PPPoA 기본 아키텍처

목차

소개

이 문서에서는 PPPoA(Point-to-Point Protocol over Asynchronous Transfer Mode)를 사용하는 엔드 투 엔드 비대칭 ADSL(Digital Subscriber Line) 아키텍처에 대해 설명합니다. 대부분의 구축은 브리징 아키텍처를 기반으로 하지만, PPPoA는 엄청난 인기를 얻고 있으며 향후 ADSL 구축에서 더 많은 부분을 차지할 것입니다.

가정

기본 아키텍처는 PPPoA를 핵심 백본으로 사용하여 최종 가입자에게 고속 인터넷 액세스 및 기업 액세스를 제공해야 한다고 가정합니다.이 아키텍처는 현재 구축에서 가장 자주 사용되는 방법인 PVC(Private Virtual Channel)를 기반으로 합니다.SVC(Switched Virtual Circuit)를 사용하는 아키텍처에 대해서는 별도의 백서에서 설명합니다.

이 문서는 기존 구축 및 아키텍처 내부 테스트를 기반으로 합니다.

이 문서는 RFC1483 브리징 베이스라인 아키텍처 백서에 설명된 대로 독자가 NAP(Network Access Provider)의 설계 고려 사항에 대해 잘 알고 있다는 가정으로 작성되었습니다.

기술 개요

PPP(Point-to-Point Protocol)(RFC 1331)는 포인트-투-포인트 연결을 통해 상위 레이어 프로토콜을

캡슐화하는 표준 방법을 제공합니다.패킷의 내용에 대한 정보를 포함하는 16비트 프로토콜 식별자를 사용하여 HDLC(High-Level Data Link Control) 패킷 구조를 확장합니다.

패킷에는 세 가지 유형의 정보가 포함되어 있습니다.

- LCP(Link Control Protocol) - 링크 매개변수, 패킷 크기 또는 인증 유형을 협상합니다.
- NCP(Network Control Protocol) - IP 및 IPX를 비롯한 상위 레이어 프로토콜과 해당 제어 프로토콜(IP용 IPCP)에 대한 정보를 포함합니다.
- 데이터가 포함된 데이터 프레임

PPP over ATM adaptation layer 5(AAL5)(RFC 2364)는 AAL5를 PVC와 SVC를 모두 지원하는 프레임 프로토콜로 사용합니다.PPPoA는 주로 ADSL의 일부로 구현되었습니다.RFC1483에 의존하며, LLC-SNAP(Logical Link Control-Subnetwork Access Protocol) 또는 VC-Mux 모드에서 작동합니다.CPE(Customer Premises Equipment) 디바이스는 ADSL 루프와 DSLAM(Digital Subscriber Line Access Multiplexer)을 통해 전송할 수 있도록 이 RFC를 기반으로 PPP 세션을 캡슐화합니다.

PPPoA 아키텍처의 장점과 단점

PPPoA 아키텍처는 다이얼 모델에 사용되는 PPP의 대부분의 장점을 상속합니다.몇 가지 핵심 사항은 아래에 나와 있습니다.

장점

- PAP(Password Authentication Protocol) 또는 CHAP(Challenge Handshake Authentication Protocol)를 기반으로 한 세션별 인증입니다. 이는 인증이 브리징 아키텍처의 보안 허점을 능가하므로 PPPoA의 가장 큰 장점입니다.
- 서비스제공자가 제공되는 다양한 서비스에 대한 세션 시간을 기준으로 가입자에게 요금을 부과할 수 있도록 세션당 계정 관리가 가능합니다.세션당 계정 관리를 사용하면 통신 사업자가 최소 비용으로 최소 액세스 수준을 제공한 다음 사용한 추가 서비스에 대해 가입자에게 요금을 부과할 수 있습니다.
- CPE의 IP 주소 보존.이를 통해 서비스 공급자는 NAT(Network Address Translation)용으로 구성된 CPE를 사용하여 CPE에 대해 하나의 IP 주소만 할당할 수 있습니다. 한 CPE의 모든 사용자는 단일 IP 주소를 사용하여 다른 대상에 연결할 수 있습니다.IP 주소를 보존하는 동시에 개별 사용자에 대한 NAP/NSP(Network Access Provider/Network Services Provider)의 IP 관리 오버헤드가 감소합니다.또한 통신 사업자는 PAT(Port Address Translation) 및 NAT의 제한을 극복하기 위해 작은 IP 주소 서브넷을 제공할 수 있습니다.
- NAP/NSP는 엔드 투 엔드 PVC를 관리하고 레이어 3 라우팅 또는 레이어 2 포워딩/레이어 2 터널링 프로토콜(L2F/L2TP) 터널을 사용하지 않고 기업 게이트웨이에 대한 보안 액세스를 제공합니다.따라서 도매 서비스 판매를 위해 비즈니스 모델을 확장할 수 있습니다.
- 개별 가입자의 문제 해결.NSP는 브리징 아키텍처의 경우와 같이 전체 그룹을 트러블슈팅하는 대신 활성 PPP 세션을 기반으로 어떤 가입자를 설정 또는 해제할 수 있습니다.
- NSP는 각 가입자에 대해 업계 표준 RADIUS(Remote Authentication Dial-In User Service) 서버를 사용하여 유휴 및 세션 시간 제한을 배포하여 초과 서브스크립션을 수행할 수 있습니다.
- 어그리게이션 라우터에서 매우 많은 수의 PPP 세션을 종료할 수 있으므로 확장성이 뛰어납니다.외부 RADIUS 서버를 사용하는 각 사용자에 대해 인증, 권한 부여 및 계정 관리를 처리할 수 있습니다.
- SSG(Service Selection Gateway)에서 최적의 기능 사용

단점

- 하나의 가상 채널(VC)에서 CPE당 단일 세션만. CPE에 사용자 이름과 비밀번호가 구성되어 있으므로 해당 특정 VC에 대해 CPE를 뒤에 있는 모든 사용자는 하나의 서비스 세트에만 액세스할 수 있습니다.여러 VC를 사용하고 서로 다른 VC에서 서로 다른 PPP 세션을 설정할 수 있지만 사용자는 서로 다른 서비스 집합을 선택할 수 없습니다.
- CPE 설정의 복잡성 증가.서비스 제공업체의 헬프 데스크 직원은 더 많은 지식을 갖춰야 합니다.사용자 이름과 비밀번호가 CPE에 구성되어 있으므로 가입자 또는 CPE 공급업체가 설정을 변경해야 합니다.여러 VC를 사용하면 구성 복잡성이 증가합니다.그러나 아직 릴리스되지 않은 자동 컨피그레이션 기능을 통해 이를 극복할 수 있습니다.
- 서비스 공급자는 모든 가입자에 대한 사용자 이름 및 비밀번호의 데이터베이스를 유지 관리해야 합니다.터널 또는 프록시 서비스를 사용하는 경우 도메인 이름을 기준으로 인증을 수행할 수 있으며 사용자 인증은 기업 게이트웨이에서 수행됩니다.이렇게 하면 서비스 공급자가 유지해야 하는 데이터베이스의 크기가 줄어듭니다.
- CPE에 단일 IP 주소를 제공하고 NAT/PAT를 구현하면 페이로드에 IP 정보를 포함하는 IPTV와 같은 특정 애플리케이션이 작동하지 않습니다.또한 IP 서브넷 기능을 사용하는 경우 CPE에 대해 IP 주소도 예약해야 합니다.

