



以太网 VPN 技术在云数据中心互联应用的研究

何晓明,唐 宏,刘志华,樊勇兵

(中国电信股份有限公司广东研究院 广州 510630)

摘要

对当前 VPLS 中存在的问题和新出现的以太网 VPN 需求进行概述,介绍并分析 IETF 最新提出的 E-VPN 和 PBB E-VPN 这两种以太网 VPN 的技术特征,结合正在兴起的云数据中心互联的实际应用需求,探讨以太网 VPN 技术在云数据中心的互联组网应用。

关键词 以太网 VPN;E-VPN;PBB E-VPN;云数据中心互联

1 引言

VPLS (virtual private LAN service, 虚拟专用局域网业务)^[1,2]作为一种标准化程度较好、通过试验验证并广泛部署的二层以太网 VPN 技术,能为企业用户提供多点到多点的广域以太网服务。然而,其也存在冗余备份、多播优化、部署便捷性等局限性。在多归宿环境下,当前 VPLS 仅支持主、备接入链路模式^[3],不支持灵活的多主接入链路模式。在多播优化的场景下,Aggarwal^[4]等提出了基于 VPLS 的多播 LSP,这种解决方案仅限于点到多点的 LSP(P2MP LSP),不能适用于多点到多点 LSP(MP2MP LSP)的应用场景。在 VPLS 部署的便捷性方面,当前 VPLS 提供了基于 BGP 的自动发现功能^[1],但仍然需要运营商配置复杂的网络参数。

与此同时,新的应用也给 VPLS 提出了一些新的需求。近年来兴起的云计算数据中心(IDC)互联应用催生出一一种新的被称为“VLAN 敏感绑定”的业务接口,而且虚拟化应用对设备 MAC 地址表容量提出了更高的要求,由此产生了网络收敛性能应能独立于 PE 学习到的 MAC 地址

数量的要求。除此以外,VPLS 也存在最小化多播帧、广播帧、未知单播帧的泛洪数量问题以及需要支持灵活的 VPN 拓扑及策略的问题。

2 以太网 VPN 需求概述

IETF 在以太网 VPN 需求草案中^[5]对当前 VPLS 中存在的问题和新出现的需求进行了描述,可以概括为以下 7 个方面。

- 冗余备份。在基于流的负载分担方面,需要为多以太网链路捆绑定义基于 IEEE 802.1AX 的 LACP 的标准化负载分担算法,以规范设备执行;在基于流的多径负载均衡方面,需要支持一对 PE 之间多条 RSVP-TE LSP 或 ECMP LSP 的负载均衡能力;在 PE 节点冗余方面,需要提供同局址和地理分割的不同局址间的 PE 节点冗余备份能力,在断电或出现自然灾害的情况下以保持关键业务的连续性;在多归宿网络方面,需要支持基于 VLAN 或 MAC 地址的多链路负载分担。

- 多播优化。需要使用 MP2MP LSP 优化多播流、广播流及未知单播流的高效传送机制。
- 部署简易性。在 MPLS 网络中,对于具有全局唯一性标识(如 VLAN ID)的以太网 VPN 实例,PE 在配置 VPN 时所需要的 VPN ID、BGP RT 等参数应能从 VLAN ID 中自动导出而无须另外配置。
- 新业务接口。城域以太网论坛(MEF)及 IEEE 802.1Q 定义了 3 种业务接口模式:端口模式、VLAN 模式、VLAN 绑定模式。在云数据中心互联应用中,产生了可透传的 VLAN 敏感绑定和可转换的 VLAN 敏感绑定两种新的业务接口类型。可透传的 VLAN 敏感绑定接口需要保证客户 VLAN 端到端的透明传送;可转换的 VLAN 敏感绑定需要对属于同一 VLAN 用户在接入网络时采用的不同 VLAN ID 进行翻译。新的业务接口与之前定义的 3 种接口的主要区别在于:新的业务接口需要支持每个 VPN 实例的多桥接域功能,即在同一个 VPN 实例中,需要为每个客户 VLAN 分配一个独立的桥接域。
- 快速收敛。在客户设备多归宿和网络多归宿接入 MPLS 网络的环境下,应提供接入电路或 PE 出现故障时的快速收敛功能,收敛时间应独立于 PE 学习到的 MAC 地址及 VPN 实例数目,这对于虚拟化数据中心互联应用尤其重要。
- 泛洪抑制。网络运营商应能基于策略在每个 VPN 实例的基础上配置未知单播帧的泛洪或丢弃;在数据中心互联的场景下,需要最小化广播帧泛洪;当拓扑发生变化时,需要消除不必要的未知单播流量泛洪。
- 支持灵活的 VPN 拓扑及策略。以太网 VPN 必须提供“hub and spoke”的拓扑控制以及每个 MAC 地址粒度的学习和转发策略控制能力。

3 以太网 VPN 技术

鉴于当前 VPLS 中存在的问题以及新出现的应用需求, IETF 最近提出了两种以太网 VPN 技术: E-VPN^[6]和 PBB E-VPN^[7], 期望能解决上述存在的问题, 并能满足新出现的应用需求。

3.1 E-VPN 技术特征

3.1.1 E-VPN 概述

在标准的 VPLS 实现中, 运营商网络 PE 设备间的 MAC 地址学习基于传统的网桥功能。在 E-VPN 技术中,

PE 之间的 MAC 地址学习则基于控制平面, 采用 MP-BGP 通告 MAC 地址的可达性信息, 其策略控制非常类似于 IP VPN。这种基于控制平面的学习能够对 MAC 地址学习过程提供更强的控制能力, 因此具有较好的扩展性, 并能维护主机或虚拟机群彼此间的隔离性, 解决了设备多归宿或网络多归宿接入时的负载分担问题, 改善了网络出现故障时的收敛时间。然而, PE 与 CE(客户端设备)间的 MAC 地址学习仍然基于数据平面实现, PE 的二层转发表是否装载所有由控制平面学到的目的 MAC 地址, 还是仅注入需要通信的 MAC 地址, 过滤未被使用的 MAC 地址, 完全由 PE 本地决定。这为 PE 的转发表所需 MAC 地址缓存大小的设计提供了很大的灵活性, 不再像标准的 VPLS 技术那样, 属于同一 VPLS 实例的二层转发所需的 MAC 地址表容量受限于最小地址缓存大小的 PE。

