



LSN 环境下政企用户 PPPoE 上网实现方案

颜永明, 叶克闯, 许斌, 徐海峰, 左良, 洪恺渊
(中国电信股份有限公司上海分公司, 上海 200085)

摘 要: 随着云计算市场的井喷式发展, 园区创客企业在云业务方面的需求不断增加。针对资费敏感的用户, 在 LSN 环境下采用传统政企 PPPoE 方式, 可在减少公网 IPv4 地址大量消耗的同时, 为用户提供云化的 ICT 服务。将传统的 PPPoE 拨号政企网关与最新 LSN 场景相结合, 提出了几套解决方案, 对各自的优缺点加以比较, 对 LSN 环境下实现政企用户拨号上网给出了建议。

关键词: LSN; PPPoE; 云业务; ICT

中图分类号: TN919

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017263

PPPoE internet access for government-enterprise customer in LSN environment

YAN Yongming, YE Kechuang, XU Bin, XU Haifeng, ZUO Liang, HONG Kaiyuan
Shanghai Branch of China Telecom Co., Ltd., Shanghai 200085, China

Abstract: With the blowout development of cloud-computing market, start-up enterprises gradually increase the demand for cloud business. For the cost-sensitive customers, using the traditional government-enterprise PPPoE in the LSN environment could reduce the wastage of public IPv4 addresses. Meanwhile, ICT services based on cloud-computing was provided for customers. Several solutions which mixed the traditional government-enterprise gateway solution and the latest LSN scene were presented. Through the analysis of advantages and disadvantages of each scheme, reference for government-enterprise customers dialing-up to access internet in LSN environment was presented.

Key words: local service node, point to point protocol over Ethernet, cloud business, information and communication technology

1 引言

随着 SDN (software defined networking, 软件定义网络) 技术的快速发展, 中国电信股份有限公司上海分公司 (以下简称中国电信上海分公司) 构建了 LSN (local service node, 区域综合信息服

务点) ——一种电信运营商基于云计算的新型的 ICT (information and communication technology, 信息和通信技术) 服务技术架构。这种技术架构充分利用了现有电信运营商的端局机房资源及光纤宽带接入网络, 将其重新构建成基于云计算、NFV (network function virtualization, 网络功能虚



拟化)、SDN 的多租户云数据中心,通过大二层网络技术将 LSN 数据中心、电信运营商光纤接入汇聚网络、CPN (customer premises network, 用户驻地网) 有机融合成承载综合 ICT 服务的网络基础设施架构。

如何在 LSN 环境下利用传统政企网关实现 PPPoE 拨号政企用户上网业务,在减少虚拟化后公网/私网 IPv4 地址大量消耗的同时,满足用户云业务方面的 ICT 需求,是本文研究的重点。

2 LSN 环境下政企网关拨号上网业务场景需求和问题

2.1 LSN 网络架构

如图 1 所示,中国电信上海分公司构建的 LSN 网络主要由 2 台 MSE 和一组 spine-leaf 架构组成。其中, MSE 是具有多业务接入能力的路由器,作为东西向、南北向流量的出口。spine-leaf 架构则由两台 spine 交换机组成交换机矩阵核心,若干台 leaf 节点作为交换机矩阵接入, leaf 从功能上又分为 Bleaf (border leaf, 边缘交换机) 和 Ileaf (internal leaf, 内部交换机)。Bleaf 主要连接出局链路,承载了去往公网、用户 CPN 侧的流量。Ileaf 主要连接局内链路,沟通网络资源、服务器资源、存储资源,承载了局内用户 vDC 中的流量和虚拟化平台的相关流量。同时, spine-leaf 架构中运用 VxLAN 技术部署大二层网络,能够适应虚拟机数量爆发式的增长。