PPPoA 아키텍처의 구현 고려 사항

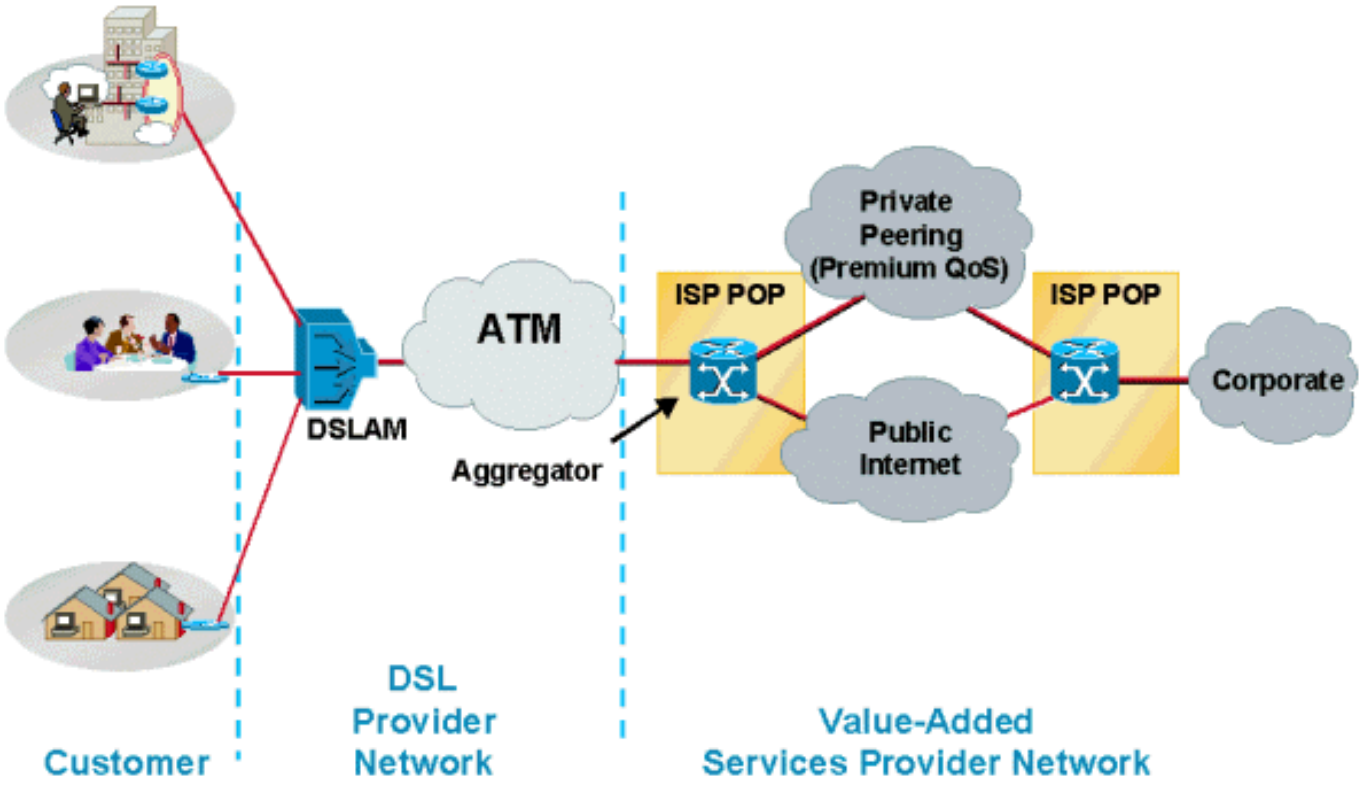
PPPoA 아키텍처를 구현하기 전에 고려해야 할 핵심 사항은 다음과 같습니다.

- 필요한 PPP 세션 수에 영향을 주기 때문에 현재 및 향후에 서비스될 가입자 수
- PPP 세션이 서비스 공급자의 어그리게이션 라우터에서 종료되는지 아니면 다른 회사 게이트웨이 또는 ISP(인터넷 서비스 공급자)로 전달되는지 여부.
- 서비스 공급자 또는 최종 서비스 대상이 가입자의 CPE에 IP 주소를 제공하는지 여부.
- 제공된 IP 주소가 합법적인 공용 주소인지 아니면 비공개 주소인지 여부.CPE가 NAT/PAT를 수행합니까, 아니면 종료 대상에서 NAT를 수행합니까?
- 최종 가입자, 가정용 사용자, SOHO(Small Office Home Office) 고객 및 재택 근무자의 프로필.
- 둘 이상의 사용자의 경우 모든 사용자가 동일한 최종 목적지 또는 서비스에 도달해야 하는지 아니면 모두 서로 다른 서비스 대상을 가지고 있는지 여부.
- 통신 사업자가 음성 또는 비디오와 같은 부가 가치 서비스를 제공합니까?통신 사업자는 최종 대상에 도달하기 전에 모든 가입자가 먼저 특정 네트워크로 가야 합니까?가입자가 SSG를 사용할 때 통과 서비스, PPP PTA(Terminated Aggregation), 중재 디바이스 또는 프록시를 사용합니까?
- 균일한 비율, 세션당 사용량 또는 사용된 서비스에 따라 통신 사업자가 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 및 음성 및 비디오와 같은 부가 가치 서비스 판매도 포함되어 있습니까?NAP와 NSP가 동일한 엔터티입니까?
- 회사의 비즈니스 모델입니다.ILEC(Independent Local Exchange Carrier), CLEC(Competitive Local Exchange Carrier) 또는 ISP와 비교됩니까?
- NSP가 최종 가입자에게 제공할 애플리케이션 유형.
- 예상되는 데이터 흐름의 업스트림 및 다운스트림 볼륨.

이러한 점을 염두에 두고, PPPoA 아키텍처가 통신 사업자를 위한 다양한 비즈니스 모델에 어떻게 적합하고 확장될 것인지 그리고 공급자가 이 아키텍처를 사용하여 어떤 혜택을 얻을 수 있는지 논의합니다.

일반적인 PPPoA 네트워크 아키텍처

다음 다이어그램은 일반적인 PPPoA 네트워크 아키텍처를 보여줍니다.CPE를 사용하는 고객은 ATM을 사용하여 Cisco 6400 어그리게이터에 연결되는 Cisco DSLAM을 통해 서비스 공급자의 네트워크에 연결합니다.



PPPoA 아키텍처의 설계 고려 사항

이 문서의 "구현 고려 사항" 섹션에서 서비스 공급자의 비즈니스 모델에 따라 다른 시나리오를 사용하여 PPPoA 아키텍처를 구축할 수 있습니다.이 섹션에서는 서비스 공급자가 솔루션을 구축하기 전에 고려해야 할 다양한 가능성과 고려 사항에 대해 살펴보겠습니다.

