RFC1483 브리징 기본 아키텍처

목차

소개

이 문서에서는 RFC1483 브리징을 사용할 때 ADSL(end-to-end asymmetric digital subscriber line) 아키텍처에 대해 설명합니다.대부분의 초기 xDSL 모뎀은 호스트 측의 10BaseT 이더넷 브리지 및 WAN 측의 캡슐화된 브리지 프레임 간의 브리지였습니다.오늘날에도 현장에 구축된 ADSL CPE(customer premises equipment)의 대부분은 순수 브리징 모드에 있습니다.

가정

기본 아키텍처는 RFC1483 브리징 모델 및 ATM을 핵심 백본으로 사용하여 최종 가입자에게 고속 인터넷 액세스를 제공한다는 가정하에 설계되었습니다.이 문서의 내용은 기존 구축 및 일부 내부 테스트의 아키텍처를 기반으로 합니다.

기술 개요

RFC1483은 ATM 네트워크를 통해 연결 없는 네트워크 인터커넥트 트래픽을 전송하는 두 가지 다른 방법을 설명합니다.라우팅된 PDU(Protocol Data Unit) 및 브리징 PDU

라우팅을 사용하면 단일 ATM VC(Virtual Circuit)를 통해 여러 프로토콜을 멀티플렉싱할 수 있습니다. PDU의 프로토콜은 PDU를 IEEE 802.2 LLC(Logical Link Control) 헤더로 미리 고정하여 식별됩니다.

브리징은 ATM 가상 회로를 통해 암시적으로 상위 계층 프로토콜 멀티플렉싱을 수행합니다.자세한 내용은 RFC1483을 참조하십시오.

이 문서는 브리징 PDU만 참조합니다.

RFC1483 브리징의 장점 및 단점

다음은 RFC1483 브리징 아키텍처의 장점과 단점에 대한 요약입니다.이 아키텍처에는 몇 가지 중요한 단점이 있는데, 대부분 브리징 모델에 내재되어 있습니다.ADSL을 고객 사이트에서 구축하는 과정에서 몇 가지 단점이 발견되었습니다.

장점

- 이해하기 쉬움.사용자의 라우팅 또는 인증 요구 사항과 같은 복잡한 문제가 없으므로 브리징은 매우 간단하게 이해하고 구현할 수 있습니다.
- CPE의 최소 구성통신 사업자는 더 이상 많은 수의 트럭 롤(truck roll)이 필요하지 않으며 더 높은 수준의 프로토콜 지원을 위해 인력을 집중 투자할 필요가 없기 때문에 이 점이 중요하다고 생각합니다.브리지 모드의 CPE는 매우 간단한 장치 역할을 합니다.이더넷에서 들어오는 모든 것이 WAN 쪽으로 직접 전달되기 때문에 CPE에는 최소 수준의 문제 해결이 포함됩니다.
- 설치가 간편합니다.브리징 아키텍처는 단순한 특성 때문에 쉽게 설치할 수 있습니다.엔드 투 엔드 PVC(Permanent Virtual Circuits)가 설정되면 상위 레이어 프로토콜의 IP와 같은 활동이 투명하게 됩니다.
- 가입자에 대한 다중 프로토콜 지원.CPE가 브리징 모드에 있을 때 어떤 상위 레이어 프로토콜이 캡슐화되는지는 상관없습니다.
- 단일 사용자 환경에서 인터넷 액세스에 이상적입니다.CPE는 셋톱 박스 역할을 하므로 상위 레이어 프로토콜에는 복잡한 트러블슈팅이 필요하지 않습니다.최종 PC에는 추가 클라이언트 설치가 필요하지 않습니다.

단점

- 브리징은 연결을 설정하기 위해 브로드캐스트에 크게 의존합니다.수천 명의 사용자 간의 브로드캐스트는 기본적으로 확장성이 없습니다.그 이유는 브로드캐스트가 사용자의 xDSL 루프를 통해 대역폭을 소비하고, 브로드캐스트에는 ATM PVC(point-to-point) 미디어를 통해 브로드캐스트에 대한 패킷을 복제하기 위해 헤드 엔드 라우터의 리소스가 필요하기 때문입니다.
- 브리징은 기본적으로 안전하지 않으며 신뢰할 수 있는 환경이 필요합니다.ARP(Address Resolution Protocol) 회신을 스푸핑하고 네트워크 주소를 해킹할 수 있습니다.또한 로컬 서브넷에서 브로드캐스트 공격을 시작할 수 있으므로 로컬 서브넷의 모든 멤버에 대한 서비스를 거부할 수 있습니다.
- IP 주소 하이재킹이 가능합니다.