2.2 LSN 环境下政企网关拨号上网的业务场景需求

创客园区、办公楼类租户大多倾向于轻资产运营,因此,更愿意租用运营商的云资源、网络设备构建自己的办公和业务环境,而这些用户对资费又较敏感,上网带宽需求一般不高。据此,电信业务部门提出了在 LSN 环境下提供政企宽带拨号上网业务,即用户通过 PON (passive optical network, 无源光纤网络) 线路连接 LSN 的

spine-leaf 网络,既能访问位于 LSN 内的 vDC 资源,又可以通过政企宽带链路使用 PPPoE 拨号满足 CPN 侧的上网需求,如图 1 所示。

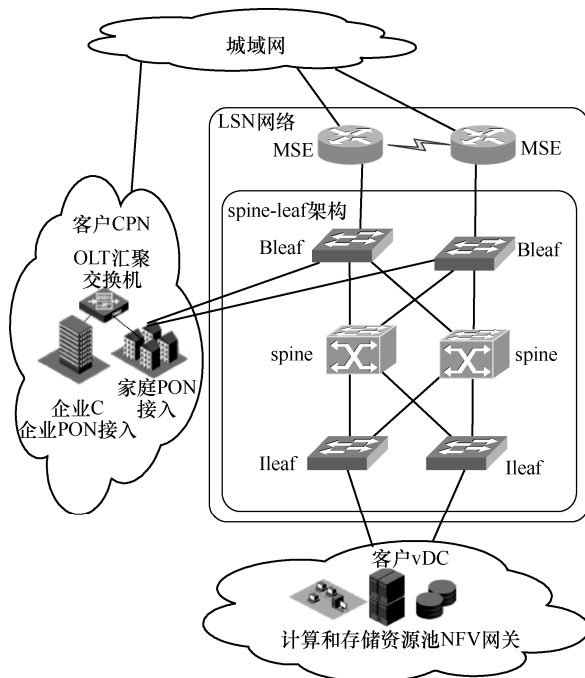


图 1 用户 CPN 通过 PON 线路接入 LSN

其中,政企用户 PON 线路直连 OLT 设备,上联至 spine-leaf 架构中的 Bleaf。Ileaf 负责接入用户 vDC 资源。spine 负责对业务流量进行交换。整个 spine-leaf 架构采用 VxLAN 技术实现二层网络的连通。MSE 则可以作为网络资源的三层出口接入城域网。

对于使用 LSN 业务的政企用户而言,期望在不改变原有使用习惯、继续沿用传统的政企宽带拨号方式的情况下同时享有传统宽带业务和 LSN 服务,即申请一根 PON 线路,通过政企网关设备,可同时实现 Internet 上网以及访问 vDC 内资源。为了和 EIP 有所区分,实现业务差异化,运营商业务部门希望为创客园区、办公楼类租户提供非固定 IP 地址的接入方式,实现政企用户拨号上网业务,从而达到降低资费的目的。同时,为了满足信息安全中溯源的要求,需要对每个用户使用的 IP 地址进行记录。

3 传统政企宽带上网实现

传统政企上网方式主要有宽带拨号上网和EIP两大类。宽带拨号上网业务通常采用PPPoE技术,IP地址动态分配。EIP则采用固定公网IP地址方式。

由于采用了PON线路,传统PPPoE宽带拨号方式在可控性和性价比方面具有明显优势。PPPoE客户端功能可由用户侧政企网关设备提供,服务器端则由运营商局端MSE设备实现,用户使用用户名和密码从用户侧政企网关向MSE发起PPPoE拨号,认证通过后,局端MSE根据AAA系统下发的参数为用户WAN口动态分配公网IPv4地址,同时,用户侧内网可使用私有IPv4地址,经过NAT(network address translation,网络地址转换)或PAT(port address translation,网络地址转换)后访问Internet。由于IP地址动态分配,此方式通常用于用户上网访问,一般不提供Internet内容发布。

EIP则为用户提供固定分配的公网IP地址,

运营商对用户接入地址可实现强管控。使用固定公网地址,用户既能实现上网访问,也可利用固定IP地址对外发布应用,拥有内容发布的能力。因为每个用户都有独立的公网IP地址,IP地址的消耗会随着用户数量的增加急速增加。

