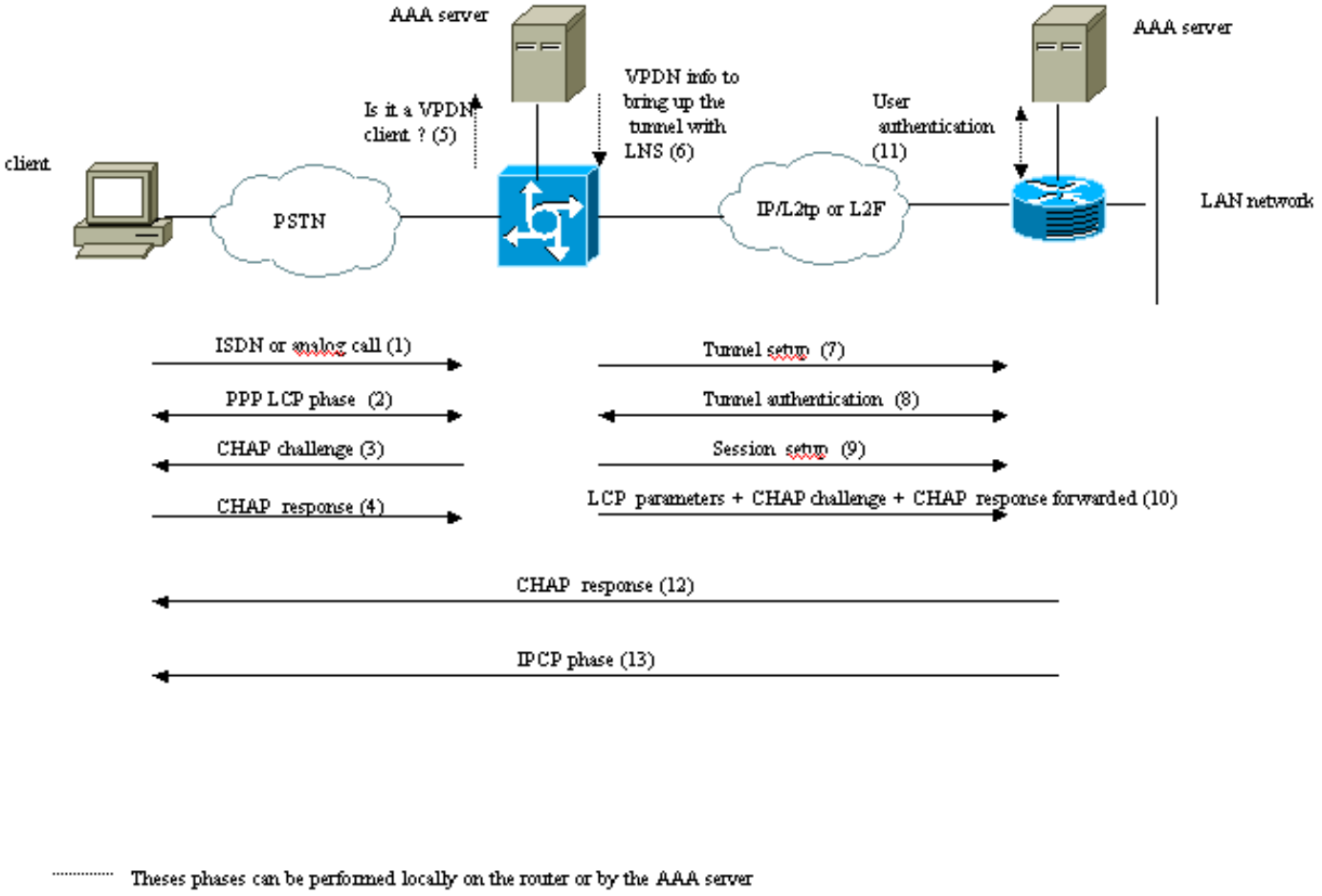
문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