구현 고려 사항

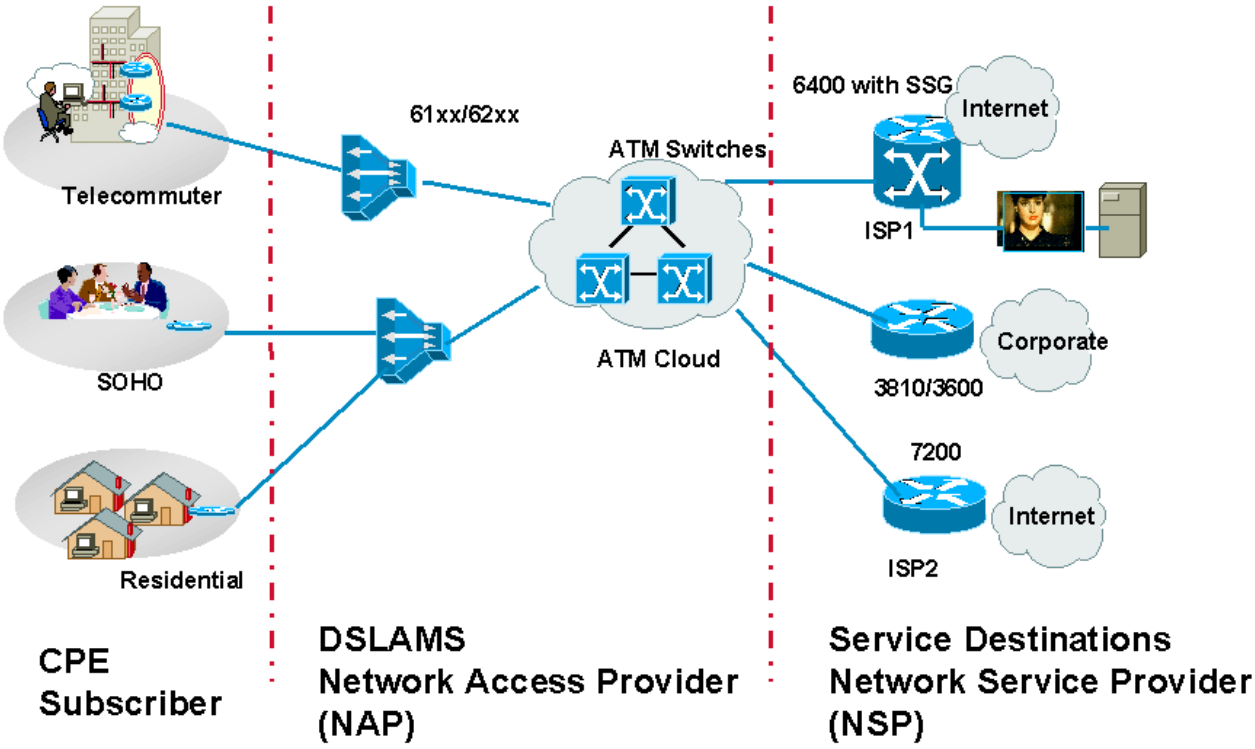
RFC1483 브리징 아키텍처를 구현하기 전에 다음 질문을 고려하십시오.

- 서비스할 구독자의 현재 및 계획된 수는 얼마입니까?
- 가입자는 서로 커뮤니케이션해야 합니까?
- 이러한 가입자는 단일 사용자 거주 고객입니까?CPE 뒤에 작은 LAN이 있을 수 있는 소규모 사무실, 홈 오피스(SOHO) 고객에게 서비스를 제공합니까?
- CPE, DSLAM(Digital Subscriber Line Access Multiplexer) 및 어그리게이션 POP(Post Office Protocols)의 구축 및 프로비저닝은 무엇입니까?