4 LSN环境下政企网关PPPoE实现方案

4.1 方案1

方案1为用户CPN侧各VLAN网关部署在PON线路政企网关设备上,基础配置以图2为例,CPN配置3个内网VLAN,分别是VLAN2、VLAN3、VLAN4,不同VLAN内的终端可访问LSN内对应的内网应用,例如生产、办公、测试类应用,这3个VLAN在政企网关上可通过配置接入口实现。另外,配置一个PPPoE拨号接口,归属于VLAN1,用于发起PPPoE拨号,将政企网关的WAN口配置成Hybrid模式,其中,VLAN1不打标签,VLAN2、VLAN3、VLAN4则加上IEEE 802.1q封装后发送,政企网关上行端口通过PON线路连接到OLT汇聚交换机,由OLT汇聚交换机

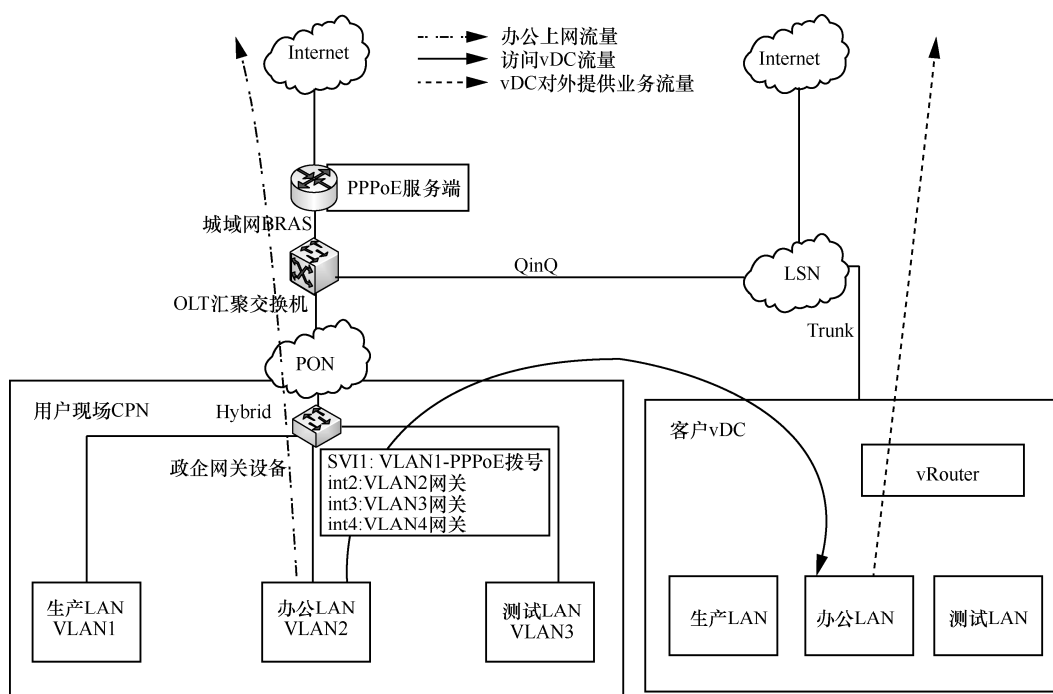


图2 方案1基础配置



作为业务分离点，分别与城域网 BRAS（实现 Internet 上网）和 LSN 网络（各 VLAN 与用户 vDC 内对应应用实现互联，从而实现 CPN 对用户 vDC 内资源的访问）连接。

本方案的特别配置在于 PPPoE 拨号和用户 CPN 侧 VLAN 网关都由政企网关设备实现，且上网流量通过城域网 BRAS 访问 Internet。具体来说，在政企网关设备上开启 4 个 SVI 接口，各个接口的作用如下：SVI 1，VLAN 1 PPPoE 拨号；SVI 2，VLAN 2 网关；SVI 3，VLAN 3 网关；SVI 4，VLAN 4 网关。上网 PPPoE 拨号由政企网关发起，由城域网 BRAS 终结。用户 CPN 内各 VLAN 终端若要上网，将政企网关内各自对应的 SVI 接口作为三层网关接口，直接走下一跳，指向 PPPoE 拨号接口所在 SVI 的默认路由。如要实现各 VLAN 之间流量的三层隔离，可在政企网关上配置 ACL 策略以增强安全性。