용어집

- **클라이언트:**통화의 개시자인 원격 액세스 네트워크에 연결된 PC 또는 라우터
- **L2TP**:레이어 2 터널 프로토콜.PPP는 L2(Layer 2) 포인트-투-포인트 링크를 통해 다중 프로토콜 패킷을 전송하기 위한 캡슐화 메커니즘을 정의합니다.일반적으로 사용자는 POTS(Plain Old Telephone Service), ISDN 또는 ADSL(Asymmetric Digital Subscriber Line)과 같은 전화 접속 기술을 사용하여 NAS(Network Access Server)에 대한 L2 연결을 얻습니다. 그런 다음 사용자는 해당 연결을 통해 PPP를 실행합니다.이러한 컨피그레이션에서는 L2 종료 지점 및 PPP 세션 엔드포인트가 동일한 물리적 디바이스(NAS)에 상주합니다.L2TP는 L2 및 PPP 엔드포인트가 네트워크에 의해 상호 연결된 서로 다른 디바이스에 상주하도록 허용하여 PPP 모델을 확장합니다.L2TP를 사용하면 사용자는 액세스 집중장치에 L2 연결이 되며 Concentrator는 개별 PPP 프레임을 NAS에 터널링합니다.이렇게 하면 PPP 패킷의 실제 처리가 L2 회로의 종료에서 이혼될 수 있습니다.
- **L2F**:레이어 2 포워딩 프로토콜.L2F는 L2TP보다 오래된 터널링 프로토콜입니다.
- **LAC**:L2TP Access Concentrator.L2TP 터널 엔드포인트의 한 쪽 역할을 하며 LNS에 대한 피어인 노드입니다.LAC는 LNS와 클라이언트 사이에 위치하며 각 LAN에서 수신되는 패킷을 전달합니다.LAC에서 LNS로 전송되는 패킷은 L2TP 프로토콜로 터널링해야 합니다.LAC에서 클라이언트로의 연결은 일반적으로 ISDN 또는 아날로그 연결을 통해 이루어집니다.
- **LNS**:L2TP 네트워크 서버.L2TP 터널 엔드포인트의 한 쪽 역할을 하며 LAC에 대한 피어인 노드입니다.LNS는 LAC에 의해 클라이언트에서 터널링되는 PPP 세션의 논리적 종료 지점입니다.
- **홈 게이트웨이**:L2F 용어에서 LNS와 동일한 정의
- **NAS**:L2F 용어에서 LAC와 동일한 정의
- **터널:**L2TP 용어에서는 LAC-LNS 쌍 사이에 터널이 있습니다.터널은 제어 연결 및 0개 이상의 L2TP 세션으로 구성됩니다.터널은 캡슐화된 PPP 데이터그램을 전송하고 LAC와 LNS 간에 메시지를 제어합니다.이 프로세스는 L2F와 동일합니다.
- **세션**:L2TP는 연결 지향적입니다.LNS 및 LAC는 LAC에서 시작하거나 응답한 각 통화에 대한 상태를 유지합니다.클라이언트와 LNS 간에 엔드 투 엔드 PPP 연결이 설정되면 LAC와 LNS 간에 L2TP 세션이 생성됩니다.PPP 연결과 관련된 데이터그램은 LAC와 LNS 사이의 터널을 통해 전송됩니다.설정된 L2TP 세션과 관련 통화 간에는 일대일 관계가 있습니다.이 프로세스는 L2F와 동일합니다.

VPDN 프로세스 개요

아래 VPDN 프로세스에 대한 설명에서 L2TP 용어(LAC 및 LNS)를 사용합니다.