- NAP(Network Access Provider)와 NSP(Network Service Provider)가 같은 엔터티입니까?NAP의 비즈니스 모델에는 안전한 기업 액세스와 같은 도매 서비스, 음성 및 비디오와 같은 부가 가치 서비스 판매도 포함됩니까?
- NSP가 서비스 선택 기능을 제공하기를 원합니까?
- 회계 및 청구를 어떻게 달성할 수 있습니까?사용량, 대역폭, 서비스별 중 어느 것입니까?
- ILEC(Independent Local Exchange Carrier), CLEC(Competitive Local Exchange Carrier) 또는 ISP(Internet Service Provider)의 비즈니스 모델입니까?
- NSP가 최종 가입자에게 제공하고자 하는 애플리케이션 유형은 무엇입니까?
- 업스트림 및 다운스트림 모두에서 데이터 흐름 볼륨은 무엇입니까?

이러한 점을 고려해 볼 때, 다음은 RFC1483 브리징 아키텍처가 서로 다른 비즈니스 모델에 적합하고 확장되는 방식에 대한 설명입니다.

네트워크 아키텍처



RFC1483 브리징:네트워크 아키텍처

설계 고려 사항

앞서 언급한 대로, RFC1483 브리징 아키텍처에 몇 가지 고유한 문제가 있습니다.

IOS 가입자 브리징 기능은 이러한 문제의 일부를 해결합니다.브리지 그룹에 가입자 정책을 선택적으로 적용하면 각 ADSL 루프에서 ARP, 알 수 없는 패킷 및 기타 트래픽의 플러딩을 제어합니다.예

를 들어, ARP가 브로드캐스트되지 않도록 방지함으로써 적대적 사용자는 다른 사용자의 IP 주소를 검색할 수 없습니다.

또 다른 해결책은 모든 가입자를 하나의 하위 인터페이스에 추가하는 것입니다.정상적인 브리징 동작은 프레임을 수신한 포트로 프레임을 전달하지 않습니다.본질적으로, 가입자 간 모든 패킷이 필터링되는 가입자 브리징 유형을 적용합니다.그러나 이 접근 방식에는 다음과 같은 결함이 있습니다.

- 가입자 정책은 하위 인터페이스 간에만 적용됩니다.서로 다른 두 사용자 간에 가입자 정책을 적용하려면 각 사용자가 다른 ATM 하위 인터페이스에 있어야 합니다.
- 레이어 2-레이어 3 주소 매핑이 학습되기 때문에(ARP를 통해) 적대적 사용자는 다른 사용자의 연결을 하이잭(hijack)할 수 있습니다.이는 다른 사용자의 IP 주소로 ARP 트래픽을 생성하고 다른 MAC 주소를 사용하여 수행됩니다.

두 번째 시나리오는 캐리어 또는 ISP에 더 심각합니다.이 경우 모든 사용자는 프린터와 같은 PC 또는 이더넷 연결 장치에 잘못된 주소를 할당하고 다른 사용자에 대해 연결 문제를 일으킬 수 있습니다.이러한 오류나 공격은 공격자의 MAC 주소를 추적해야만 행위자를 추적할 수 있기 때문에 정확하게 찾아내지 못합니다.

일부 통신사는 브리지 그룹 간에 사용자를 분리하고 하위 인터페이스 간에 가입자 브리징을 구현하여 이 문제를 해결하려고 합니다.이 경우 IRB(Integrated Routing and Bridging)가 필요한 경우 각 사용자에게 고유한 브리지 그룹과 BVI(Bridge Group Virtual Interface)가 할당됩니다. 이러한 접근 방식은 가입자당 2개의 인터페이스를 사용하므로 관리하기가 어려울 수 있습니다.

이러한 문제는 Cisco 6400의 Cisco IOS® Software Release 12.0(5)DC에 도입된 RBE(Routed Bridged Encapsulation) 기능을 통해 해결되고 해결됩니다.

브리징의 몇 가지 단점을 고려할 때 브리징 아키텍처가 왜 구현되었는지 궁금할 수 있습니다.답은 간단하다.필드에 설치된 ADSL CPE는 대부분 브리징 프레임을 포워딩할 수 있습니다.이러한 경우 NSP는 브리징을 구현해야 합니다.