关键配置举例如下。

（1）SVI1

VLAN1-PPPoE 拨号，获得 IP 地址是 101.80.1.100/24。PPPoE 服务器端 IP 地址是 101.80.1.1/24。政企网关设备默认路由是 IP route 0.0.0.0 0.0.0.0 101.80.1.1，且配置 NAT 以 101.80.1.100 访问外网。

（2）SVI2

用户生产 LAN，配置为 VLAN2，对应 CPN 及 vDC 使用网段 192.168.2.2-254，在政企网关设备上配置 VLAN2 网关地址：192.168.2.1/24。

（3）SVI3

用户办公 LAN，配置为 VLAN3，对应 CPN 及 vDC 使用网段 192.168.3.2-254，在政企网关设备上配置 VLAN3 网关地址：192.168.3.1/24。

（4）SVI4

用户测试 LAN，配置为 VLAN4，对应 CPN 及 vDC 使用网段 192.168.4.2-254，在政企网关设备上配置 VLAN4 网关地址：192.168.4.1/24。

用户流量走向举例如下。

- CPN 办公上网流量在政企网关设备上走默认路由，经过 PAT 成 SVI 1 的公网地址后，直接从 OLT 汇聚交换机流出，经过城域网 BRAS 访问 Internet。
- CPN 访问 vDC 的流量经过政企网关设备后，以 QinQ 封装形式流向 OLT 汇聚交换机，到达 LSN 节点的 Bleaf 后转换成 VxLAN 封装，流经 spine-leaf 网络至 LSN 节点的 Ileaf 后再转成 VLAN 到达用户 vDC 内。用户 vDC 内资源与 CPN 是二层互联，以生产 VLAN 为例，与 VLAN2 二层互通，两者在同一个广播域中，VLAN 2 内终端可直接通过二层交换方式访问生产 LAN 内资源。
- 流量从生产 LAN、办公 LAN 或者测试 LAN 发起，三层网关终结于 vRouter 上，通过 NAT 1:1 转换成公网地址后，经由 LSN 网络流向 Internet。

4.2 方案 2

方案 2 为用户 CPN 侧各 VLAN 网关部署在 LSN vRouter 上，基础配置如图 3 所示。CPN 配置 3 个内网 VLAN，分别是 VLAN 2、VLAN 3、VLAN 4，不同 VLAN 内的终端可访问 LSN 内对应的内网应用，例如生产、办公、测试类应用，这 3 个 VLAN 在政企网关上可通过配置接入口实现。配置一个 PPPoE 拨号接口，归属于 VLAN 1，用于发起 PPPoE 拨号。在政企网关和 LSN 的 vRouter 上分别配置一个 VLAN 5 接口，用于政企网关与 vRouter 之间实现三层互连。将政企网关的 WAN 口配置成 Hybrid 模式，其中，VLAN 1 不打标签，VLAN 2、VLAN 3、VLAN 4、VLAN 5 则加上 IEEE 802.1q 封装后发送，政企网关上行端口通过 PON 线路连接到 OLT 汇聚交换机，由 OLT 汇聚交换机作为业务分离点，分别与城域网 BRAS（实现 Internet 上网）和 LSN 网络（各 VLAN 与