PPPoA 아키텍처 및 이 아키텍처에 대한 특정 솔루션을 구축하기 전에 서비스 공급자의 비즈니스 모델을 이해하는 것이 중요합니다.서비스 공급자가 제공할 서비스를 고려하십시오.이 통신 사업자는 최종 가입자에게 고속 인터넷 액세스와 같은 하나의 서비스를 제공할 것인가, 아니면 다른 ISP에 도매 서비스를 판매하고 이러한 가입자에게 부가 가치 서비스를 제공할 것인가?통신 사업자가 모든 서비스를 제공합니까?

NSP와 NAP가 동일한 환경에서 고속 인터넷 액세스의 경우 구축된 어그리게이션 라우터에서 가입자의 PPP 세션을 종료해야 합니다.이 시나리오에서 서비스 공급자는 단일 라우터 어그리게이션 디바이스에서 종료할 수 있는 PPP 세션 수, 사용자를 인증하는 방법, 어카운팅을 수행하는 방법 및 사용자 세션이 종료된 후 인터넷 경로를 고려해야 합니다.PPP 세션 및 가입자 수에 따라 어그리게이션 라우터는 Cisco 6400 또는 Cisco 7200일 수 있습니다.현재 NRP(Node Route Processor)가 7개인 Cisco 6400은 최대 14,000개의 PPP 세션을 종료할 수 있습니다.Cisco 7200은 2,000개의 PPP 세션으로 제한됩니다.이러한 수치는 새로운 릴리스에 따라 달라집니다.각 어그리게이션 라우터가 지원할 수 있는 세션의 정확한 수는 릴리스 정보 및 제품 문서를 확인하십시오.

이 시나리오에서 사용자 인증 및 어카운팅은 사용 중인 사용자 이름 또는 VPI/VCI(virtual path

identifier/virtual channel identifier)를 기반으로 사용자를 인증할 수 있는 업계 표준 RADIUS 서버를 사용하여 가장 효과적으로 처리됩니다.

고속 인터넷 액세스의 경우 NSP는 일반적으로 고객에게 균일한 요금을 청구합니다.현재 대부분의 구축은 이러한 방식으로 구현되고 있습니다.NSP와 NAP가 동일한 엔티티인 경우 고객은 고정 액세스 요금으로 청구되고 인터넷 액세스는 또 다른 고정 요금으로 청구됩니다.이 모델은 서비스 공급자가 부가 가치 서비스를 제공하기 시작할 때 변경됩니다.서비스 공급자는 서비스 유형 및 서비스 사용 기간을 기준으로 고객에게 비용을 부과할 수 있습니다.고객은 OSPF(Open Shortest Path First) 또는 EIGRP(Enhanced Interior Gateway Routing Protocol)와 같은 라우팅 프로토콜을 사용하여 어그리게이션 라우터를 통해 인터넷에 연결하여 BGP(Border Gateway Protocol)를 실행할 수 있는 에지 라우터에 연결합니다.

고속 인터넷 액세스를 제공하기 위해 통신 사업자가 가지고 있는 또 다른 옵션은 L2TP/L2F 터널링을 사용하여 가입자의 수신 PPP 세션을 별도의 ISP로 전달하는 것입니다.L2x 터널링을 사용할 경우 터널 대상에 도달할 수 있는 방법에 대해 특별히 고려해야 합니다.사용 가능한 옵션은 일부 라우팅 프로토콜을 실행하거나 어그리게이션 라우터에서 고정 경로를 제공하는 것입니다.L2TP 또는 L2F 터널을 사용할 때의 제한 사항은 다음과 같습니다.(1) 터널 수 및 터널 안에서 지원할 수 있는 세션 수(2) 정적 경로를 사용해야 할 수 있는 타사 ISP와 호환되지 않는 라우팅 프로토콜을 사용하는 경우

서비스 공급자가 최종 가입자에 대해 서로 다른 ISP 또는 기업 게이트웨이에 대한 서비스를 제공하는 경우 어그리게이션 라우터에서 SSG 기능을 구현해야 할 수 있습니다.이렇게 하면 가입자가 웹 기반 서비스 선택을 사용하여 다른 서비스 대상을 선택할 수 있습니다.서비스 공급자는 ISP로 향하는 모든 세션을 단일 PVC로 결합하여 선택한 대상에 가입자의 PPP 세션을 전달하거나 서비스 공급자가 여러 서비스 수준을 제공하는 경우 코어에 둘 이상의 PVC를 설정할 수 있습니다.

도매 서비스 모델에서는 통신 사업자가 SSG 기능을 사용할 수 없습니다.이 모델에서는 서비스 공급자가 모든 PPP 세션을 홈 게이트웨이로 확장합니다.홈 게이트웨이는 최종 가입자에게 IP 주소를 제공하고 최종 사용자를 인증합니다.

이러한 시나리오에서 가장 중요한 고려 사항은 통신 사업자가 다양한 서비스에 대해 다른 QoS(Quality of Service)를 제공하는 방법과 대역폭 할당을 계산하는 방법입니다.현재 대부분의 통신 사업자가 이 아키텍처를 구축하는 방식은 서로 다른 PVC에 서로 다른 QoS를 제공합니다.가정용 및 비즈니스 고객을 위해 코어에 별도의 PVC가 있을 수 있습니다.다른 PVC를 사용하면 통신 사업자가 다른 서비스에 대해 다른 QoS를 지정할 수 있습니다.이렇게 하면 QoS가 별도의 PVC 또는 레이어 3에 있을 수 있습니다.

레이어 3에서 QoS를 적용하려면 통신 사업자가 최종 목적지를 알아야 하며, 이는 제한 요인이 될 수 있습니다.그러나 다른 VC에 적용하여 레이어 2 QoS와 함께 사용할 경우 서비스 제공업체에 유용할 수 있습니다.이 모델의 제한 사항은 이 모델이 고정되어 있고 서비스 공급업체가 QoS를 사전에 프로비저닝해야 한다는 것입니다.서비스 선택 시 QoS가 동적으로 적용되지 않습니다.현재 사용자는 마우스 클릭 한 번으로 다양한 서비스에 대해 다른 대역폭을 선택할 수 없습니다.그러나 이 기능을 개발하기 위해 상당한 엔지니어링 작업이 투자되었습니다.

CPE는 사용자 이름 및 비밀번호에 대해 구성해야 하므로 이 아키텍처에서는 CPE 구축, 관리 및 프로비저닝이 매우 어려울 수 있습니다.간단한 솔루션으로서 일부 통신 사업자는 모든 CPE에 대해 동일한 사용자 이름과 비밀번호를 사용하고 있습니다.이는 상당한 보안 위험을 초래합니다.또한 CPE에서 서로 다른 세션을 동시에 열어야 하는 경우 CPE, NAP 및 NSP에서 추가 VC를 프로비저닝해야 합니다.Cisco DSLAM 및 어그리게이션 장치는 CPE 컨피그레이션 및 프로비저닝을 간소화할 수 있습니다.엔드 투 엔드 PVC 프로비저닝을 위해 플로우 스루 관리 툴도 사용할 수 있습니다.PVC를 사용하는 많은 가입자에 대해 NSP에서 프로비저닝하는 것은 모든 다른 PVC를 관리해야 하기 때문에 제한 요소입니다.또한 마우스를 클릭하거나 몇 개의 키 스트로크를 입력하여 단일 NRP에서 2000 PVC를 프로비저닝하는 간단한 방법이 없습니다.

