RFC1483 Bridging-Baseline-Architektur

Inhalt

Einführung

Dieses Dokument beschreibt die End-to-End-Architektur der ADSL (Asymmetric Digital Subscriber Line) bei der Verwendung von RFC1483-Bridging. Beachten Sie, dass es sich bei den meisten früheren Versionen von xDSL-Modems um Bridges zwischen 10BaseT Ethernet auf der Hostseite und gekapselten RFC1483-Bridge-Frames auf der WAN-Seite handelte. Noch heute befinden sich die meisten am Standort implementierten ADSL-Geräte für Kundenstandorte im reinen Bridging-Modus.

Annahme

Bei der Entwicklung der Basisarchitektur wird davon ausgegangen, dass Endkunden über das RFC1483-Bridging-Modell und den ATM als Core-Backbone Hochgeschwindigkeits-Internetzugriff erhalten. Der Inhalt dieses Dokuments basiert auf der Architektur bestehender Bereitstellungen und einiger interner Tests.

Technologiebeschreibung

RFC 1483 beschreibt zwei verschiedene Methoden für die Übertragung von verbindungslosem Netzwerkverbindungen über ein ATM-Netzwerk: geroutete Protokoll-Dateneinheiten (PDUs) und überbrückte PDUs.

Routing ermöglicht das Multiplexing mehrerer Protokolle über einen einzigen ATM Virtual Circuit (VC). Das Protokoll einer mitgeführten PDU wird identifiziert, indem der PDU ein IEEE 802.2

Logical Link Control (LLC)-Header vorangestellt wird.

Bridging führt ein Protokoll-Multiplexing auf höherer Ebene durch, das implizit von virtuellen ATM-Schaltkreisen ausgeführt wird. Weitere Informationen finden Sie unter RFC1483.

Dieses Dokument bezieht sich nur auf überbrückte Stromverteilereinheiten.

Vorteile und Nachteile von RFC1483-Bridging

Im Folgenden werden die Vor- und Nachteile der RFC1483 Bridging-Architektur zusammengefasst. Diese Architektur hat einige wichtige Nachteile, die meisten von ihnen sind in der Bridging-Modell. Einige der Nachteile wurden bei ADSL-Bereitstellungen an Kundenstandorten festgestellt.

Vorteile

- Einfach zu verstehen.Bridging ist sehr einfach zu verstehen und zu implementieren, da es keine komplexen Probleme wie Routing oder Authentifizierungsanforderungen für Benutzer gibt.
- Minimale CPE-KonfigurationDer Service Provider hält dies für wichtig, da er nicht mehr eine große Anzahl von Technikereinsätzen benötigt und nicht mehr viel in Personal für die Unterstützung von Protokollen höherer Ebene investieren muss. Der CPE im Bridge-Modus fungiert als sehr einfaches Gerät. Beim CPE ist nur eine minimale Fehlerbehebung erforderlich, da alles, was vom Ethernet eingeht, direkt an die WAN-Seite weitergeleitet wird.
- Einfache Installation.Die Bridging-Architektur ist einfach zu installieren, da sie sehr einfach ist. Nach der Einrichtung von End-to-End-PVCs (Permanent Virtual Circuits) werden Aktivitäten wie IP auf den Protokollen der oberen Schicht transparent.
- Unterstützung mehrerer Protokolle für den Teilnehmer.Wenn sich das CPE im Bridging-Modus befindet, geht es nicht darum, welches Protokoll der oberen Schicht gekapselt wird.
- Ideal für den Internetzugriff in einer einzigen Benutzerumgebung.Da das CPE als Set-Top-Box fungiert, ist für Protokolle der oberen Schicht keine komplexe Fehlerbehebung erforderlich. Auf den End-PCs ist keine zusätzliche Client-Installation erforderlich.

Nachteile

- Das Bridging hängt in hohem Maße von Broadcasts ab, um die Konnektivität herzustellen.Broadcasts zwischen Tausenden von Benutzern sind von Natur aus nicht skalierbar. Die Gründe hierfür sind, dass die Broadcast-Übertragung Bandbreite über die xDSL-Schleife der Benutzer verbraucht, und für die Übertragung werden Ressourcen am Head-End-Router benötigt, um Pakete für die Broadcast over Point-to-Point (ATM PVC)-Medien zu replizieren.
- Bridging ist von Natur aus unsicher und erfordert eine vertrauenswürdige Umgebung.Die ARP-Antworten (Address Resolution Protocol) können gefälscht und eine Netzwerkadresse entführt werden. Zusätzlich können Broadcast-Angriffe im lokalen Subnetz initiiert werden, wodurch allen Mitgliedern des lokalen Subnetzes der Dienst verweigert wird.
- IP-Adressen-Hijacking ist möglich.