1. 클라이언트는 LAC를 호출합니다(일반적으로 모뎀 또는 ISDN 카드를 사용).
2. 클라이언트와 LAC는 LCP 옵션(인증 방법 PAP(Password Authentication Protocol) 또는 CHAP(Challenge Handshake Authentication Protocol), PPP 멀티링크, 압축 등)을 협상하여 PPP 단계를 시작합니다.
3. 2단계에서 CHAP가 협상되었다고 가정해 보겠습니다. LAC가 클라이언트에 CHAP 챌린지를 보냅니다.
4. LAC는 응답을 받습니다(예: username@DomainName 및 비밀번호).
5. CHAP 응답에서 수신된 도메인 이름 또는 ISDN 설정 메시지에서 수신된 DNIS(Dialed Number Information Service)를 기반으로 LAC는 클라이언트가 VPDN 사용자인지 확인합니다.로컬 VPDN 컨피그레이션을 사용하거나 AAA(Authentication, Authorization, and Accounting) 서버에 연결하여 이를 수행합니다.
6. 클라이언트는 VPDN 사용자이므로 LAC는 LNS를 사용하여 L2TP 또는 L2F 터널을 생성하는 데 사용하는 일부 정보(로컬 VPDN 컨피그레이션 또는 AAA 서버에서)를 가져옵니다.
7. LAC는 LNS와 함께 L2TP 또는 L2F 터널을 표시합니다.
8. LAC에서 수신한 이름에 따라 LNS는 LAC가 터널을 열 수 있는지 확인합니다(LNS는 로컬 VPDN 컨피그레이션을 확인합니다). 또한 LAC와 LNS는 서로를 인증합니다(로컬 데이터베이스를 사용하거나 AAA 서버에 연결). 그런 다음 두 디바이스 간에 터널이 작동합니다.이 터널에서 여러 VPDN 세션을 전달할 수 있습니다.
9. 클라이언트 username@DomainName의 경우 LAC에서 LNS로 VPDN 세션이 트리거됩니다.클라이언트당 하나의 VPDN 세션이 있습니다.
10. LAC는 클라이언트와 협상한 LCP 옵션을 클라이언트에서 받은 username@DomainName 및 비밀번호와 함께 LNS에 전달합니다.
11. LNS는 VPDN 컨피그레이션에 지정된 가상 템플릿에서 가상 액세스를 복제합니다.LNS는 LAC에서 받은 LCP 옵션을 사용하여 로컬에서 또는 AAA 서버에 연결하여 클라이언트를 인

증합니다.

12. LNS는 클라이언트에 CHAP 응답을 보냅니다.
13. IPCP(IP Control Protocol) 단계가 수행된 다음 경로가 설치됩니다.클라이언트와 LNS 간에 PPP 세션이 실행 중입니다.LAC는 PPP 프레임을 전달합니다.LAC와 LNS 간에 PPP 프레임이 터널링됩니다.