오늘날 CPE는 ATM(PPPoA), RFC1483 브리징 및 RFC1483 라우팅을 통해 Point-to-Point 프로토콜을 수행할 수 있습니다.NSP는 브리징 또는 PPP를 수행할지 결정합니다.이 결정은 앞서 언급한 구현 고려 사항과 각 아키텍처의 장점 및 단점을 기반으로 합니다.

브리징 아키텍처의 단점에도 불구하고 NAP가 아닐 수 있는 소규모 ISP 또는 더 적은 수의 가입자를 제공하는 NAP/NSP에 적합합니다.이러한 시나리오에서 NAP는 일반적으로 모든 가입자 트래픽을 ISP/NSP로 전달하며, 이 경우 해당 가입자를 종료합니다.NAP는 ATM 또는 Frame Relay를 Layer 2 프로토콜로 사용하여 가입자 트래픽을 제공하도록 선택할 수 있습니다.

현재 세대 DSLAM을 사용하는 NAP는 ATM을 사용하여 가입자 트래픽만 전송할 수 있습니다.이 경우 ISP는 라우터에 대한 ATM 영구 가상 회로(PVC)를 종료해야 합니다.

ISP/NSP에 ATM 인터페이스가 없는 경우 ATM DXI(Encapsulation ATM Data Exchange Interface)가 포함된 일반 직렬 인터페이스를 사용하여 수신 브리지 PDU를 수용할 수 있습니다.

두 시나리오 모두에서 NSP/ISP는 라우터에서 IRB를 구성해야 할 수 있습니다(캡슐화 ATM DXI를 사용하거나 투명 브리징의 경우 제외). 오늘날 NSP/ISP 라우터에서 브리지 가입자를 종료하는 가장 일반적인 방법은 IRB를 구현하는 것입니다. 서비스 공급자는 점진적으로 RBE로 마이그레이션할 것으로 예상됩니다.

위에서 언급한 일부 제한 사항 때문에 NSP/ISP는 각 가입자 집합에 대해 별도의 브리지 그룹을 구성하거나 하나의 브리지 그룹에 있는 모든 가입자를 구성하도록 선택할 수 있습니다.일반적인 방법

은 몇 개의 브리지 그룹을 구성한 다음 개별 멀티포인트 인터페이스에서 모든 가입자를 구성하는 것입니다.앞에서 언급했듯이 동일한 멀티포인트 인터페이스의 가입자는 서로 통신할 수 없습니다 .특정 사용자가 통신해야 하는 경우 서로 다른 인터페이스에서 해당 가입자를 구성합니다(여전히 동일한 브리지 그룹에 있을 수 있음).

소규모 ISP/NSP의 경우, 브리징 가입자를 종료하는 데 사용되는 가장 일반적인 라우터는 Cisco 3810, Cisco 3600 및 Cisco 7200입니다.가입자 기반이 큰 ISP/NSP의 경우 Cisco 6400이 좋습니다 .이러한 라우터의 메모리 요구 사항을 계산하기 전에 다른 환경과 동일한 요소를 고려하십시오.사용자 수, 대역폭 및 라우터 리소스

이 아키텍처의 핵심 요소

다음은 아키텍처의 핵심 사항입니다.