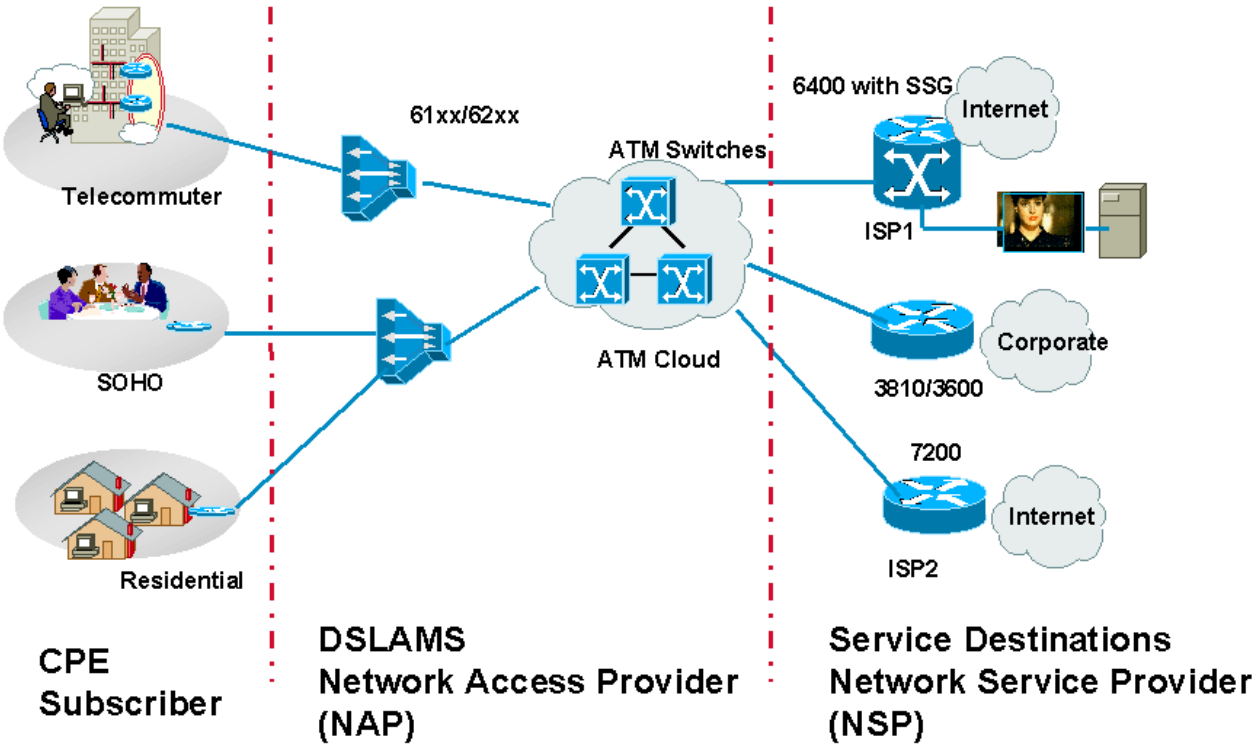
Überlegungen zur Implementierung

Vor der Implementierung der RFC1483-Bridging-Architektur sollten Sie folgende Fragen prüfen.

