Cisco 6400 UAC용 PPPoE 기본 아키텍처

목차

소개

이 문서에서는 PPPoE(Point-to-Point Protocol over Ethernet)를 사용하는 엔드 투 엔드 ADSL(Asymmetric Digital Subscriber Line) 아키텍처에 대해 설명합니다.

현재 Access 기술 환경에서는 동일한 고객 구내 액세스 디바이스를 통해 원격 사이트의 여러 호스트를 연결하는 것이 좋습니다.또한 PPP(Point-to-Point Protocol)를 사용하는 전화 접속 서비스와 유사한 방식으로 액세스 제어 및 청구 기능을 제공해야 합니다. 많은 액세스 기술에서, 여러 호스트를 고객 구내 액세스 디바이스에 연결하는 가장 비용 효율적인 방법은 이더넷을 통해서입니다.또한 이 장치의 비용을 최대한 낮게 유지하고 컨피그레이션 요구 사항을 줄이거나 아예 없음으로 유지하는 것이 좋습니다.

고객이 ADSL을 구축할 때 기존 브리징 CPE(Customer Premises Equipment)의 대규모 설치 기반에 대한 PPP 스타일 인증 및 권한 부여를 지원해야 합니다.PPPoE는 간단한 브리징 액세스 디바이스를 통해 호스트 네트워크를 원격 액세스 집중기 또는 집선 집중 장치에 연결할 수 있는 기능을 제공합니다.이 모델에서는 각 호스트가 자체 PPP 스택을 사용합니다.따라서 사용자에게 친숙한 사용자 인터페이스를 제공합니다.사이트별로 액세스할 수 있는 것이 아니라 사용자별로 제어, 청구 및 서비스 유형에 액세스할 수 있습니다.

가정

기본 아키텍처는 다음 항목이 제공된다고 가정합니다.

- PPPoE를 사용하는 최종 가입자에 대한 고속 인터넷 액세스 및 기업 액세스
- Cisco 6400 UAC(Universal Access Concentrator)에서 구현한 핵심 백본 기술인 ATM입니다.

이러한 설계 구현 제한은 다른 플랫폼에서 이 아키텍처의 사용을 제한할 수 있지만 PPPoE는 지속적으로 발전합니다.관련 제품에 대한 최신 릴리스 정보를 읽고 새로운 기능과 업데이트된 기능을

활용하십시오.

이 백서는 Cisco 6400 UAC를 사용하는 내부 테스트와 현재 구축을 기반으로 합니다.이 백서는 PPPoA Baseline Architecture 종이의 연속으로 자주 언급됩니다.PPPoA Baseline Architecture 백서를 읽고 PPP의 기본 사항을 이해하고 최신 소프트웨어 릴리스에 대한 릴리스 노트를 읽은 것으로 가정합니다.

기술 개요

RFC 2516에 지정된 대로 PPPoE에는 두 가지 단계가 있습니다.검색 단계 및 PPP 세션 단계.호스트가 PPPoE 세션을 시작할 때 먼저 검색을 수행하여 클라이언트의 요청을 충족할 수 있는 서버를 식별해야 합니다.둘째, 피어의 이더넷 MAC 주소를 식별하고 PPPoE 세션 ID를 설정해야 합니다. PPP는 피어 투 피어 관계를 정의하지만 검색은 클라이언트-서버 관계를 근본적으로 정의합니다.

검색 프로세스에서 호스트(클라이언트)는 하나 이상의 액세스 집중기(서버)를 검색하고 하나를 선택합니다.검색이 성공적으로 완료되면 호스트와 선택한 액세스 집중기 모두 이더넷을 통한 포인트-투-포인트 연결을 구축하기 위한 정보를 갖게 됩니다.PPP 세션이 설정되면 호스트와 액세스 집중기 모두 PPP 가상 인터페이스에 리소스를 할당해야 합니다(모든 구현에서는 그렇지 않을 수 있음). PPPoE 사양에 대한 자세한 내용은 RFC 2516을 참조하십시오.