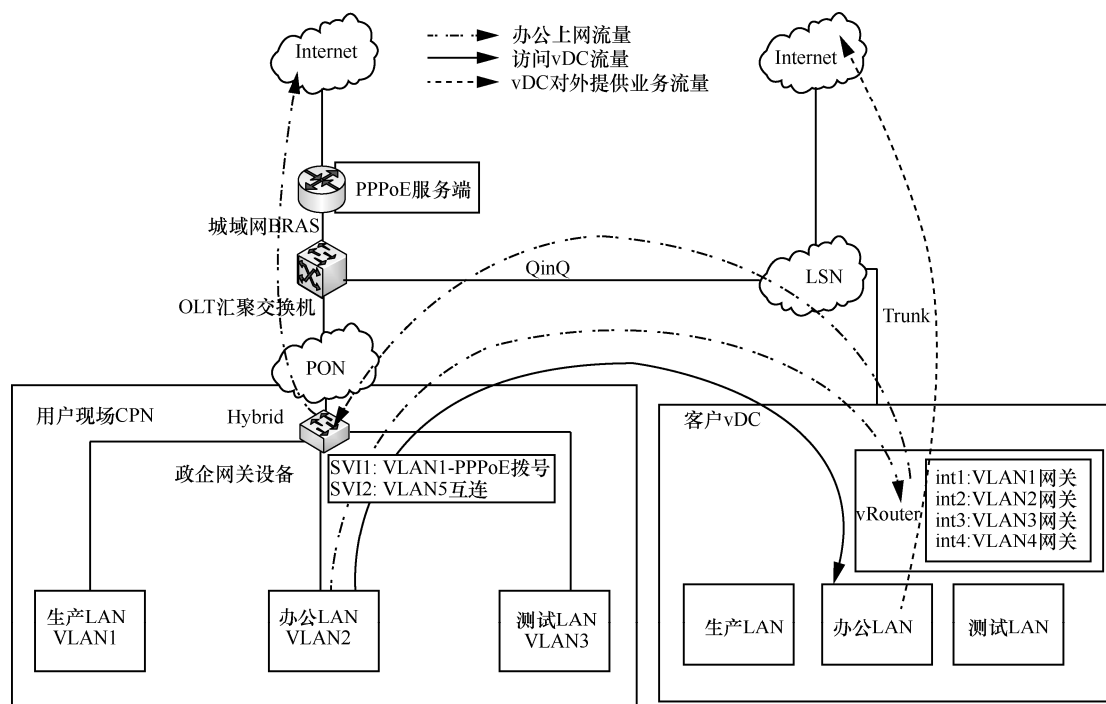


图3 方案2基础配置

用户 vDC 内对应应用实现互联，从而实现 CPN 对用户 vDC 内资源的访问）连接。

本方案配置的特别之处在于，虽然 PPPoE 拨号仍由 PON 线路政企网关设备发起，上网流量仍是通过城域网 BRAS 访问 Internet，但是用户 CPN 侧各内网 VLAN 的三层网关均设置在 LSN 节点的 vRouter 上。具体来说，在政企网关设备上配置 2 个 SVI，其中，SVI1 归属于 VLAN 1，用作 PPPoE 拨号使用；SVI2 归属于 VLAN5，用于与 LSN 内 vRouter 三层互连。在 vRouter 上开启 4 个接口，分别作为政企网关上 SVI2 接口的互联地址以及 VLAN 2、VLAN 3、VLAN 4 的三层网关。如要实现各 VLAN 之间流量三层隔离，可在 LSN 内 vRouter 上配置 ACL 策略以增强安全性。

关键配置举例如下。

(1) vRouter int1

用户生产 LAN，配置为 VLAN2，对应 CPN 及 vDC 使用网段 192.168.2.2-254，在 vRouter 上

配置 VLAN2 网关地址：192.168.2.1/24。

(2) vRouter int2

用户办公 LAN，配置为 VLAN3，对应 CPN 及 vDC 使用网段 192.168.3.2-254，在 vRouter 上配置 VLAN3 网关地址：192.168.3.1/24。

(3) vRouter int3

用户测试 LAN，配置为 VLAN4，对应 CPN 及 vDC 使用网段 192.168.4.2-254，在 vRouter 上配置 VLAN4 网关地址：192.168.4.1/24。

(4) vRouter int4

用户互联 LAN，配置为 VLAN5，在 int4 上配置 VLAN5 互联接口地址：192.168.5.1/30。int4 作为与政企网关设备的互联接口，配置默认路由 IP route 0.0.0.0 0.0.0.0 192.168.5.2，将上网流量转发至政企网关设备。

(5) 政企网关设备 SVI1

VLAN1-PPPoE 拨号，获得 IP 地址是 101.80.1.100/24。PPPoE 服务器端 IP 地址是 101.80.1.1/24。政企网关设备默认路由是 IP route