- Wie viele und wie viele Abonnenten sollen derzeit betreut werden?
- Müssen die Teilnehmer miteinander kommunizieren?
- Handelt es sich bei diesen Abonnenten um Privatkunden mit einem Benutzer? Bieten Sie Kunden für kleine Büros und Heimbüros (SOHO) an, die möglicherweise ein kleines LAN hinter den CPE haben?
- Wie werden CPEs, Digital Subscriber Line Access Multiplexer (DSLAMs) und Aggregation Post Office Protocols (POPs) bereitgestellt und bereitgestellt?
- Sind der Netzwerkzugriffs-Provider (NAP) und der Netzwerkdienstanbieter (NSP) dieselbe Einheit? Umfasst das Geschäftsmodell für den NAP auch den Verkauf von Großkundenservices wie sicheren Unternehmenszugang und Mehrwert-Services wie Sprache und Video?
- Möchte der NSP Funktionen zur Serviceauswahl anbieten?
- Wie können Rechnungsstellung und Rechnungsstellung umgesetzt werden? Handelt es sich dabei um die Nutzung, die Bandbreite oder den Service?
- Handelt es sich um das Geschäftsmodell eines unabhängigen lokalen Börsenbetreibers (ILEC), eines konkurrierenden lokalen Börsenbetreibers (CLEC) oder eines Internetdienstanbieters (ISP)?
- Welche Arten von Anwendungen möchte der NSP dem Endkunden anbieten?
- Wie hoch ist das Datenflussvolumen sowohl im Upstream als auch im Downstream?

Unter Berücksichtigung dieser Punkte wird im Folgenden beschrieben, wie die RFC1483-Bridging-Architektur auf unterschiedliche Geschäftsmodelle zugeschnitten und skaliert wird.

Netzwerkarchitektur



RFC1483-Bridging: Netzwerkarchitektur

Überlegungen zum Design

Wie bereits erwähnt, gibt es einige inhärente Probleme mit der RFC1483-Bridging-Architektur.

Die Bridging-Funktion für IOS-Teilnehmer behebt einige dieser Probleme. Die selektive Anwendung von Teilnehmerrichtlinien auf eine Bridge-Gruppe steuert die Überflutung von ARPs, unbekannten Paketen und anderen Geräten in jeder ADSL-Schleife. Wenn beispielsweise ARPs nicht gesendet werden können, kann ein feindlicher Benutzer die IP-Adresse eines anderen Benutzers nicht ermitteln.

Eine weitere Lösung besteht darin, alle Abonnenten in einer einzigen Subschnittstelle zu speichern. Das normale Bridging-Verhalten leitet Frames nicht an den Port weiter, an dem der Frame empfangen wurde. Im Wesentlichen erzwingt dies eine Art von Subscriber-Bridging, in der alle Pakete zwischen Subscribern gefiltert werden. Dieser Ansatz weist jedoch folgende Mängel auf:

- Die Teilnehmerrichtlinie wird nur auf Subschnittstellen angewendet. Zum Anwenden von Teilnehmerrichtlinien zwischen zwei verschiedenen Benutzern muss sich jeder Benutzer in einer anderen ATM-Subschnittstelle befinden.
- Da die Layer-2-zu-Layer-3-Adressenzuordnung (über ARP) erfasst wird, können feindliche Benutzer weiterhin die Verbindung anderer Benutzer übernehmen. Dies geschieht durch

Generieren von ARP-Datenverkehr mit der IP-Adresse eines anderen Benutzers und Verwendung einer anderen MAC-Adresse.

Das zweite Szenario ist für den Carrier oder ISP schwerwiegender. In dieser Situation kann jeder Benutzer einem PC oder einem Ethernet-angeschlossenen Gerät (z. B. einem Drucker) die falsche Adresse zuweisen und Verbindungsprobleme für einen anderen Benutzer verursachen. Solche Fehler oder Angriffe sind schwer zu identifizieren und zu korrigieren, da der Täter nur durch Rückverfolgung der MAC-Adresse des Täters verfolgt werden kann.

Einige Betreiber versuchen, dieses Problem zu umgehen, indem sie Benutzer über Bridge-Gruppen hinweg voneinander trennen und das Abonnenten-Bridging über Subschnittstellen hinweg implementieren. Wenn ein integriertes Routing und Bridging (IRB) erforderlich ist, wird jedem Benutzer eine eindeutige Bridge-Gruppe und eine Bridge Group Virtual Interface (BVI) zugewiesen. Dieser Ansatz verwendet zwei Schnittstellen pro Teilnehmer und kann daher eine Herausforderung darstellen.

Diese Probleme werden mithilfe der Funktion für die Routed Bridge Encapsulation (RBE) behoben, die in Cisco IOS® Software Release 12.0(5)DC auf dem Cisco 6400 eingeführt wurde.

Angesichts der Nachteile von Bridging fragen Sie sich vielleicht, warum die Bridging-Architektur jemals implementiert würde. Die Antwort ist einfach. Die meisten im Feld installierten ADSL-CPEs können lediglich überbrückte Frames weiterleiten. In diesen Fällen muss der NSP Bridging implementieren.