PPPoE 아키텍처의 장점과 단점

PPPoE 아키텍처는 다이얼업 모델과 PPPoA 아키텍처에서 사용되는 PPP의 대부분의 장점을 상속합니다.이 섹션에서는 PPPoE의 몇 가지 주요 장점과 단점과 PPPoA와 어떻게 다른지 설명합니다.

장점

다음은 PPPoE의 몇 가지 주요 장점이며 PPPoA와 어떻게 다릅니까?

- PAP(Password Authentication Protocol) 또는 CHAP(Challenge Handshake Authentication Protocol)를 기반으로 한 세션별 인증입니다. 이는 인증이 브리징 아키텍처의 보안 허점을 능가하므로 PPPoE의 가장 큰 장점입니다.
- 서비스제공자가 제공되는 다양한 서비스에 대한 세션 시간을 기준으로 가입자에게 요금을 부과할 수 있도록 세션당 계정 관리가 가능합니다.통신 사업자는 최소 액세스 요금이 필요할 수도 있습니다.
- PPP로 업그레이드할 수 없거나 PPPoA를 실행할 수 없는 현재 CPE 설치에서 PPPoE를 사용할 수 있으며, 이 경우 PPP 세션이 브리징된 이더넷 LAN을 통해 PC로 확장됩니다.
- PPPoE는 현재 전화 접속 모델에서 ISP(Internet Service Provider)가 사용하는 포인트 투 포인트 세션을 유지합니다.PPPoE는 중간 IP 스택의 요구 사항 없이 Point-to-Point over Ethernet을 실행할 수 있는 유일한 프로토콜입니다.
- NAP(Network Access Provider) 또는 NSP(Network Service Provider)는 엔드 투 엔드 PVC(Virtual Circuits)를 관리하지 않고 레이어 3 라우팅 및/또는 L2TP(Layer 2 Tunneling Protocol) 터널을 사용하지 않고도 회사 게이트웨이에 안전하게 액세스할 수 있습니다.따라서 도매 서비스 및 VPN(Virtual Private Network)의 비즈니스 모델을 확장할 수 있습니다.
- PPPoE는 지정된 시간에 여러 대상에 대한 호스트(PC) 액세스를 제공할 수 있습니다.PVC당 여러 PPPoE 세션을 가질 수 있습니다.
- NSP는 각 가입자에 대한 업계 표준 RADIUS(Remote Authentication Dial-In User Service) 서버의 도움을 받아 유휴 및 세션 시간 제한을 구축함으로써 초과 서브스크립션을 수행할 수 있습

니다.
- PPP를 SSG(서비스 선택 게이트웨이) 기능과 함께 사용할 수 있습니다.

단점

다음은 PPPoE의 몇 가지 주요 단점과 PPPoA와 어떻게 다른지입니다.

- 이더넷 세그먼트에 연결되는 모든 호스트(PC)에 PPPoE 클라이언트 소프트웨어를 설치해야 합니다.즉, 액세스 공급자는 PC에서 CPE 및 클라이언트 소프트웨어를 유지해야 합니다.
- PPPoE 구현에서는 RFC 1483 브리징을 사용하므로 브로드캐스트 스톰과 서비스 거부 공격에 취약합니다.