현재 이 아키텍처의 다양한 구성 요소에 대해 서로 다른 관리 애플리케이션을 사용하고 있습니다. 예를 들어 DSLAM용 뷰어, Cisco 6400용 SCM 등이 있습니다. 모든 구성 요소를 프로비저닝할 단일 관리 플랫폼은 없습니다.이는 잘 알려진 제한이며 CPE, DSLAM 및 Cisco 6400을 프로비저닝하기 위한 종합적이고 단일 관리 애플리케이션을 사용하기 위해 많은 노력을 기울이고 있습니다.또한 현재 SVC와 함께 PPPoA를 구현할 수 있는 솔루션을 보유하고 있으며, 이를 통해 구축 작업을 훨씬 쉽게 수행할 수 있습니다.SVC를 사용하는 PPPoA는 최종 사용자가 동적으로 대상 및 QoS를 선택할 수도 있습니다.

이 아키텍처를 사용하는 대규모 ADSL 구축의 또 다른 중요한 점은 어그리게이션 라우터에서 RADIUS 서버로의 통신입니다.어그리게이션 디바이스에서 수천 개의 PPP 세션이 종료될 때 NRP 블레이드가 실패할 경우 해당 PPP 세션을 모두 다시 설정해야 합니다.즉, 모든 가입자를 인증해야 하며 연결이 설정되면 해당 어카운팅 레코드가 중지되고 다시 시작됩니다.많은 가입자가 동시에 인증을 시도하면 RADIUS 서버에 대한 파이프가 병목 현상이 발생할 수 있습니다.일부 가입자를 인증할 수 없으므로 서비스 공급자에 문제가 발생할 수 있습니다.

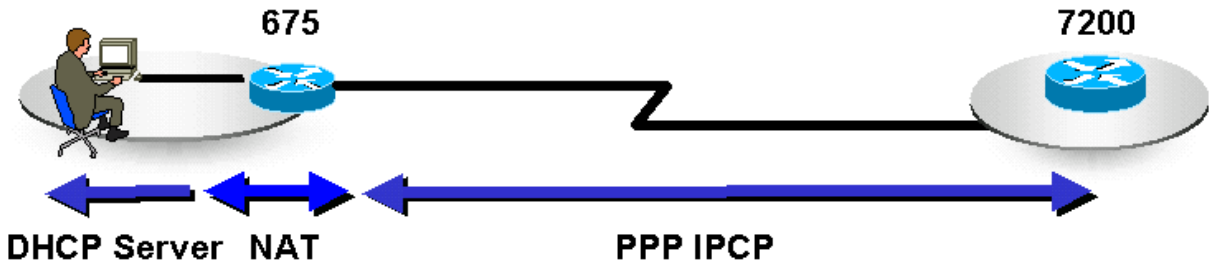
모든 가입자를 동시에 수용할 수 있는 충분한 대역폭이 있는 RADIUS 서버에 대한 링크가 있어야 합니다.또한 RADIUS 서버는 모든 가입자에게 권한을 부여할 수 있을 만큼 강력해야 합니다.수천 명의 가입자의 경우 사용 가능한 RADIUS 서버 간에 로드 밸런싱을 수행할 수 있는 옵션을 고려해야 합니다.이 기능은 Cisco IOS® Software에서 사용할 수 있습니다.

마지막으로, 어그리게이션 라우터는 많은 PPP 세션을 수용할 만큼 충분히 수행해야 합니다.다른 구현에서 사용하는 것과 동일한 트래픽 엔지니어링 원칙을 적용합니다.이전에는 지점 간 하위 인터페이스에서 PVC를 구성해야 했습니다.오늘날 PPPoA를 사용하면 다중 지점 하위 인터페이스와 포인트 투 포인트에서 여러 PVC를 구성할 수 있습니다.각 PPPoA 연결에는 더 이상 가상 액세스 인터페이스용, ATM 하위 인터페이스용 IDB(Interface Descriptor Block)가 두 개 필요하지 않습니다.이 개선 사항은 라우터에서 실행되는 PPPoA 세션의 최대 수를 늘립니다.

플랫폼에서 지원되는 최대 PPPoA 세션 수는 메모리 및 CPU 속도와 같은 사용 가능한 시스템 리소스에 따라 달라집니다.각 PPPoA 세션은 하나의 가상 액세스 인터페이스를 사용합니다.각 가상 액세스 인터페이스는 하드웨어 인터페이스 설명자 블록 및 hwidb/swidb(software interface descriptor block) 쌍으로 구성됩니다.각 위젯은 약 4.5K가 소요됩니다.각 위젯은 약 2.5K가 소요됩니다.가상 액세스 인터페이스를 함께 사용하려면 7.5K. 2000개의 가상 액세스 인터페이스가 필요합니다. 2000 * 7.5K 또는 15M.2,000개의 세션을 실행하려면 라우터에 1,500만 개의 세션이 추가로 필요합니다.세션 제한이 증가함에 따라 라우터가 더 많은 IDB를 지원해야 합니다.이러한 지원은 PPP 상태 시스템의 인스턴스를 더 많이 실행하기 위해 CPU 사이클의 증가로 인해 성능에 영향을 줍니다.

PPPoA 아키텍처의 핵심 포인트

이 섹션에서는 PPPoA 아키텍처의 세 가지 핵심 사항에 대해 설명합니다.CPE, IP 관리 및 서비스 대상에 도달합니다.



The CPE configuration in this architecture depends on NSP or the Corporate Gateway, which may terminate the PPP sessions from the subscriber. When the CPE is configured, it must have at least one set of VPI/VCI, and a username and password should be defined.

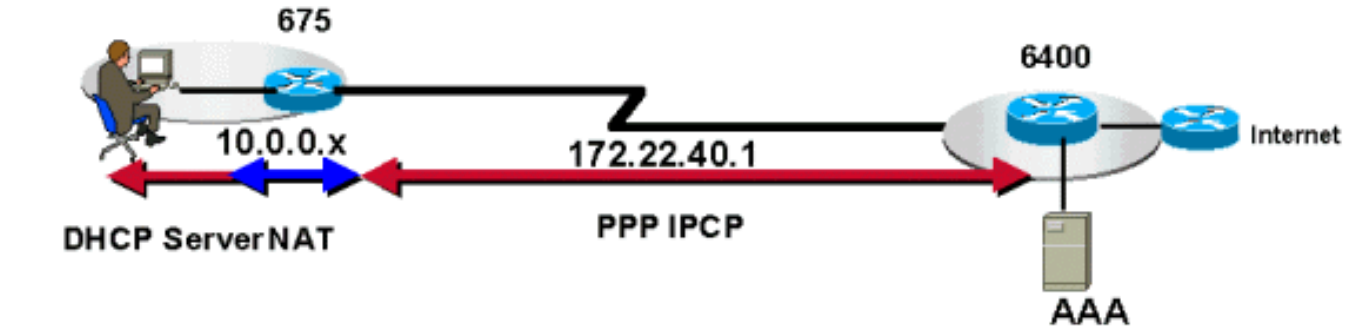
Optionally, the CPE may be configured as a DHCP server to provide private IP addresses to end stations on the LAN. The CPE can also be configured to do Port Address Translation (PAT). A CPE configured for PAT and DHCP usually gets a single public IP address from the final destination and all the stations on the LAN are translated to that address when they wish to go out of that network. Using this method the subscriber can easily host a Web or an email server using private IP addresses. Then, opening port 80 (HTTP) and port 25 (SMTP) on the static NAT entries in the CPE, these servers can be accessed from the outside. This is the most common scenario today.