Heute können CPEs Point-to-Point Protocol over ATM (PPPoA), RFC1483-Bridging und RFC1483-Routing verwenden. Der NSP bestimmt, ob Bridging oder PPP ausgeführt werden soll. Die Entscheidung basiert neben den Vor- und Nachteilen der einzelnen Architekturen auf den zuvor erwähnten Implementierungsüberlegungen.

Selbst mit den Nachteilen der Bridging-Architektur kann sie für einen kleinen ISP (der nicht der NAP sein darf) oder einen NAP/NSP geeignet sein, der eine kleinere Anzahl von Abonnenten bedient. In diesen Szenarien leitet das NAP normalerweise den gesamten Teilnehmerverkehr an den ISP/NSP weiter, der diese Teilnehmer terminiert. Das NAP kann wahlweise mithilfe von ATM oder Frame Relay als Layer-2-Protokoll Teilnehmerverkehr bereitstellen.

NAPs, die DSLAMs der aktuellen Generation verwenden, können nur den Teilnehmerverkehr mithilfe von ATMs übertragen. In diesem Fall sollte der ISP permanente ATM Virtual Circuits (PVCs) an einen Router anschließen.

Verfügt der ISP/NSP nicht über die ATM-Schnittstelle, kann eine reguläre serielle Schnittstelle mit KapselungsATM Data Exchange Interface (DXI) (möglicherweise auf einem zusätzlichen Gerät) verwendet werden, um die eingehenden überbrückten PDUs zu akzeptieren.

In beiden Szenarien muss der NSP/ISP möglicherweise IRB auf dem Router konfigurieren (außer bei Verwendung der Kapselung von ATM DXI oder bei transparentem Bridging). Die gängigste Praxis für das Terminieren überbrückter Abonnenten auf dem NSP/ISP-Router besteht heute in der Implementierung von IRB. (Es wird erwartet, dass Service Provider nach und nach zu RBE migrieren.)

Aufgrund einiger der oben genannten Einschränkungen kann der NSP/ISP separate Bridge-Gruppen für jede Gruppe von Abonnenten konfigurieren oder alle Abonnenten in einer Bridge-Gruppe konfigurieren. Die gängige Praxis besteht darin, einige Bridge-Gruppen zu konfigurieren und dann alle Teilnehmer über separate Multipoint-Schnittstellen zu konfigurieren. Wie bereits erwähnt, können die Teilnehmer unter derselben Multipoint-Schnittstelle möglicherweise nicht

miteinander kommunizieren. Wenn bestimmte Benutzer miteinander kommunizieren müssen, konfigurieren Sie diese Teilnehmer unter verschiedenen Schnittstellen (sie können sich immer noch in derselben Bridge-Gruppe befinden).

Für einen kleinen ISP/NSP werden die Cisco Router 3810, Cisco 3600 und Cisco 7200 am häufigsten zum Terminieren überbrückter Teilnehmer verwendet. Für ISPs/NSPs mit einem großen Teilnehmerstamm wird der Cisco 6400 bevorzugt. Berücksichtigen Sie vor der Berechnung der Speicheranforderungen für diese Router dieselben Faktoren wie für jede andere Umgebung: Anzahl der Benutzer, Bandbreite und Router-Ressourcen.

Die wichtigsten Punkte dieser Architektur

Im Folgenden sind die wichtigsten Punkte der Architektur aufgeführt.