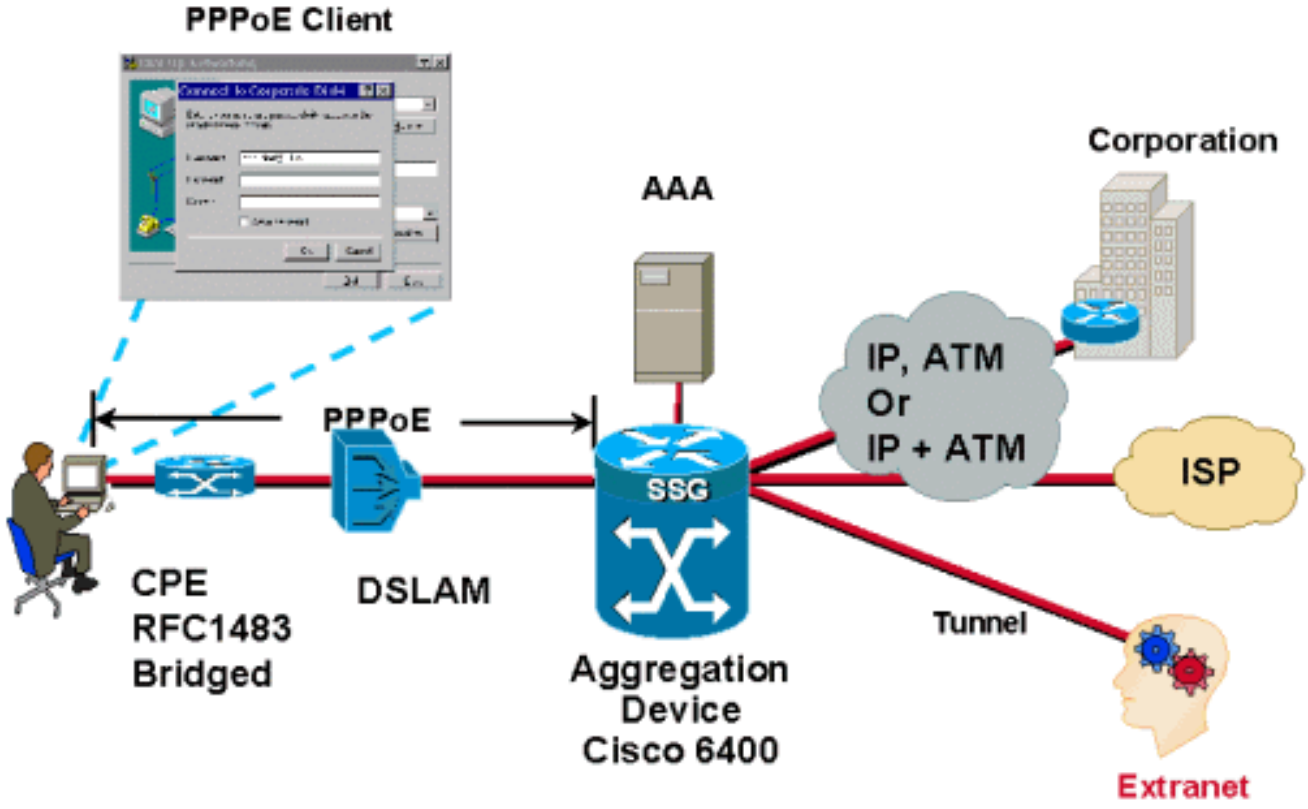
PPPoE 아키텍처의 구현 고려 사항

이러한 유형의 아키텍처를 구현하기 전에 고려해야 할 몇 가지 핵심 사항입니다.

- 지원되는 구독자 수입니다.필요한 PPPoE 서버 수는 세션 수에 따라 달라집니다.
- PPP 세션이 서비스 공급자의 어그리게이션 라우터에서 종료되는지 아니면 다른 기업 게이트웨이 또는 ISP에 전달되는지 여부.
- 서비스 공급자 또는 최종 서비스 대상이 IP 주소를 제공하는지 여부.
- 둘 이상의 사용자의 경우 모든 사용자가 동일한 최종 목적지 또는 서비스에 도달해야 하는지 아니면 모두 서로 다른 서비스 대상을 가지고 있는지 여부.최종 가입자에게 여러 대상에 대한 동시 액세스가 필요합니까?
- 액세스 공급자가 사용하는 PPPoE 클라이언트 소프트웨어 및 소프트웨어 테스트 여부, 호스트가 사용하는 운영 체제, 해당 운영 체제가 지능적인 라우팅 결정을 내릴 수 있는지 여부.
- 통신 사업자가 균일한 속도, 세션당 사용량 또는 사용된 서비스에 따라 가입자에게 청구하는 방식
- CPE, DSLAM 및 POP(Aggregation Point of Presence)의 구축 및 프로비저닝
- NAP의 비즈니스 모델입니다.또한 이 모델에는 안전한 기업 액세스와 같은 도매 서비스 판매와 음성 및 비디오와 같은 부가 가치 서비스가 포함됩니까?NAP와 NSP가 동일한 엔터티입니까?
- 회사의 비즈니스 모델입니다.ILEC(Independent Local Exchange Carrier), CLEC(Competitive Local Exchange Carrier) 또는 ISP와 비교됩니까?
- NSP가 최종 가입자에게 제공하는 애플리케이션 유형입니다.
- 예상되는 데이터 흐름의 업스트림 및 다운스트림 볼륨.NRP 처리량, 트래픽 엔지니어링 및 모든 QoS 문제를 고려하십시오.