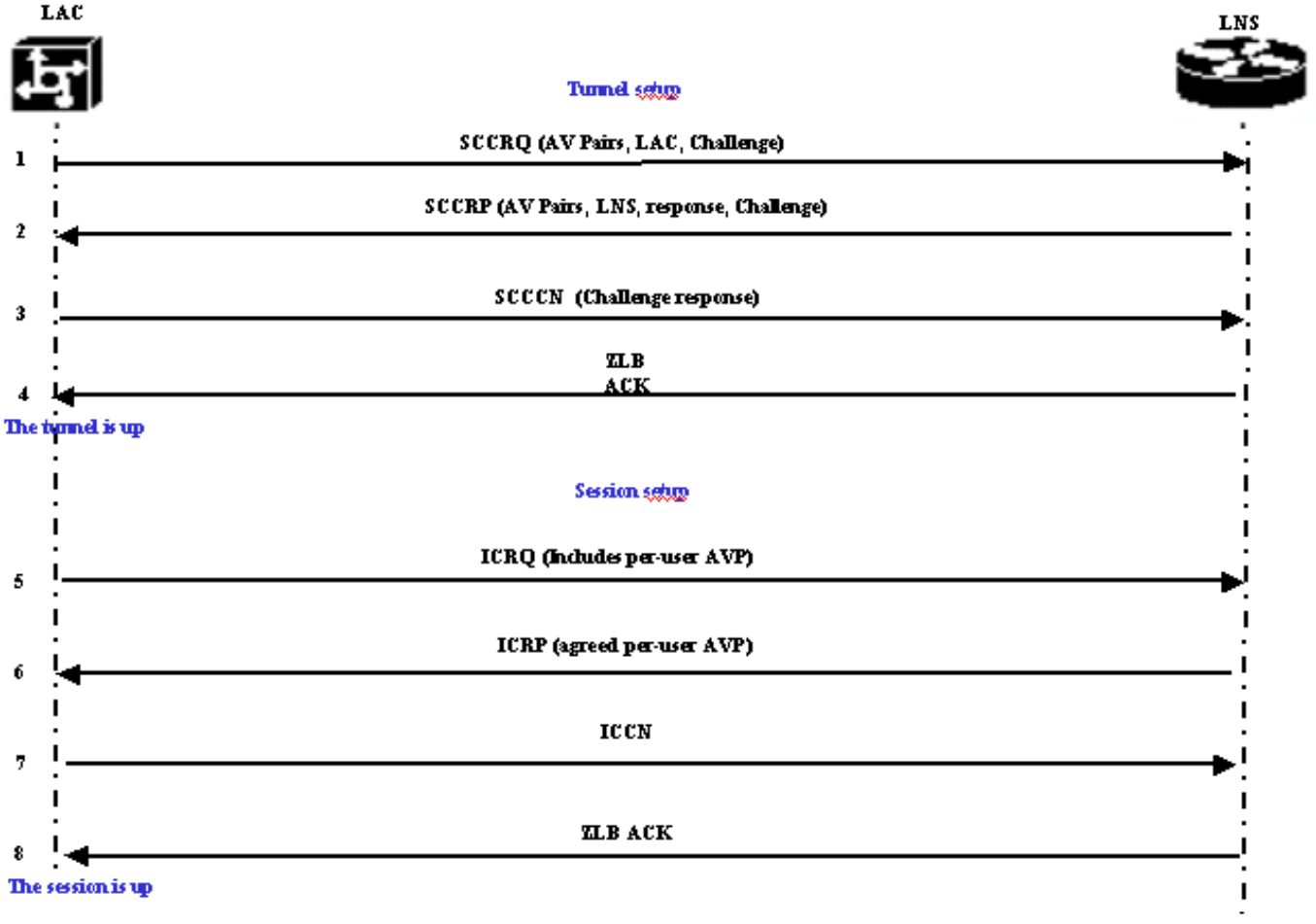
터널링 프로토콜

VPDN 터널은 L2F(Layer-2 Forwarding) 또는 L2TP(Layer-2 Tunneling Protocol)를 사용하여 구축할 수 있습니다.

- L2F는 RFC(Request For Comments) 2341에서 Cisco에 소개되었으며 멀티섀시 멀티링크 PPP에 대한 PPP 세션을 전달하는 데 사용됩니다.
- RFC 2661에 도입된 L2TP는 Cisco L2F 프로토콜과 Microsoft PPTP(Point-to-Point Tunneling Protocol)의 장점을 결합합니다. 또한 L2F는 Dial-in VPDN만 지원하는 반면 L2TP는 Dial-in 및 Dial-out VPDN을 모두 지원합니다.

두 프로토콜 모두 UDP 포트 1701을 사용하여 IP 네트워크를 통해 터널을 구축하여 링크 레이어 프레임을 전달합니다.L2TP의 경우 PPP 세션 터널링 설정은 다음 두 단계로 구성됩니다.

1. LAC와 LNS 간의 터널 설정이 단계는 두 디바이스 간에 활성 터널이 없는 경우에만 발생합니다.
2. LAC와 LNS 간의 세션 설정



LAC는 LAC에서 LNS로 터널을 시작해야 한다고 결정합니다.