CPE

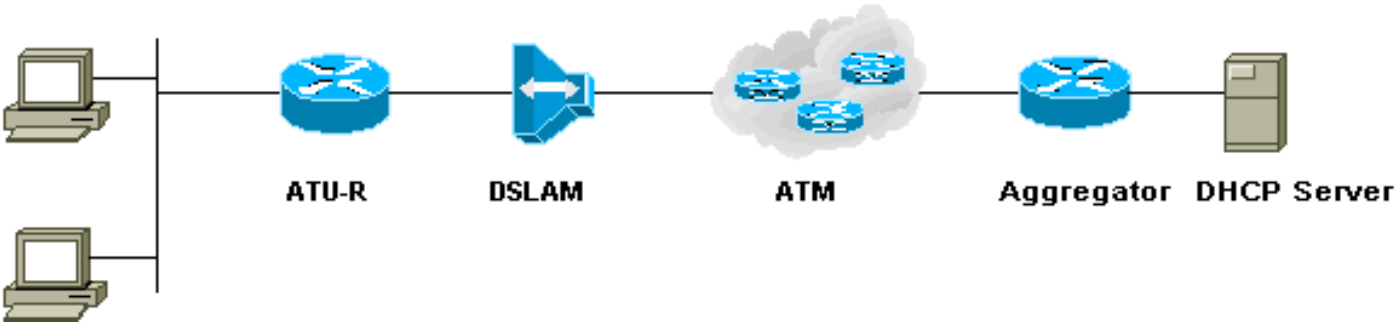
Cisco bietet verschiedene CPEs an, die mit DSLAMs von Cisco und anderen Anbietern arbeiten. Die Konfiguration für jedes dieser CPEs ist problemfrei und erfordert keine Eingaben des Teilnehmers. Die primäre Anforderung besteht darin, dass CPE eine ATM Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) definiert. Dadurch kann das CPE mit dem DSLAM fortfahren und mit der Weiterleitung des Datenverkehrs beginnen. In den meisten Fällen kann das NAP dasselbe VPI/VCI für alle Teilnehmer konfigurieren. Der NAP stellt die CPE in der Regel vor, bevor sie am Standort des Abonnenten bereitgestellt wird.

Bei der Bridging-Architektur ist die wichtigste Überlegung für das CPE und seine Bereitstellung, wie das NAP das CPE nach seiner Installation vor Ort verwaltet. Dies ist problematisch, da für das Bridging keine IP-Adresse für das CPE erforderlich ist. Cisco CPEs können jedoch im Bridging-Modus eine IP-Adresse zugewiesen werden. Der NAP kann diese Funktion für Telnet zu CPE verwenden, um Statistiken zu sammeln oder den Abonnenten bei der Fehlerbehebung zu unterstützen. Damit CPEs über die DSLAMs verwaltet werden können, wird eine neue Proxy-Elementfunktionalität hinzugefügt.

Wenn dem CPE im Bridging-Modus keine Management-IP-Adresse zugewiesen ist, kann der Operator das CPE nur über den CPE-Management-Port verwalten. Wenn eine Management-IP-Adresse zugewiesen ist, kann der Operator das Gerät über einen HTTP-Browser (Hypertext Transfer Protocol) verwalten. Diese Option ist jedoch im Allgemeinen nicht verfügbar.

Wenn sich das CPE im Bridging-Modus befindet, sollte das Service-Ziel (das der NSP/ISP sein könnte) eine IP-Adresse bereitstellen, die als Standard-Gateway für die PCs hinter dem CPE verwendet wird. Diese PCs müssen auf das richtige Standard-Gateway eingestellt sein. Andernfalls kann der Teilnehmer den Datenverkehr möglicherweise nicht weiterleiten, selbst wenn das Modem geschult wurde (d. h. die physische Schicht zwischen CPE und DSLAM gut ist). Dies ist kein Problem, wenn das Dynamic Host Configuration Protocol (DHCP) verwendet wird, um DHCP-Adressen für Teilnehmer zuzuweisen, da der Standard-Router vom DHCP-Server zurückgegeben wird.

IP-Management



RFC1483-Bridging: IP-Management

In einer überbrückten Umgebung werden die IP-Adressen den Endstationen von einem DHCP-Server zugewiesen, der sich am Dienstziel befindet, normalerweise im NSP/ISP-Netzwerk. Dies ist der gängigste Ansatz und wird von den meisten NSPs/ISPs implementiert, die dieses Modell verwenden.

Ein weiterer Ansatz besteht darin, den Abonnenten statische IP-Adressen zur Verfügung zu stellen. In diesem Fall wird je nach Teilnehmeranforderungen entweder ein Subnetz mit IP-Adressen oder eine einzelne IP-Adresse pro Teilnehmer zugewiesen. Abonnenten, die einen Webserver oder einen E-Mail-Server hosten möchten, benötigen beispielsweise statt einer einzigen IP-Adresse einen Satz von IP-Adressen. Das Problem dabei ist, dass der NSP/ISP öffentliche IP-Adressen bereitstellen muss und diese schnell nicht mehr zur Verfügung stehen.

Einige NSP/ISPs haben ihren Abonnenten private IP-Adressen bereitgestellt. Anschließend führen sie Network Address Translation (NAT) am Service-Ziel-Router aus.