이 문서에서는 PPPoE 아키텍처가 통신 사업자를 위한 다양한 비즈니스 모델에 부합하고 확장되는 방법과 이 아키텍처의 도움을 통해 제공자가 어떤 혜택을 얻을 수 있는지 설명합니다.

네트워크 아키텍처



PPPoE 아키텍처의 설계 고려 사항

이 섹션에서는 PPPoE 아키텍처에 적용되는 문제에 대해 설명합니다.

아키텍처를 구축하기 전에 통신 사업자의 비즈니스 모델과 제공자가 제공하는 서비스를 이해하는 것이 중요합니다.PC에서 사용되는 클라이언트 소프트웨어를 알아야 합니다.가장 일반적인 소프트웨어는 RouterWare입니다.클라이언트 소프트웨어가 PC에 설치되어 있으므로 통신 사업자 기술자는 해당 PC와 해당 운영 체제를 잘 알고 있어야 합니다.

RFC 2516에 지정된 대로 MRU(최대 수신 장치) 옵션은 1492보다 큰 크기로 협상하지 않아야 합니다.이더넷의 최대 페이로드 크기는 15008입니다.PPPoE 헤더는 6octet이고 PPP 프로토콜 ID는 2octet이므로 PPP MTU(Maximum Transmission Unit)는 1492보다 크지 않아야 합니다.이는 PPPoE 가상 템플릿 인터페이스를 위한 IP MTU 1492를 구성함으로써 가능합니다.

기본적으로 PPPoE VPDN 그룹이 구성되면 가상 액세스 인터페이스가 미리 복제되지 않습니다.사용자는 **virtual-template <number> pre-clone <number>** 전역 명령을 실행하여 사전 복제된 가상 액세스 인터페이스**의** 최대 수를 변경할 수 있습니다.

서비스 거부 공격으로부터 라우터를 보호하기 위해 PPPoE(기본값)는 VC를 통해 MAC 주소에서 하나의 세션만 소싱할 수 있도록 합니다.사용자는 **ppoe session-limit per-mac** 및 pppoe session-**limit per-vc** 명령**을 실행하여** 기본값을 변경할 수 있습니다.