CPE

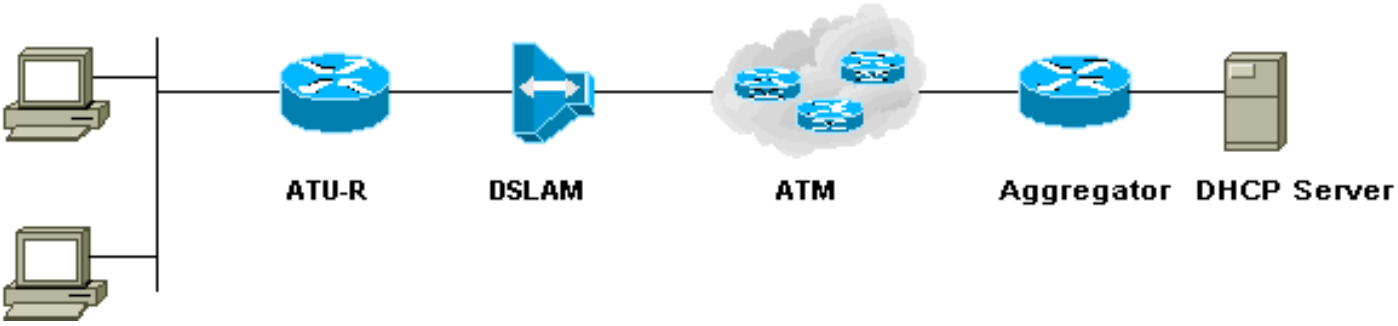
Cisco는 Cisco 및 타사 DSLAM과 함께 작동하는 다양한 CPE를 제공합니다.이러한 각 CPE에 대한 컨피그레이션은 문제가 없으며 가입자로부터 입력이 필요하지 않습니다.주요 요구 사항은 CPE가 ATM VPI/VCI(Virtual Path Identifier/Virtual Channel Identifier)를 정의한다는 것입니다. 이를 통해 CPE는 DSLAM을 사용하여 교육을 시작하고 트래픽을 전달할 수 있습니다.대부분의 경우 NAP는 모든 가입자에 대해 동일한 VPI/VCI를 구성할 수 있습니다.NAP는 일반적으로 가입자의 위치에 배포하기 전에 CPE를 미리 프로비저닝합니다.

브리징 아키텍처에서 CPE 및 CPE 구축의 주요 고려 사항은 CPE가 현장에 설치된 후 NAP가 CPE를 관리하는 방법입니다.브리징에는 CPE에 대한 IP 주소가 필요하지 않기 때문에 이러한 문제가 발생합니다.그러나 브리징 모드에서 Cisco CPE는 IP 주소로 프로비저닝할 수 있습니다.NAP는 이 기능을 사용하여 CPE에 텔넷하여 통계를 수집하거나 가입자의 문제 해결을 지원할 수 있습니다 .DSLAM을 통해 CPE를 관리할 수 있도록 새로운 프록시 요소 기능이 추가됩니다.

브리징 모드에서 CPE에 관리 IP 주소가 할당되지 않은 경우 운영자는 CPE 관리 포트를 통해서만 CPE를 관리할 수 있습니다.관리 IP 주소가 할당된 경우 운영자는 HTTP(Hypertext Transfer Protocol) 브라우저를 사용하여 디바이스를 관리할 수 있습니다.그러나 이 옵션은 일반적으로 사용할 수 없습니다.

CPE가 브리징 모드에 있을 때 서비스 대상(NSP/ISP일 수 있음)은 CPE 뒤에 있는 PC의 기본 게이트웨이로 사용될 IP 주소를 제공해야 합니다.이러한 PC는 올바른 기본 게이트웨이로 설정해야 합니다.그렇지 않으면 모뎀을 교육한 경우(즉, CPE와 DSLAM 간에 물리적 레이어가 양호함) 가입자가 트래픽을 전달하지 못할 수 있습니다.DHCP(Dynamic Host Configuration Protocol)를 사용하여 가입자 DHCP 주소를 할당하는 경우 기본 라우터가 DHCP 서버에서 반환되므로 문제가 아닙니다.

IP 관리



RFC1483 브리징:IP 관리

브리지 환경에서 IP 주소는 일반적으로 NSP/ISP 네트워크에 있는 서비스 대상에 있는 DHCP 서버에 의해 엔드 스테이션에 할당됩니다.이는 가장 일반적인 접근 방식이며 이 모델을 사용하는 대부분의 NSP/ISP에 의해 구현됩니다.

또 다른 방법은 가입자에게 고정 IP 주소를 제공하는 것입니다.이 경우 가입자 요건에 따라 IP 주소의 서브넷 또는 단일 IP 주소가 가입자별로 할당됩니다.예를 들어, 웹 서버 또는 이메일 서버를 호스팅하려는 가입자에게는 단일 IP 주소가 아닌 IP 주소 집합이 필요합니다.문제는 NSP/ISP가 공용 IP 주소를 제공해야 하며 이러한 주소가 곧 고갈될 수 있다는 점입니다.

일부 NSP/ISP는 가입자에게 사설 IP 주소를 제공했습니다.그런 다음 서비스 대상 라우터에서 NAT(Network Address Translation)를 수행합니다.