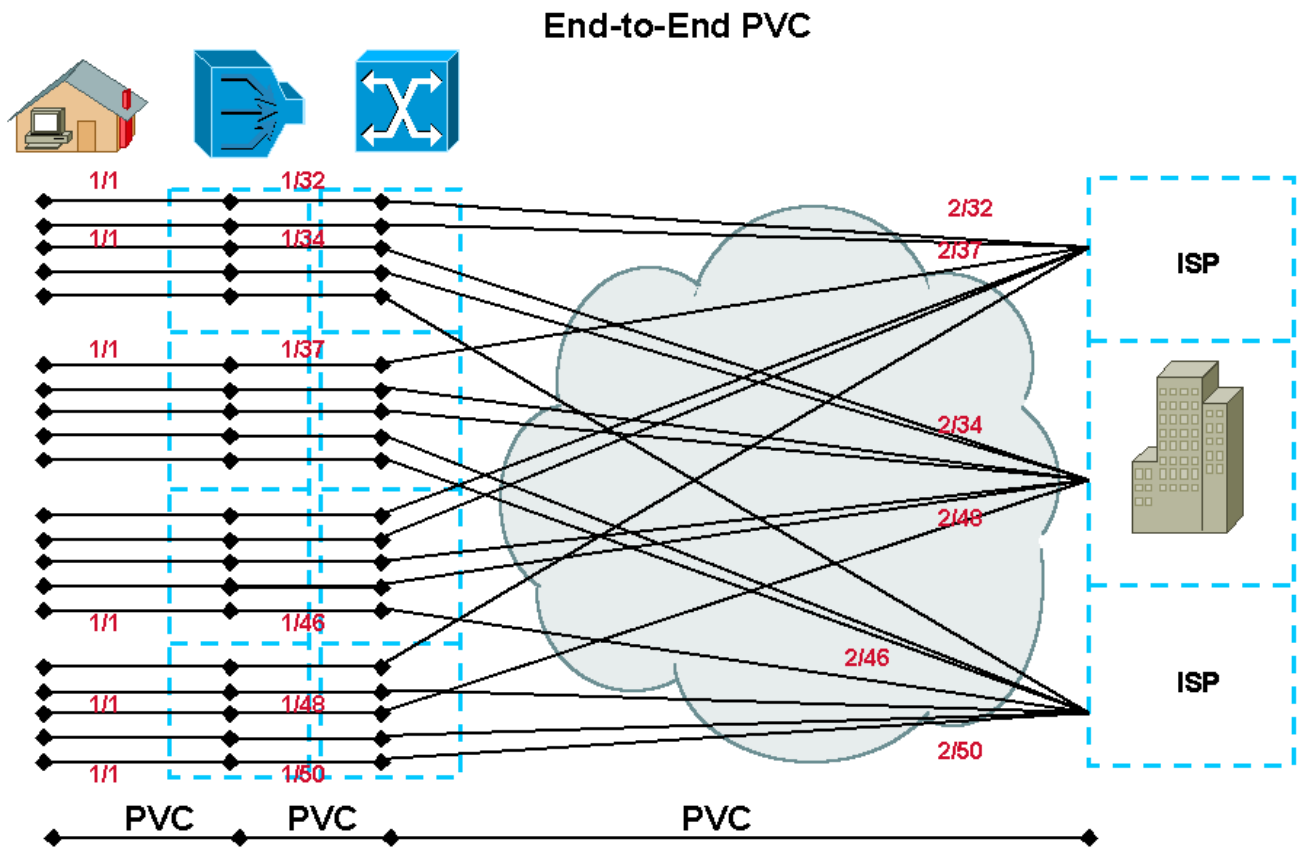
NSPs/ISPs, die ein vollständiges Subnetz für eine Bridge-Gruppe (mit mehr als einem Subscriber) bereitstellen, sollten wissen, dass ein Benutzer einem PC oder einem Ethernet-angeschlossenen Gerät (z. B. einem Drucker) die falsche Adresse zuweisen und Verbindungsprobleme für einen anderen Benutzer verursachen kann.

Ein NSP/ISP kann auch die Anzahl der PCs einschränken, die gleichzeitig auf den Service zugreifen können. Dies erfolgt durch die Konfiguration der maximalen Benutzer auf der Ethernet-Schnittstelle.