1. LAC는 SCCRQ(Start-Control-Connection-Request)를 전송합니다.CHAP 챌린지 및 AV 쌍이

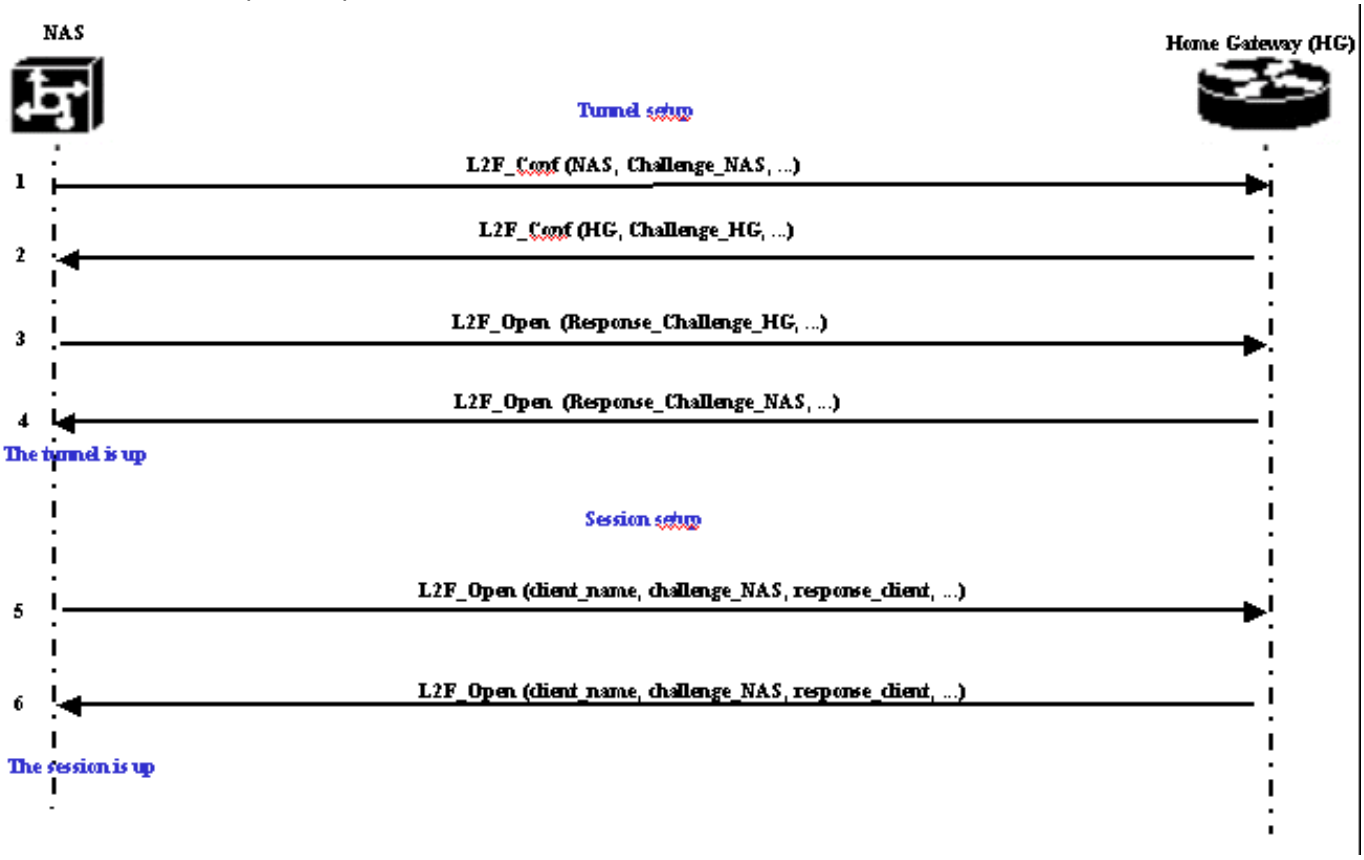
이 메시지에 포함되어 있습니다.
2. LNS는 SCCRP(Start-Control-Connection-Reply)로 응답합니다.CHAP 과제, LAC의 과제 및 AV 쌍에 대한 응답이 이 메시지에 포함되어 있습니다.
3. LAC는 SCCCN(Start-Control-Connection-Connected)을 전송합니다. CHAP 응답이 이 메시지에 포함되어 있습니다.
4. LNS는 길이가 0인 본문 승인(ZLB ACK)으로 응답합니다. 그 승인은 다른 메시지로 전달될 수 있습니다.터널이 작동 중입니다.
5. LAC는 ICRQ(Incoming-Call-Request)를 LNS에 전송합니다.
6. LNS는 ICRP(Incoming-Call-Reply) 메시지로 응답합니다.
7. LAC는 ICCN(Incoming-Call-Connected)을 전송합니다.
8. LNS는 ZLB ACK로 다시 응답합니다.해당 승인도 다른 메시지로 전달될 수 있습니다.
9. 세션이 시작되었습니다.