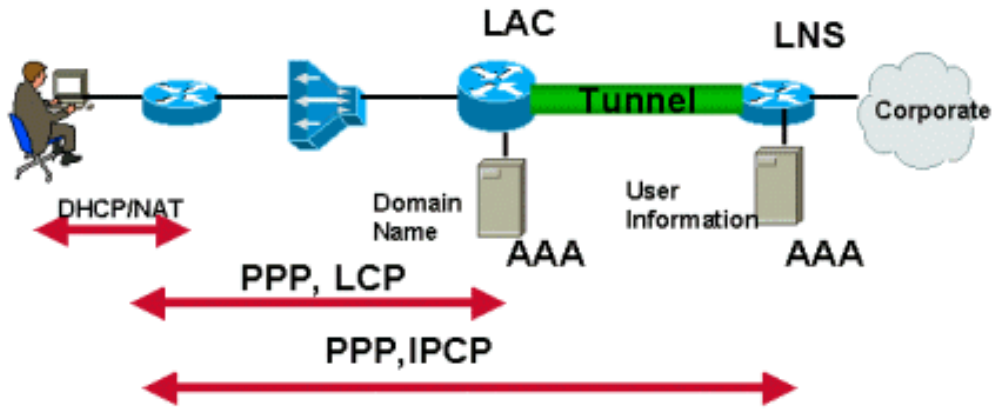
PAT의 특성 때문에 페이로드에 IP 정보를 포함하는 특정 애플리케이션은 이 시나리오에서 작동하지 않습니다.이 문제를 해결하려면 단일 IP 주소가 아닌 IP 주소의 서브넷을 적용합니다.

이 아키텍처에서는 IP 주소가 CPE에 할당되었으므로 NAP/NSP가 CPE에 텔넷하여 구성 및 문제를 해결하는 것이 더 쉽습니다.

CPE는 가입자의 프로필에 따라 다른 옵션을 사용할 수 있습니다.예를 들어 가정용 사용자의 경우 PAT/DHCP 없이 CPE를 구성할 수 있습니다.PC가 두 개 이상인 가입자의 경우 PAT/DHCP에 대해 또는 가정용 사용자의 CPE와 동일한 방식으로 CPE를 구성할 수 있습니다.CPE에 연결된 IP 전화기가 있는 경우 CPE가 둘 이상의 PVC에 대해 구성될 수 있습니다.

IP 관리





PPPoA 아키텍처에서 가입자 CPE에 대한 IP 주소 할당은 다이얼 모드에서 PPP의 동일한 원칙인 IPCP 협상을 사용합니다.IP 주소는 가입자가 사용하는 서비스 유형에 따라 할당됩니다.가입자가 NSP에서 인터넷에 액세스만 하는 경우 NSP는 가입자로부터 해당 PPP 세션을 종료하고 IP 주소를 할당합니다.IP 주소는 로컬로 정의된 풀, DHCP 서버에서 할당되거나 RADIUS 서버에서 적용할 수 있습니다.또한 ISP에서 가입자에게 정적 IP 주소 집합을 제공했을 수 있으며 가입자가 PPP 세션을 시작할 때 동적으로 IP 주소를 할당하지 않을 수 있습니다.이 시나리오에서 서비스 공급자는 RADIUS 서버만 사용하여 사용자를 인증합니다.

가입자가 여러 서비스를 사용할 수 있기를 원할 경우 NSP에서 SSG를 구현해야 할 수 있습니다.다음은 IP 주소를 할당할 수 있는 방법입니다.

- SP는 로컬 풀 또는 RADIUS 서버를 통해 가입자에게 IP 주소를 제공할 수 있습니다.사용자가 서비스를 선택하면 SSG는 해당 대상에 사용자의 트래픽을 전달합니다.SSG가 프록시 모드를 사용 중인 경우 최종 목적지는 IP 주소를 제공할 수 있습니다. 이 IP 주소는 SSG가 NAT의 표시 주소로 사용됩니다.
- PPP 세션은 서비스 공급자의 집계 라우터에서 종료되지 않습니다.최종 목적지 또는 홈 게이트웨이로 터널링되거나 전달됩니다. 그러면 결국 PPP 세션이 종료됩니다.최종 목적지 또는 홈 게이트웨이는 가입자와 IPCP를 협상하므로 IP 주소를 동적으로 제공합니다.고정 주소는 최종 목적지에서 해당 IP 주소를 할당하고 해당 주소에 경로를 갖는 한 가능합니다.

Cisco 6400 NRP용 Cisco IOS Software 릴리스 12.0.5DC 이전에는 통신 사업자가 가입자에게 IP 주소의 서브넷을 제공할 방법이 없었습니다.Cisco 6400 플랫폼과 Cisco 600 Series CPE를 사용하면 PPP 협상 중에 CPE에서 IP 서브넷을 동적으로 구성할 수 있습니다.이 서브넷의 IP 주소 하나가 CPE에 할당되고 나머지 IP 주소는 DHCP를 통해 스테이션에 동적으로 할당됩니다.이 기능을 사용하면 CPE를 PAT에 대해 구성할 필요가 없으며 일부 애플리케이션에서는 작동하지 않습니다.