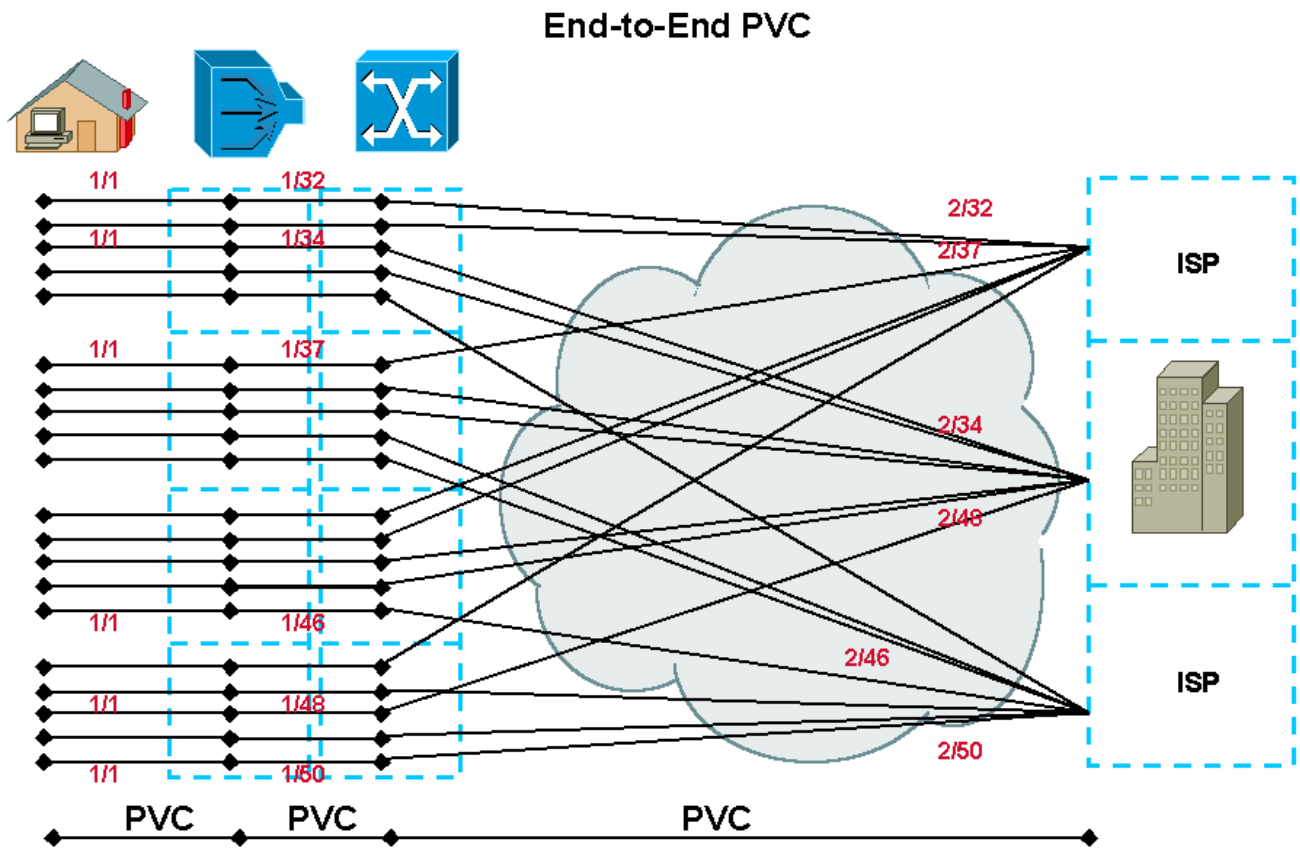
하나의 브리지 그룹(둘 이상의 가입자 포함)에 대해 전체 서브넷을 제공하는 NSP/ISP는 한 사용자가 프린터와 같은 PC 또는 이더넷 연결 장치에 잘못된 주소를 할당할 수 있으며 다른 사용자에 대해 연결 문제를 일으킬 수 있음을 알아야 합니다.

또한 NSP/ISP에서 서비스에 한 번에 액세스할 수 있는 PC 수를 제한할 수도 있습니다.이는 이더넷 인터페이스에서 최대 사용자를 구성하는 방식으로 수행됩니다.