참고: 터널 또는 세션을 여는 데 사용되는 위의 메시지는 RFC 2661에 정의된 AVP(Attribute Value Pairs)를 전달합니다.속성 및 정보(예: Bearrcap, 호스트 이름, 공급업체 이름 및 창 크기)에 대해 설명합니다. 일부 AV 쌍은 필수 사항이며 다른 쌍은 선택 사항입니다.

참고: 터널 ID는 LAC와 LNS 간의 멀티플렉스 터널에 사용됩니다.세션 ID는 터널과의 특정 세션을 식별하는 데 사용됩니다.

L2F의 경우 PPP 세션 터널링 설정은 L2TP와 동일합니다.여기에는 다음이 포함됩니다.

1. NAS와 홈 게이트웨이 간의 터널 설정이 단계는 두 디바이스 간에 활성 터널이 없는 경우에만 발생합니다.
2. NAS와 홈 게이트웨이 간의 세션 설정



NAS는 NAS에서 홈 게이트웨이로 터널을 시작해야 한다고 결정합니다.

1. NAS는 L2F_Conf를 홈 게이트웨이로 전송합니다.이 메시지에는 CHAP 챌린지가 포함되어 있습니다.

2. 홈 게이트웨이는 L2F_Conf로 응답합니다.이 메시지에는 CHAP 챌린지가 포함되어 있습니다.
3. NAS는 L2F_Open을 전송합니다.이 메시지에는 홈 게이트웨이 챌린지의 CHAP 응답이 포함되어 있습니다.
4. 홈 게이트웨이는 L2F_Open으로 응답합니다.NAS 챌린지의 CHAP 응답은 이 메시지에 포함되어 있습니다.터널이 작동 중입니다.
5. NAS는 홈 게이트웨이로 L2F_Open을 전송합니다.패킷에는 클라이언트의 사용자 이름(client_name), NAS에서 클라이언트로 보낸 CHAP 과제(challenge_NAS) 및 응답(response_client)이 포함됩니다.
6. L2F_OPEN을 다시 전송하여 홈 게이트웨이는 클라이언트를 수락합니다.이제 트래픽은 클라이언트와 홈 게이트웨이 간에 어느 방향으로든 자유롭게 이동할 수 있습니다.

참고: 터널은 CLID(Client ID)로 식별됩니다. MID(Multiplex ID)는 터널 내에서 특정 연결을 식별합니다.

VPDN 구성

VPDN 구성에 대한 자세한 내용은 Configuring Virtual Private Networks 설명서를 참조하고 VPN 구성 섹션으로 이동하십시오.

관련 정보

- 다이얼 및 액세스 기술 지원 페이지
- 기술 지원 및 문서 – Cisco Systems