0.0.0.0 0.0.0.0 101.80.1.1，且配置 NAT 以 101.80.1.100 访问外网。

(6) 政企网关设备 SVI2

用户互联 VLAN，配置为 VLAN5，在 SVI2 上配置 VLAN5 互联接口地址：192.168.5.2/30，SVI2 作为与 vRouter int4 的互联接口，配置路由 IP route 192.168.2.0 255.255.255.0 192.168.5.1、IP route 192.168.3.0 255.255.255.0 192.168.5.1、IP route 192.168.4.0 255.255.255.0 192.168.5.1。

用户流量走向举例如下。

- 以办公 VLAN 3 为例，CPN 办公上网流量依次经过政企网关设备、OLT 汇聚交换机、LSN 网络，通过二层通道到达 vRouter 后，由 vRouter 作为 VLAN 3 三层网关，并通过 vRouter 上的默认路由（下一跳出接口为 int4，下一跳地址为政企网关上的 SVI2 地址）折返经过 LSN 网络、OLT 汇聚交换机到达政企网关设备，并根据政企网关上的默认路由流向 SVI1 PPPoE 接口，通过 PAT 成为公网 IP 地址后，接着从 OLT 汇聚交

机流出，经过城域网 BRAS 访问 Internet。这种方式下的 CPN 办公上网流量存在折返现象。

- CPN 访问 vDC 流量与方案 1 相同。
- vDC 对外提供业务流量与方案 1 相同。

4.3 方案 3

方案 3 为在 vRouter 上实现上网 PPPoE 拨号，基础配置如图 4 所示，CPN 使用 3 个 VLAN，分别为 VLAN 2、VLAN 3、VLAN 4。这 3 个 VLAN 均由 PON 线路政企网关设备负责接入（接口采用 access 模式），政企网关作为三层交换机使用，流量从政企网关 WAN 口发出时采用 IEEE 802.1q 封装，再通过 PON 以 QinQ 封装发送到 OLT 汇聚交换机，然后通过 OLT 汇聚交换机与 LSN 连接。LSN 再与用户 vDC 实现互联，使 CPN 可以访问用户 vDC 内资源。

本方案的特点是 PPPoE 拨号和用户 CPN 侧 VLAN 网关均在 vRouter 上，虽然上网流量仍是通过城域网 BRAS 访问 Internet，但在 LSN 的 vRouter 上开启 4 个接口，分别用作 PPPoE 拨号和 3 个