Diese Methode hat jedoch den folgenden Fehler. Wenn drei PCs für die Nutzung des Dienstes konfiguriert sind und einer der Teilnehmer einen Netzwerkdrucker (der über eine eigene MAC-Adresse verfügt) hinzufügt, wenn einer der PCs inaktiv ist, wird die MAC-Adresse des PCs aus dem ARP-Eintrag des CPE entfernt.

Wenn der Drucker aktiv wird, während sich ein PC im Leerlauf befindet, wird die MAC-Adresse des Druckers im ARP-Eintrag eingegeben. Wenn ein Benutzer beschließt, diesen PC für den Zugriff auf das Internet zu verwenden, ist er nicht verfügbar, da CPE bereits drei MAC-Einträge zugelassen hat. Die Strategie, die Nutzer auf CPE zu beschränken, kann genutzt werden, aber bei der Festlegung der Zahlen ist Vorsicht geboten.

Erreichen eines Serviceziels



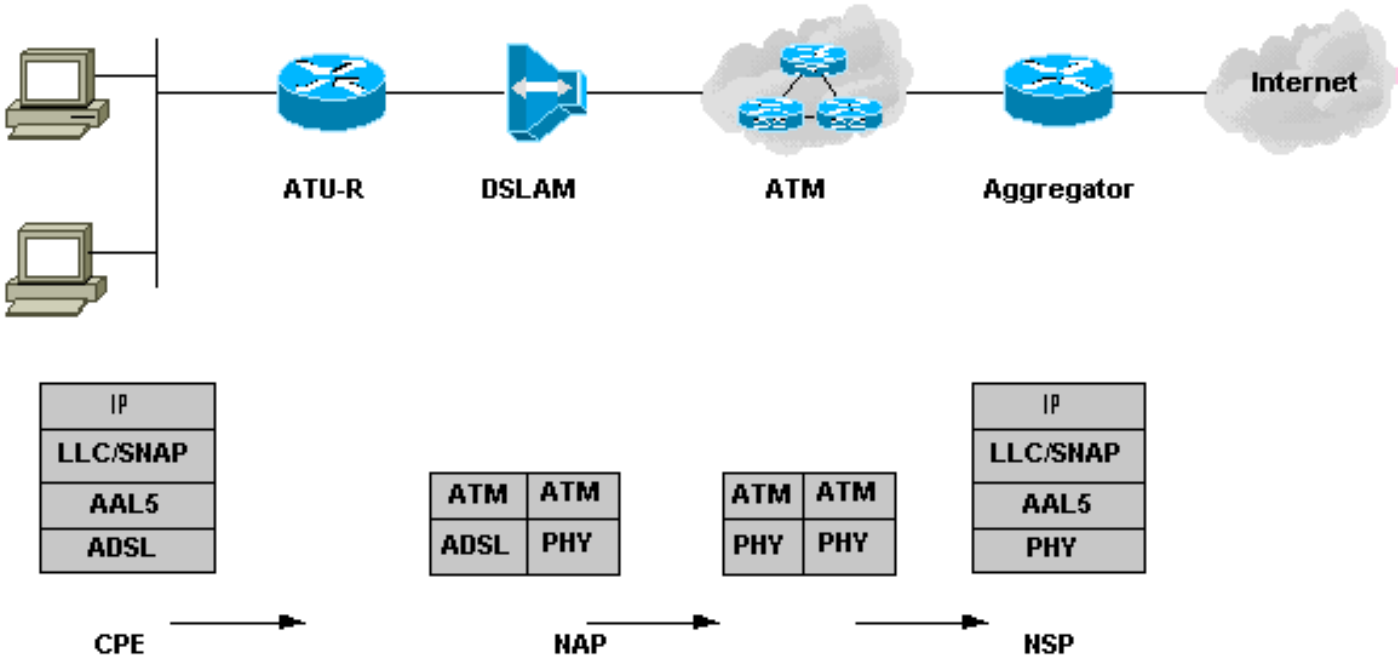
RFC1483-Bridging: End-to-End-PVC

In einer End-to-End-PVC-Architektur mit Bridging wird das Serviceziel durch die Erstellung von PVCs zwischen den einzelnen Hops erreicht. Die Verwaltung dieser PVCs kann für das NAP/NSP jedoch eine Herausforderung darstellen. Darüber hinaus ist die Anzahl der PVCs, die über die ATM-Cloud definiert werden können, begrenzt. Diese Einschränkung betrifft viele NAPs/NSPs, die ein End-to-End-PVC-Modell einsetzen. Jeder Abonnent erhält über den gesamten Pfad einen festen, eindeutigen Satz von VPIs/VCIs. Switched Virtual Circuits (SVCs) helfen dabei, einige dieser Probleme zu überwinden. Viele Access Provider migrieren zu IP-fähigen Kernnetzwerken, um das Problem der VC-Erschöpfung zu lösen.