서비스 대상에 도달하는 방법

PPPoA 아키텍처에서는 다양한 방식으로 서비스 대상에 연결할 수 있습니다.가장 일반적으로 사용

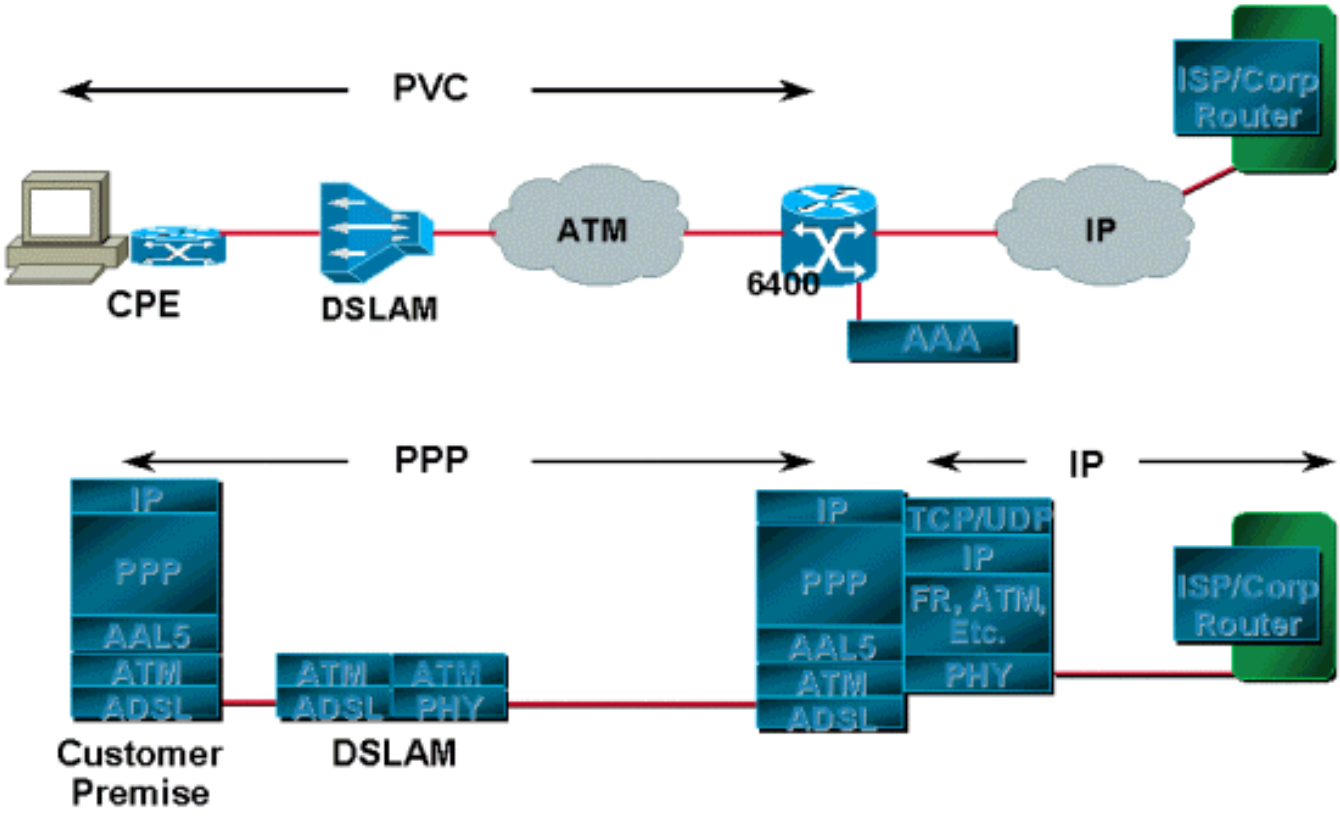
되는 몇 가지 방법은 다음과 같습니다.

- 서비스 공급자에서 PPP 세션 종료
- L2TP 터널링
- SSG 사용

세 가지 방법 모두 CPE에서 DSLAM으로 정의된 고정 PVC 집합이 있습니다. 이 집합은 어그리게이션 라우터의 고정 PVC 집합으로 전환됩니다.PVC는 ATM 클라우드를 통해 DSLAM에서 어그리게이션 라우터로 매핑됩니다.

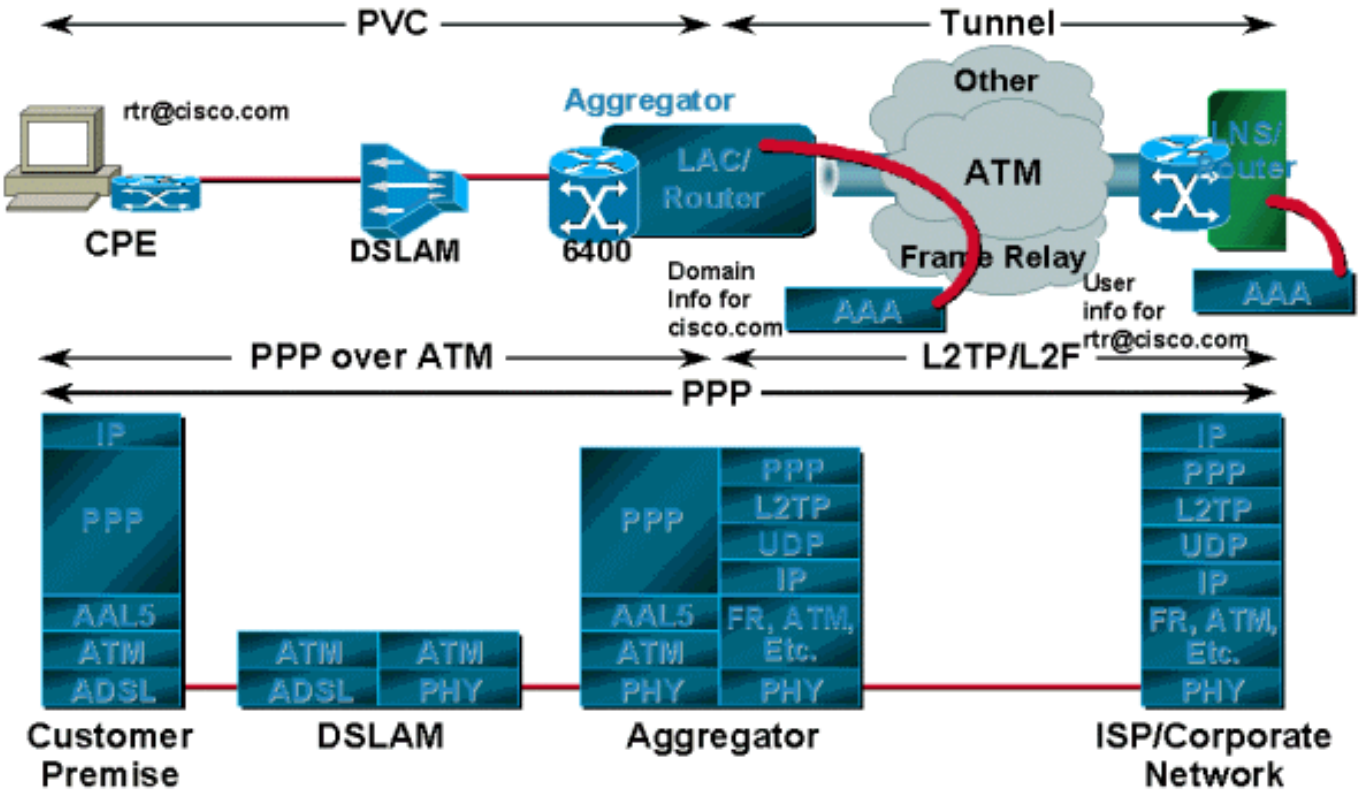
SVC가 있는 PPPoA 또는 Multiprotocol Label Switching/Virtual Private Network와 같은 다른 방법을 사용하여 서비스 대상에 연결할 수도 있습니다.이러한 방법은 이 문서의 범위를 벗어나며 별도의 문서에서 논의됩니다.

집계에서 PPP를 종료하는 중



가입자가 시작한 PPP 세션은 라우터의 로컬 데이터베이스 또는 RADIUS 서버를 통해 사용자를 인증하는 서비스 공급자에서 종료됩니다.사용자가 인증되면 IPCP 협상이 발생하고 IP 주소가 CPE에 할당됩니다.IP 주소가 할당되면 CPE와 어그리게이션 라우터에 모두 설정된 호스트 경로가 있습니다.가입자에 할당된 IP 주소(합법인 경우)는 에지 라우터에 광고됩니다.에지 라우터는 가입자가 인터넷에 액세스할 수 있는 게이트웨이입니다.IP 주소가 비공개인 경우 서비스 공급자는 에지 라우터로 광고하기 전에 이를 변환합니다.