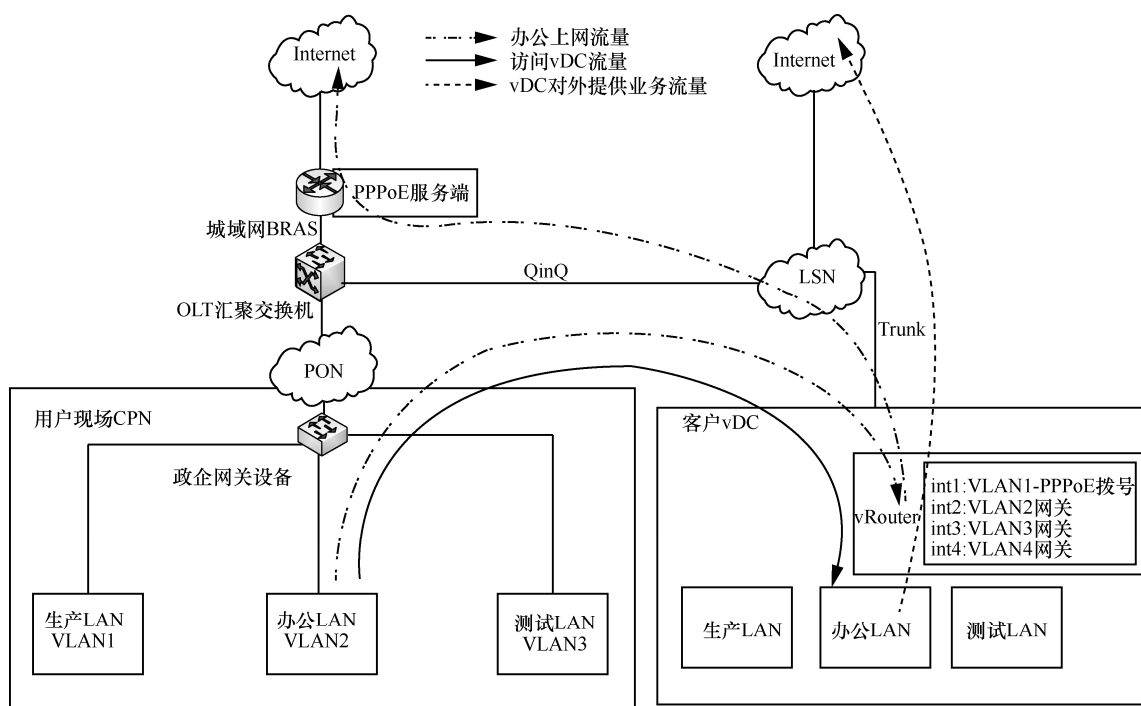


图 4 方案 3 基础配置

VLAN 的网关。

由于目前 LSN 网络与 BRAS 没有直接连通,故只能复用 LSN 网络到 OLT 汇聚交换机之间的链路作为 PPPoE 拨号链路。

关键配置举例如下。

(1) vRouter int1

VLAN1-PPPoE 拨号,获得 IP 地址是 101.80.1.100/24。PPPoE 服务器端 IP 地址是 101.80.1.1/24。政企网关设备默认路由是 IP route 0.0.0.0 0.0.0.0 101.80.1.1,且配置 NAT 以 101.80.1.100 访问外网。

(2) vRouter int2

用户生产 LAN,配置为 VLAN2,对应 CPN 及 vDC 使用网段为 192.168.2.2-254,在 vRouter 上配置 VLAN2 网关地址:192.168.2.1/24。

(3) vRouter int3

用户办公 LAN,配置为 VLAN3,对应 CPN 及 vDC 使用网段为 192.168.3.2-254,在 vRouter 上配置 VLAN3 网关地址:192.168.3.1/24。

(4) vRouter int4

用户测试 LAN,配置为 VLAN3,对应 CPN

及 vDC 使用网段为 192.168.4.2-254,在 vRouter 上配置 VLAN3 网关地址:192.168.4.1/24。

用户流量走向举例如下。

- CPN 办公上网流量依次经过政企网关设备、OLT 汇聚交换机、LSN 网络设备组成的二层通道到达 vRouter,并将 vRouter 作为三层网关,配置 vRouter 完成 PPPoE 拨号后,生成一跳为城域网 BRAS 的默认路由,流量在 vRouter 上通过网络地址转换成公网 IP 地址后,再依次经过 LSN、OLT 汇聚交换机、城域网 BRAS 访问 Internet。
- CPN 访问 vDC 流量与方案 1 相同。
- vDC 对外提供业务流量与方案 1 相同。