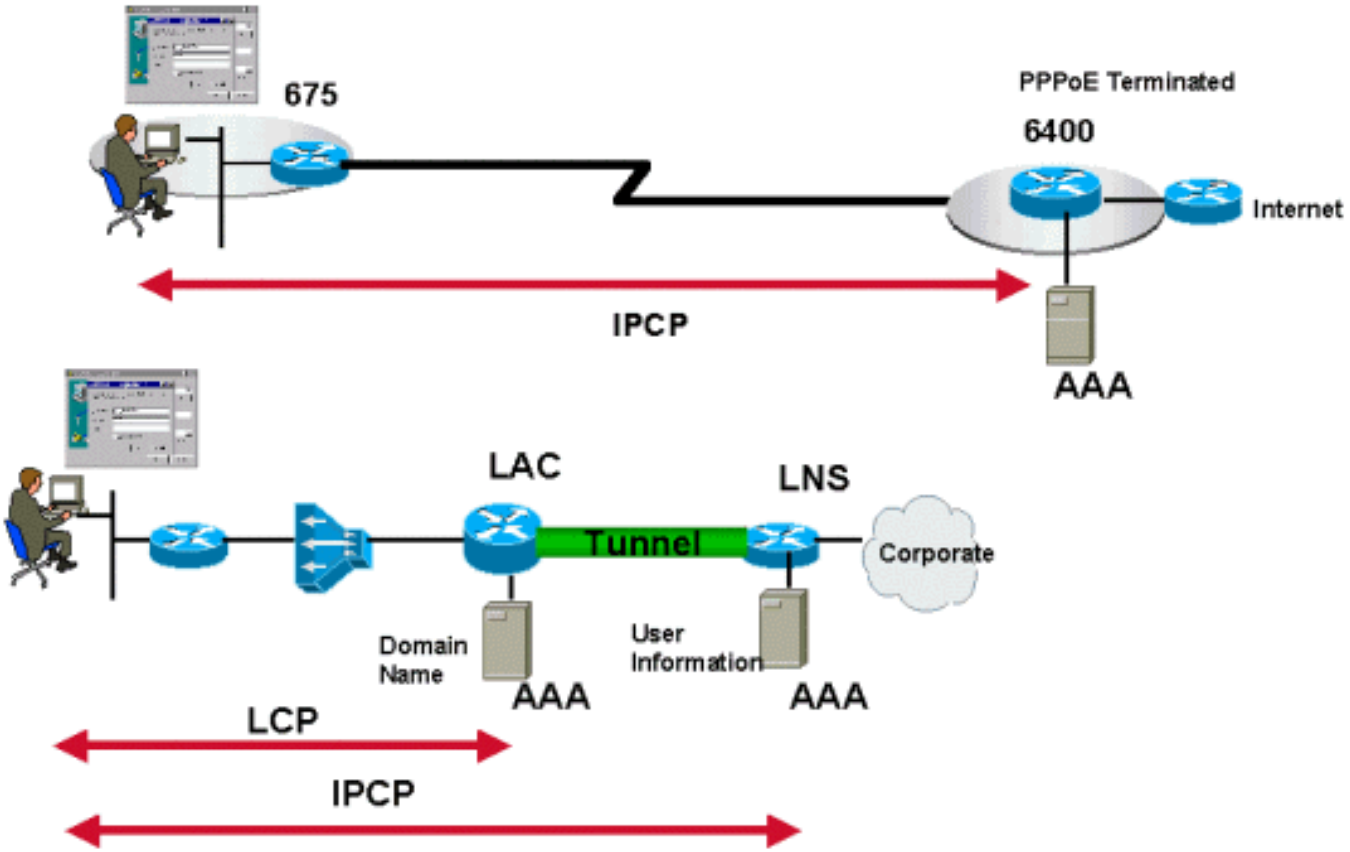
어카운팅, 권한 부여 및 인증 프로세스는 PPPoA와 동일합니다.유일한 차이점은 현재 PPPoA에 사용할 수 있고 PPPoE에 사용할 수 없는 VPI/VCI 기반 인증은 도매 서비스에 L2TP 및 SSG 아키텍처를 사용할 수 있다는 것입니다.

PPPoE 아키텍처의 핵심 요소

CPE

CPE는 순수 RFC 1483 브리징을 위해 구성됩니다.각 CPE는 하나의 VPI/VCI 쌍만 사용하며 이 CPE 뒤에 있는 호스트에서 시작한 모든 PPPoE 세션은 이 단일 VC에서 이월됩니다.

IP 관리



PPPoE 클라이언트를 실행하는 개별 호스트에 대한 IP 주소 할당은 다이얼 모드-IPCP 협상에서 동일한 PPP 원칙을 기반으로 합니다.IP 주소 출처는 가입자가 구매한 서비스의 유형 및 PPP 세션이 종료되는 위치에 따라 달라집니다.PPPoE는 Microsoft Windows의 전화 접속 네트워킹 기능을 사용하며, 할당된 IP 주소는 PPP 어댑터에 반영됩니다.