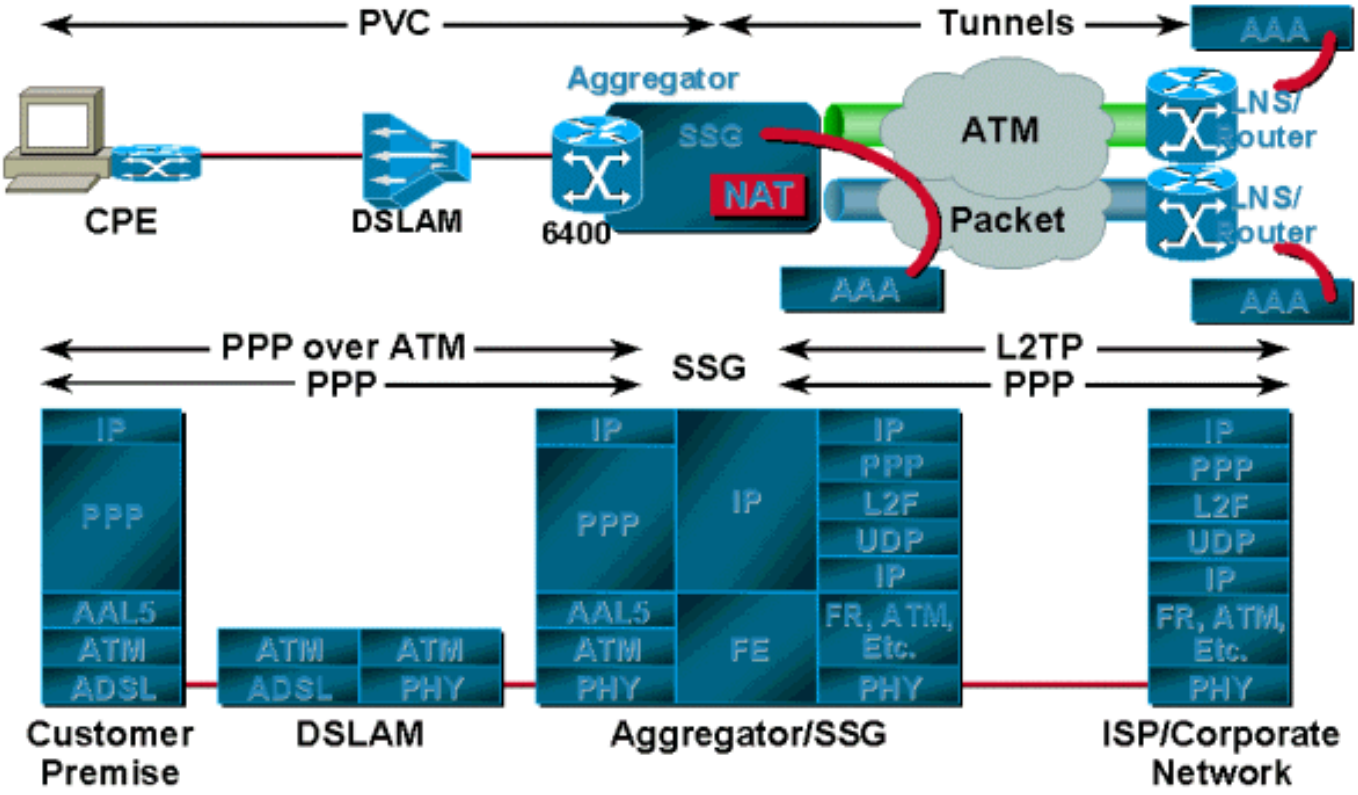
L2TP/L2F 터널링



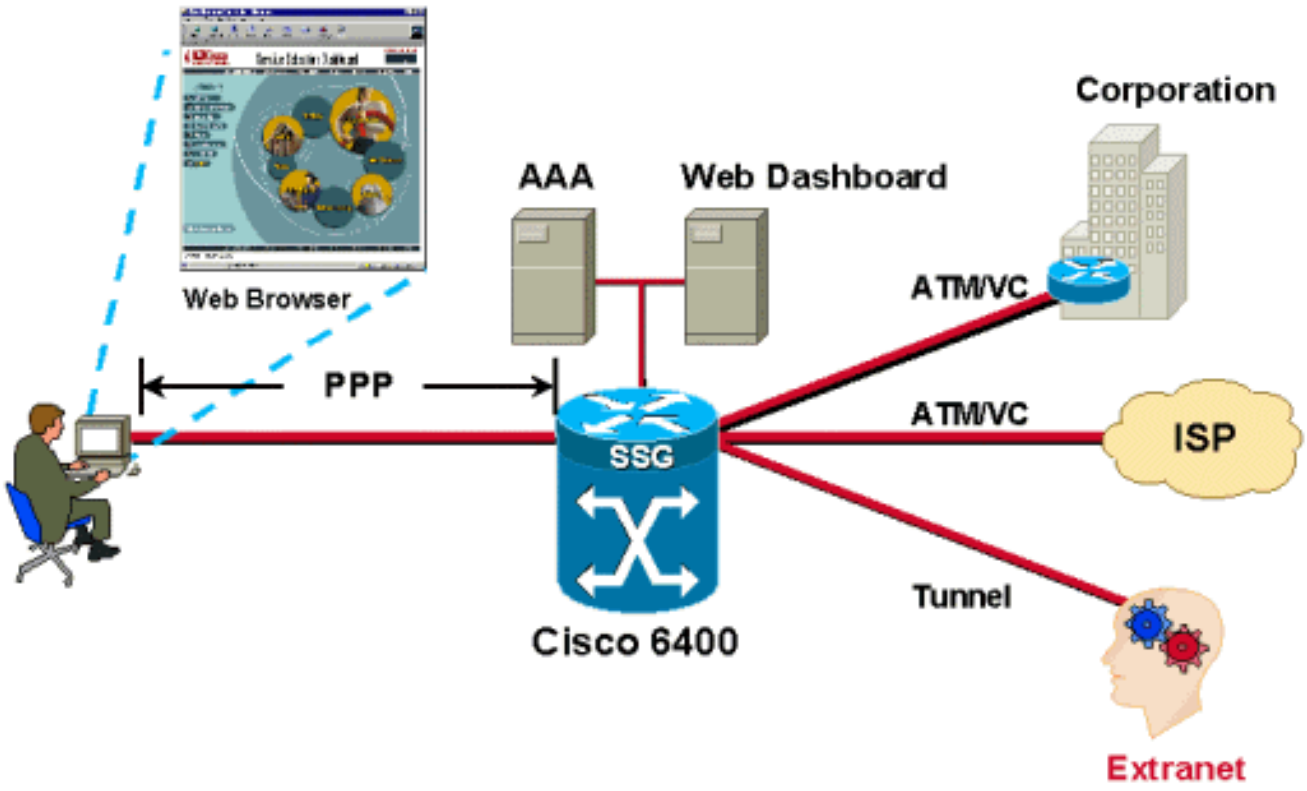
PPP 세션은 서비스 공급자 또는 법인에 따라 서비스 공급자의 집계 라우터에서 종료되는 대신 L2TP 또는 L2F를 사용하여 업스트림 종료 지점으로 터널링합니다.이 종료 지점은 사용자 이름을 인증하고 가입자에게 DHCP 또는 로컬 풀을 통해 IP 주소가 할당됩니다.이 시나리오에서는 일반적으로 L2TP Access Concentrator/network access server(LAC/NAS)와 홈 게이트웨이 또는 L2TP Network Server(LNS) 간에 하나의 터널이 설정됩니다. LAC는 도메인 이름을 기반으로 수신 세션을 인증합니다.사용자 이름은 최종 목적지 또는 홈 게이트웨이에서 인증됩니다.