그러나 이 방법은 다음과 같은 단점이 있습니다.3대의 PC가 서비스를 사용하도록 구성되어 있고 가입자 중 하나가 PC 중 하나가 유휴 상태일 때 네트워크 프린터(자체 MAC 주소가 있는)를 추가하면 CPE의 ARP 항목에서 PC의 MAC 주소가 사라집니다.

PC가 유휴 상태일 때 프린터가 활성 상태가 되면 ARP 항목에 프린터의 MAC 주소가 입력됩니다.사용자가 이 PC를 사용하여 인터넷에 액세스하기로 결정한 경우 CPE에서 이미 세 개의 MAC 항목을 허용했기 때문에 사용할 수 없습니다.CPE에서 사용자를 제한하는 전략을 사용할 수 있지만 숫자를 수정하는 데 주의를 기울여야 합니다.

서비스 대상에 도달하는 방법



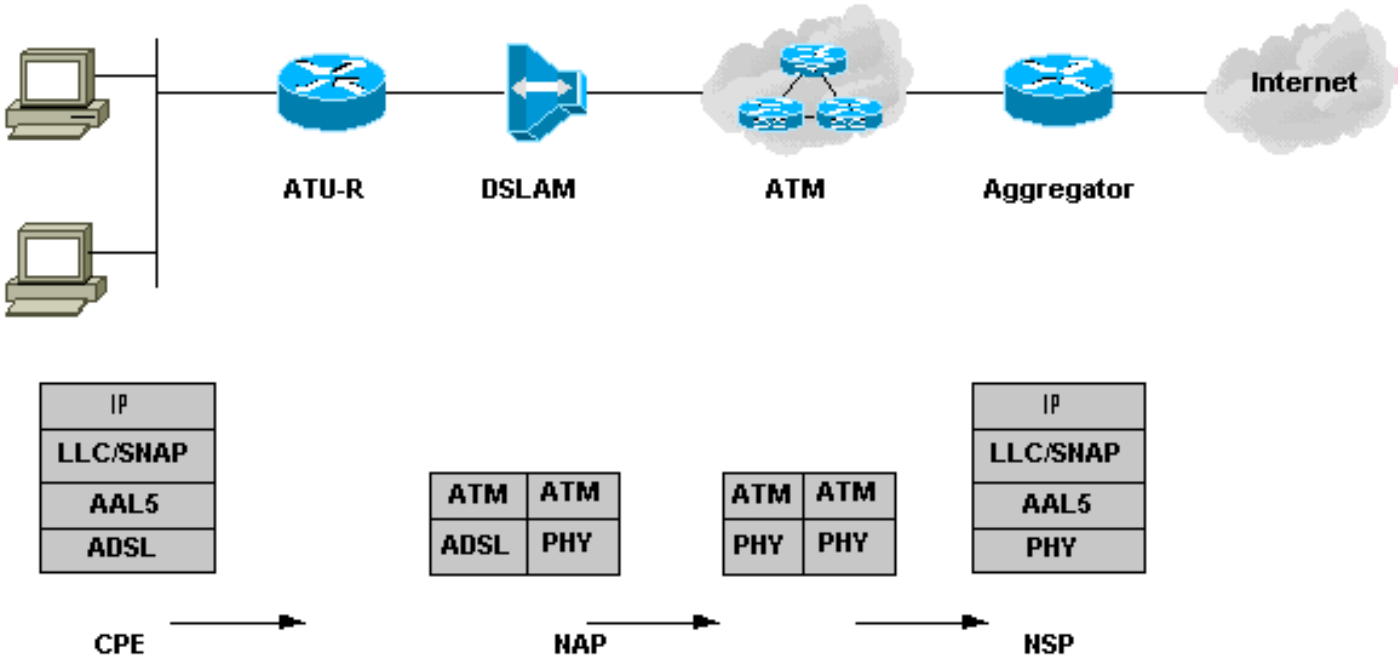
RFC1483 브리징:엔드 투 엔드 PVC

브리징이 있는 엔드 투 엔드 PVC 아키텍처에서는 각 홉의 PVC를 생성하여 서비스 대상에 연결합니다.그러나 NAP/NSP에는 이러한 PVC를 관리하는 것이 어려울 수 있습니다.또한 ATM 클라우드를 통해 정의할 수 있는 PVC의 수는 제한되어 있습니다.이 제한은 엔드 투 엔드 PVC 모델을 도입하는 NAP/NSP에 영향을 미칩니다.각 가입자에 대해 전체 경로에 고정 고유 VPI/VCI 집합이 있습니다.SVC(Switched Virtual Circuit)는 이러한 문제를 해결하는 데 도움이 되며, 많은 액세스 제공업체가 IP 지원 코어 네트워크로 마이그레이션하여 VC 소모 문제를 해결하고 있습니다.