IP 주소 할당은 PPPoE 세션을 종료하는 액세스 집중 장치 또는 L2TP의 경우 홈 게이트웨이에서 가져올 수 있습니다.각 PPPoE 세션에 대해 IP 주소가 할당됩니다.

CPE는 브리징되고 할당된 IP 주소가 없으므로 NAT/DHCP(Network Address Translation/Dynamic Host Configuration Protocol)를 수행할 수 없습니다.

서비스 대상에 도달하는 방법

서비스 대상에 도달하는 방법은 다음과 같습니다.

- 서비스 공급자에서 PPP 세션 종료
- L2TP 터널링

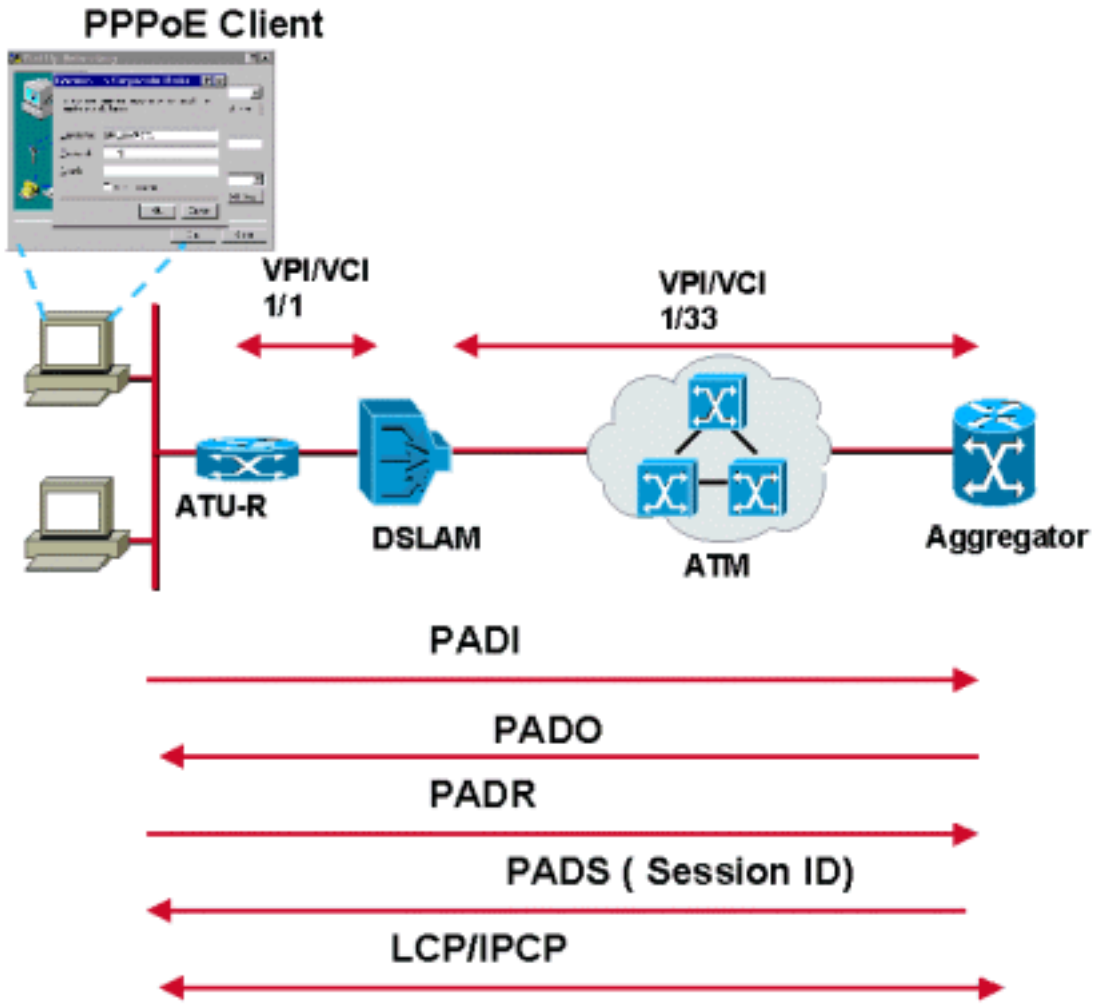
- SSG를 사용하는 경우

이러한 아키텍처에 대한 자세한 설명은 별도의 백서에서 다룹니다.

PPPoE에 대한 운영 설명

이 PPPoE 클라이언트 소프트웨어 릴리스는 RFC 2516에 설명된 검색 및 세션 단계를 지원합니다 .검색 단계에는 4단계가 있습니다.이 작업이 완료되면 두 피어는 모두 PPPoE 세션 ID와 피어의 이더넷 주소를 알고 있습니다. 피어는 함께 PPPoE 세션을 고유하게 정의합니다.다음은 단계입니다.

1. 호스트가 시작 패킷을 브로드캐스트합니다.호스트는 PPPoE PADI(Active Discovery Initiation) 패킷을 브로드캐스트 주소에 destination_addr이 설정된 상태로 전송합니다.PADI는 요청하는 서비스 유형을 나타내는 하나의 태그로 구성됩니다.
2. 하나 이상의 액세스 집중 장치가 제공 패킷을 전송합니다.액세스 집중기 또는 라우터가 제공할 수 있는 PADI를 수신하면 PPPoE PADO(Active Discovery Offer) 패킷을 전송합니다 .destination_addr은 PDI를 보낸 호스트의 유니캐스트 주소입니다.액세스 집중 장치가 PADI를 지원할 수 없는 경우 PADO로 응답해서는 안 됩니다.PADI가 방송되었으므로 호스트는 둘 이상의 PADO를 수신할 수 있습니다