5 方案比较

上述 3 种方案之间可能存在一定共性,但是又各有优缺点,详细情况见表 1。

考虑到现网兼容性、网络结构、运维体系等,方案 3 相较于其他方案是最优的。在该方案中,实现了 LSN 环境下政企用户 PPPoE 拨号上网需

表 1 方案优缺点比较

方案	优点	缺点
方案 1	当在原有用户的政企拨号上网业务上叠加 LSN 应用时,对网关设备配置改动较小; 二、三层流量分别走东西向、南北向通道,流量走向清晰	因政企网关位于 CPN 侧,且三层配置较复杂,各家用户 IP 地址规划存在差异,新装或维修时需上门进行个性化配置; 政企网关仍担负 PPPoE 拨号及全部三层转发功能,这与 LSN 架构设想将用户 IP 地址、IT 设备功能全部上移到运营商端局的终极设想存在差距
方案 2	政企网关不直接设三层网关,各 VLAN 之间隔离性好、安全性高	流量有折返现象,由于用户流量两次经过 PON、OLT 汇聚交换机、LSN、互联链路和政企网关,增加了链路和设备负荷; 政企网关仍担负 PPPoE 拨号功能,这与 LSN 架构设想将用户 IP 地址、IT 设备功能全部上移到运营商端局的终极设想存在差距
方案 3	用户三层转发功能全部上移至 LSN 节点,符合 LSN 架构的设想,为运营商在 LSN 节点内提供更加丰富的业务提供了无限可能; 政企网关设备的配置简化,只需保留二层 VLAN 相关功能,可通过预设统一配置,减少现场安装、维护工作量,有利于进一步降低政企网关设备的成本; 政企网关不直接设三层网关,各 VLAN 之间隔离性好、安全性高; 折返流量不经过政企网关,可减少政企网关转发压力	流量有折返现象,由于用户流量两次经过 OLT 汇聚交换机、LSN 及互联链路,增加了链路负荷,但是流量折返不经过政企网关和 PON,对负载的影响比方案 2 小



求,同时 PPPoE 拨号和三层路由功能全部上收至 LSN 节点内的 vRouter,大大简化了 CPN 侧政企网关功能要求,可进一步降低用户侧设备投入成本。CPN 侧设备形态和网络结构大幅简化,则为运营商在 LSN 内提供更加丰富的业务提供了无限可能,这与 LSN 架构简化用户侧网络设备和 IT 系统,将相关功能上移至端局的理念相一致。虽然有流量折返现象,但是由于用户是低带宽型的,且折返路径利用的是 LSN 和互联链路上下行不同方向的带宽,故对现网流量增加压力较小。

总体来看,方案 3 是基于政企用户需求和目前网络现状,适合于 LSN 环境下实现政企用户 PPPoE 拨号应用的最佳实践方案。

6 结束语

LSN 政企网关实现 PPPoE 的方法有很多,在现网部署时,需要结合技术成熟度、技术经济性、技术扩展性、现有资源保护性等因素综合考虑,选择对现网影响最小、运营效率最高、风险最低的技术进行组网。最后,建议 LSN 作为用户 CPN 与 vDC 之间的桥梁,应该加速与城域网的融合,这样资源浪费和流量折返的问题就迎刃而解了。

参考文献:

- [1] 吴志明,傅志仁,张宏斌,等. LSN: 面向 ICT 服务的电信网络架构及其技术实现[J]. 电信科学, 2014, 30(8): 112-130.
WU Z M, FU Z R, ZHANG H B, et al. An ICT service oriented telecom network infrastructure architecture and implementation[J]. Telecommunications Science, 2014, 30(8): 112-130.
- [2] 颜永明,许斌,徐海峰,等. 解决 NFV 环境下拨号上网地址占用问题的 NAT444 方案[J]. 电信科学, 2016, 32(11): 154-160.
YAN Y M, XU B, XU H F, et al. NAT444 solution to the dial-up address occupation in NFV environment[J]. Telecommunications Science, 2016, 32(11): 154-160.

[作者简介]



颜永明(1978-),男,中国电信股份有限公司上海分公司信息网络部综合运营监控中心副经理、高级工程师,主要研究方向为数据网络、云组网等。



叶克阗(1991-),男,中国电信股份有限公司上海分公司信息网络部 IDC 浦西运营中心技术工程师、助理工程师,主要研究方向为数据网络、云组网等。



许斌(1988-),男,中国电信股份有限公司上海分公司信息网络部 IDC 浦西运营中心技术室经理、助理工程师,主要研究方向为数据网络、网络安全等。



徐海峰(1974-),男,中国电信股份有限公司上海分公司信息网络部 IDC 浦东运营中心技术工程师、助理工程师,主要研究方向为数据网络、云组网等。



左良(1976-),男,中国电信股份有限公司上海分公司信息网络部 IDC 浦东运营中心技术工程师、助理工程师,主要研究方向为数据网络、网络安全等。



洪恺渊(1991-),男,中国电信股份有限公司上海分公司信息网络部 IDC 浦西运营中心技术工程师、助理工程师,主要研究方向为数据网络、网络安全等。