또한 NSP/ISP는 가입자에게 다양한 서비스를 제공하기 위해 Cisco SSG(Service Selection Gateway) 기능을 사용할 수 있습니다.

이 아키텍처에서는 계층 2의 기업 라우터에서 직접 가입자 트래픽 PVC를 종료하여 기업 게이트웨이에 대한 보안 액세스를 구현합니다. PVC 기반 아키텍처는 다른 서비스 대상과 데이터를 공유할 때 기본적으로 안전합니다.

운영 설명



RFC1483 브리징:운영 설명

Cisco 6xx CPE는 기본적으로 라우팅 모드로 설정됩니다.따라서 브리징 모드로 구성되고 필요한 스플리터/마이크로필터로 가입자 위치에 설치되면 전원이 켜지면 자동으로 연결됩니다.CPE가 작동하면 CPE와 DSLAM 사이의 물리적 레이어가 정상임을 나타냅니다.엔드 스테이션의 IP 주소 구성 방식(즉, DHCP 서버를 통해 할당되었는지 또는 기본 게이트웨이 정보가 있는 고정 IP 주소인지 여부)에 따라 서비스 대상과 통신할 수 있습니다.

다음은 패킷 플로우에 대한 설명입니다.

사용자의 데이터는 PC에서 IEEE 802.3으로 캡슐화되고 Cisco 6xx CPE로 들어갑니다.그런 다음 LLC/SNAP(Logical Link Control/Subnetwork Access Protocol) 헤더로 캡슐화되며, ATM 적응형 레이어 5(AAL5)에서 캡슐화되고 ATM 레이어로 전송됩니다.

그런 다음 ATM 셀은 ADSL 전송 기술, CAP(Carrierless Amplitude and Phase) 변조 또는 DMT(Discrete Multi-Tone)에 의해 변조되고 DSLAM으로 와이어를 통해 전송됩니다.DSLAM에서 이러한 모듈형 신호는 POTS Splitter에서 먼저 수신되며, 이는 신호의 주파수가 4kHz 이하인지 여부를 확인합니다.신호를 4kHz 이상으로 식별한 후 DSL 전송 장치 - 중앙 사무실(ATU-C)으로 전달합니다.

ATU-C는 신호를 분석하고 ATM 셀을 검색합니다. ATM 셀은 멀티플렉싱 디바이스(MUX)에서 NIC(네트워크 인터페이스 카드)로 전달됩니다. NIC는 ATM 헤더에서 가입자 측 VPI/VCI 정보를 확인하고 서비스 대상 라우터로 전달할 다른 VPI/VCI로 스위칭을 결정합니다.서비스 대상 라우터는 특정 ATM 인터페이스에서 이러한 셀을 수신한 후 다시 어셈블하고 상위 레이어를 확인한 다음 BVI 인터페이스에 정보를 전달합니다.BVI 인터페이스는 레이어 3 정보를 확인하고 패킷이 전달되는 위치를 결정합니다.

결론

RFC1483 브리징 모델은 확장성이 문제가 되지 않는 소규모 ISP 또는 기업 액세스에 더 적합합니다.이를 이해하고 구현하는 것은 매우 간단하기 때문에 더 작은 규모의 ISP를 선택할 수 있게 되었습니다.그러나 일부 보안 및 확장성 문제로 인해 브리징 아키텍처의 인기가 떨어지고 있습니다.NSP/ISP는 RBE를 선택했거나 PPPoA 또는 PPPoE로 전환하고 있습니다. PPPoA는 확장성이 뛰어나고 매우 안전하지만 구현이 더 복잡하고 어렵습니다.

관련 정보

- DSL 기술 지원
- Technical Support - Cisco Systems