.

3. 호스트가 유니캐스트 세션 요청 패킷을 전송합니다.호스트는 수신하는 PADO 패킷을 확인하고 이를 선택합니다.각 액세스 집중 장치가 제공하는 서비스에 따라 선택할 수 있습니다.그런 다음 호스트가 선택한 액세스 집중장치에 PADR 패킷 하나를 전송합니다.destination_addr 필드는 액세스 집중기 또는 PADO를 전송하는 라우터의 유니캐스트 이더넷 주소로 설정됩니다.
4. 선택한 액세스 집중 장치가 확인 패킷을 전송합니다.Access Concentrator가 PADR 패킷을 수

신하면 PPP 세션을 시작할 준비를 합니다.PPPoE 세션에 대해 고유한 세션 ID를 생성하고 PPPoE PADS(Active Discovery Session-Confirmation) 패킷을 사용하여 호스트에 응답합니다 .destination_addr 필드는 PADR을 전송하는 호스트의 유니캐스트 이더넷 주소입니다.

PPPoE 세션이 시작되면 다른 PPP 캡슐화에서와 같이 PPP 데이터가 전송됩니다.모든 이더넷 패킷은 유니캐스트입니다.

PPPoE 활성 검색 종료(PADT) 패킷은 PPPoE 세션이 종료되었음을 나타내기 위해 세션이 설정된 후 언제든지 호스트 또는 액세스 집중기에서 전송할 수 있습니다.

자세한 설명은 RFC 2516을 참조하십시오.

결론

ADSL의 경우, PPPoE가 인기를 얻고 PPPoA에 이어 두 번째입니다.

참조

- RFC 2516 - PPPoE(PPPoE)를 통한 PPP 전송 방법
- RFC 1483 - ATM Adaptation Layer 5를 통한 다중 프로토콜 캡슐화
- RFC 2364 - AAL5를 통한 Point-to-Point

관련 정보

- PPPoA 기본 아키텍처
- DSL 기술 지원
- Technical Support - Cisco Systems