Der NSP/ISP kann darüber hinaus die Cisco Service Selection Gateway (SSG)-Funktion verwenden, um Abonnenten unterschiedliche Services bereitzustellen.

In dieser Architektur wird der sichere Zugriff auf ein Corporate Gateway durch Abschließen des Teilnehmer-Datenverkehrs-PVC direkt im Corporate Router auf Layer 2 erreicht. Die PVC-basierten Architekturen sind bei der Datenfreigabe mit anderen Servicezielen von Natur aus sicher.

Betriebsbeschreibung



RFC1483-Bridging: Betriebsbeschreibung

Der Cisco 6xx CPE verwendet standardmäßig den Routing-Modus. Wenn es für den Bridging-Modus konfiguriert und am Standort des Teilnehmers mit den erforderlichen Splittern/Mikrofiltern installiert wird, wird die Verbindung daher beim Einschalten automatisch aufgebaut. Wenn die CPE hochfährt, weist dies darauf hin, dass die physische Schicht zwischen CPE und DSLAM in Ordnung ist. Je nachdem, wie die IP-Adresse der Endstation konfiguriert wird (d. h. ob sie über einen DHCP-Server zugewiesen wird oder es sich um eine statische IP-Adresse mit Standard-Gateway-Informationen handelt), kann sie dann mit dem Serviceziel kommunizieren.

Im Folgenden wird der Paketfluss beschrieben.

Die Daten des Benutzers werden vom PC in IEEE 802.3 eingekapselt und gelangen in das Cisco 6xx CPE. Anschließend wird sie in einen LLC/SNAP-Header (Logical Link Control/Subnetwork Access Protocol) gekapselt, der wiederum in ATM Adaption Layer 5 (AAL5) eingekapselt und an die ATM-Ebene übergeben wird.

Die ATM-Zellen werden dann durch die ADSL-Übertragungstechnologie, die Carrierless Amplitude and Phase (CAP) Modulation oder die Diskrete Multi-Tone (DMT) moduliert und über das Kabel an die DSLAM gesendet. Beim DSLAM werden diese modulierten Signale zuerst vom POTS Splitter empfangen, der prüft, ob die Frequenz des Signals unter oder über 4 kHz liegt. Nachdem die Signale über 4 kHz identifiziert wurden, werden sie an die ADSL Transmission Unit - Central Office (ATU-C) im DSLAM weitergeleitet.

Die ATU-C demoduliert das Signal und ruft die ATM-Zellen ab, die dann an die Netzwerkschnittstellenkarte (NIC) im Multiplexing-Gerät (MUX) übergeben werden. Die NIC überprüft die VPI/VCI-Informationen auf der Subscriber-Seite im ATM-Header und trifft die Switching-Entscheidung für ein anderes VPI/VCI, das an den Service-Ziel-Router weitergeleitet wird. Wenn der Service-Ziel-Router diese Zellen an einer bestimmten ATM-Schnittstelle empfängt, setzt er sie neu zusammen, prüft die obere Ebene und leitet die Informationen an die BVI-Schnittstelle weiter. Die BVI-Schnittstelle überprüft die Layer-3-Informationen und entscheidet, wo das Paket zugestellt werden soll.

Schlussfolgerung

Das RFC1483-Bridging-Modell eignet sich besser für kleinere ISPs oder den Unternehmenszugriff, für die Skalierbarkeit kein Problem darstellt. Da es sehr einfach zu verstehen und zu implementieren ist, ist es inzwischen die Wahl vieler kleinerer ISPs. Aufgrund einiger Sicherheits- und Skalierbarkeitsprobleme verliert die Bridging-Architektur jedoch ihre Beliebtheit. NSPs/ISPs entscheiden sich für RBE oder streben PPPoA oder PPPoE an, die hochgradig skalierbar und sehr sicher, aber komplexer und schwieriger zu implementieren sind.

Zugehörige Informationen

- Technischer DSL-Support
- Technischer Support - Cisco Systems