그러나 이 모델에서는 최종 목적지에 대한 액세스 권한만 가질 수 있으며 한 번에 하나의 목적지만 액세스할 수 있습니다.예를 들어 CPE가 사용자 이름 rtr@cisco.com으로 구성된 경우 해당 CPE 뒤에 있는 PC는 Cisco 도메인에만 액세스할 수 있습니다.다른 기업 네트워크에 연결하려면 해당 기업 도메인 이름을 반영하도록 CPE에서 사용자 이름과 암호를 변경해야 합니다.이 경우 터널 대상은 라우팅 프로토콜, 고정 경로를 사용하거나 ATM을 통한 기존 IP(ATM이 Layer 2로 선호되는 경우)를 사용하여 도달할 수 있습니다.

SSG(서비스 선택 게이트웨이) 사용



SSG over tunneling의 주요 장점은 SSG가 일대다 서비스의 매핑을 제공하는 반면 터널링은 일대일 매핑만 제공한다는 것입니다.이 기능은 단일 사용자가 여러 서비스에 액세스해야 하거나 단일 위치에서 여러 사용자에게 각각 고유한 서비스에 액세스해야 하는 경우 매우 유용합니다.SSG는 다양한 서비스로 구성되어 있으며 사용자에게 제공되는 웹 기반 SSD(Service Selection Dashboard)를 사용합니다.사용자는 한 번에 하나의 서비스 또는 여러 서비스에 액세스할 수 있습니다.SSG를 사용할 때의 또 다른 이점은 통신 사업자가 사용한 서비스 및 세션 시간을 기준으로 사용자에게 요금을 부과할 수 있으며 사용자가 SSD를 통해 서비스를 켜거나 끌 수 있다는 것입니다.



사용자는 가입자로부터 PPP 세션이 수신될 때 인증됩니다.사용자는 로컬 풀 또는 RADIUS 서버에서 IP 주소를 할당합니다.사용자가 성공적으로 인증되면 SSG 코드에 의해 소스 객체가 생성되고 사용자에게 기본 네트워크에 대한 액세스 권한이 부여됩니다.기본 네트워크에는 SSD 서버가 포함됩니다.브라우저를 사용하면 사용자가 대시보드에 로그인하고 AAA 서버에서 인증하며 RADIUS 서버에 저장된 사용자의 프로필에 따라 액세스할 수 있는 서비스 집합이 제공됩니다.

인증된 사용자가 서비스를 선택할 때마다 SSG는 해당 사용자에 대한 대상 객체를 생성합니다.대상 개체에는 대상 주소, 해당 대상의 DNS 서버 주소, 홈 게이트웨이에서 할당된 소스 IP 주소 등의 정보가 포함됩니다.사용자 측에서 들어오는 패킷은 대상 객체에 포함된 정보에 따라 대상으로 전달됩니다.

프록시 서비스, 투명 패스스루 또는 PTA에 대해 SSG를 구성할 수 있습니다.가입자가 프록시 서비스에 대한 액세스를 요청하면 NRP-SSG는 액세스 요청을 원격 RADIUS 서버에 전달합니다 .access-accept를 수신하면 SSG는 access-accept로 가입자에게 응답합니다.SSG는 원격 RADIUS 서버에 대한 클라이언트로 나타납니다.

투명 패스스루를 사용하면 인증되지 않은 가입자 트래픽이 SSG를 통해 어떤 방향으로든 라우팅될 수 있습니다.필터를 사용하여 투명한 통과 트래픽을 제어합니다.

PTA는 PPP 유형 사용자만 사용할 수 있습니다.인증, 권한 부여 및 계정 관리는 프록시 서비스 유형과 동일하게 수행됩니다.가입자가 user@service 형식의 사용자 이름을 사용하여 서비스에 로그인합니다.SSG는 이를 RADIUS 서버로 전달하여 서비스 프로필을 SSG에 로드합니다.SSG는 서비스 프로필의 RADIUS 서버 특성에 지정된 대로 원격 RADIUS 서버에 요청을 전달합니다.요청이 인증되면 IP 주소가 가입자에게 할당됩니다.NAT가 수행되지 않습니다.모든 사용자 트래픽이 원격 네트워크에 집계됩니다.PTA를 사용하면 사용자는 하나의 서비스에만 액세스할 수 있으며 기본 네트워크 또는 SSD에 액세스할 수 없습니다.

PPPoA 아키텍처에 대한 운영 설명

CPE의 전원이 처음 켜지면 LCP 컨피그레이션 요청을 어그리게이션 서버로 보내기 시작합니다 .PVC가 구성된 어그리게이션 서버는 PVC와 연결된 가상 액세스 인터페이스에서 LCP 컨피그레이션 요청도 전송합니다. 각 사용자가 서로의 컨피그레이션 요청을 확인하면 요청을 승인하고 LCP 상태가 열리게 됩니다.

인증 단계의 경우 CPE는 인증 요청을 어그리게이션 서버로 전송합니다.서버는 구성에 따라 도메인 이름(제공된 경우)을 기반으로 사용자를 인증하거나 로컬 데이터베이스 또는 RADIUS 서버를 사용하여 사용자 이름을 인증합니다.구독자의 요청이 username@domainname 형식인 경우 집계 서버는 대상에 대한 터널을 생성하려고 시도합니다(아직 없는 경우).터널이 생성되면 집계 서버는 가입자에서 대상으로 PPP 요청을 전달합니다.그러면 대상이 사용자를 인증하고 IP 주소를 할당합니다 .가입자의 요청에 도메인 이름이 포함되지 않은 경우 사용자는 로컬 데이터베이스에서 인증됩니다 .어그리게이션 라우터에 SSG가 구성된 경우 사용자는 지정된 대로 기본 네트워크에 액세스할 수 있으며 다른 서비스를 선택하는 옵션을 얻을 수 있습니다.

결론

PPPoA는 확장성이 뛰어나고 SSG 기능을 사용하며 보안을 제공하기 때문에 많은 통신 사업자에게 가장 적합한 아키텍처가 되고 있습니다.이 백서의 핵심은 PPPoA 아키텍처이므로 SSG와 같은 기능을 심층적으로 다룰 수 없었습니다.이러한 기능은 후속 문서에서 다룹니다.이 문서에서 설명하는 다양한 시나리오에 대한 샘플 구성도 함께 제공되며 별도의 문서로 설명합니다.

관련 정보

- Cisco DSL 제품 지원 정보
- Technical Support - Cisco Systems