在多归宿接入的场景下, 如果一个 CE 多归宿到两个或更多 PE, 这些连接到 PE 的以太网链路组便构成了一个以太网段(ES), 每个 ES 都有一个标识符, 称为 ESI, 由一个 10 byte 的整型数标识, 这是 E-VPN 技术中一个非常重要的概念。E-VPN 定义了一种新的 BGP NLRI, 称为 E-VPN NLRI, 并定义了 5 种路由类型: 以太网自动发现路由、MAC 地址通告路由、包含性多播路由、选择性多播自动发现路由和叶子自动发现路由。

E-VPN 提供了 3 种自动发现机制: E-VPN 自动发现、以太网段上特定以太网标签(VLAN ID)自动发现、以太网段自动发现。E-VPN 自动发现使用第 3 种路由类型——包含性多播路由通告来发现同一个 VPN 实例中的 PE 成员, PE 根据多播路由通告中的 P2MP LSP 或 MP2MP LSP 向其他成员发送多播帧、广播帧和未知单播帧。以太网段上具有相同 VLAN ID 的自动发现使用第 1 种路由类型——以太网自动发现路由通告来发现同一个 VPN 实例中具有同一广播域(全局 VLAN ID 相同)的 PE 成员, 可支持上述以太网 VPN 需求提出的“VLAN 敏感绑定”新业务接口。以太网段自动发现也使用以太网自动发现路由通告来发现同一个或多个 VPN 实例中具有相同以太网段标识(ESI)的 PE 成员, 这是 E-VPN 中最重要的功能, 可使用在多归宿接入的负载分担、多归宿接入 PE 的指定转发器(DF)选举及“水平分割”、优化控制平面的收敛及减少 MAC 地址路由通告数目等各种应用场景。

3.1.2 E-VPN 存在的问题

基于 BGP MPLS 的 E-VPN 的协议框架基本能满足一



般场景下以太网 VPN 应用中的各种需求,但协议框架及实现机制本身还有许多需要完善和进一步研究的地方,如广播帧的抑制(ARP 报文的优化等)、DF 选举策略、多播树的构建流程、故障修复、LACP 状态同步等,目前仍处于 IETF Draft 阶段。随着新的应用场景特别是虚拟化数据中心的出现以及下一代以太网技术(如 TRILL、IEEE 802.1aq)的发展,E-VPN 面临的新问题表现为如下几个方面。

(1) MAC 地址路由通告的扩展性

E-VPN 为每个客户 MAC(C-MAC)地址发送一条 BGP MAC 地址通告路由,这将对存在上百万虚拟主机(VM)的大规模云数据中心环境产生路由通告的扩展性问题。当虚拟主机在云数据中心之间频繁迁移以及网络出现故障的情况下,需要产生大量 BGP MAC 地址通告路由更新,使得网络和设备承受沉重的信令协议负荷。

(2) 基于 MAC 地址子网化的 C-MAC 移动性

对于虚拟机迁移(VMotion)应用,E-VPN 虽然可以通过 MAC 地址子网化的方式通告 MAC 地址的可达性,但是需要对客户 MAC 地址进行精细规划。由于客户设备及主机 MAC 地址的规划不属于运营商的管辖范围,因此当大量虚拟机从一个网段移动到另一个网段时,需要逐条通告每一个具体的 C-MAC 地址信息。

(3) C-MAC 地址学习及限制

当某一个 PE 发送 BGP MAC 地址通告路由时,属于同一 VPN 实例的其他 PE 都会学习,即使这些 C-MAC 地址并不会用来进行通信,PE 仍然需要在路由信息表(RIB)跟踪记录相关 C-MAC 地址,这会引起存储资源的浪费,因此需要对学习到的 C-MAC 地址进行限制,仅允许保留需要通信的 C-MAC 地址。

(4) 与 TRILL 和 IEEE 802.1aq 网络的互操作

TRILL^[8]和 IEEE 802.1aq 定义了下一代以太网桥技术,借助于 IS-IS 控制平面优化以太网帧的转发,采用以太网隧道技术实现客户以太网帧的传送以保持 C-MAC 地址的透明性。当基于 TRILL 或 IEEE 802.1aq 的接入网络互联 MPLS/IP 网络时,需要 MPLS 网络边缘 PE 保持 C-MAC 地址的透明性,PE 对 TRILL 或 IEEE 802.1aq 报文封装的终结不能满足这种透明性要求,同时还会产生 PE 所要支持 C-MAC 地址的扩展性问题。

(5) 每站点的策略支持

E-VPN 提供每个 MAC 地址粒度的学习和转发策略控制能力,在许多应用中,运营商更需要基于站点的策略控

制,用以提供 E-tree、半网状互联等业务,此时基于 C-MAC/EVI 的策略控制难以满足实际应用需求。

3.2 PBB E-VPN 技术

PBB E-VPN 把基于 IEEE 802.1ah 标准的 PBB 技术及 E-VPN 技术结合在一起。MPLS 网络入口 PE 设备把从接入电路(AC)接收的 IEEE 802.1Q 以太网帧封装成 PBB 报文,通过 IP/MPLS 网络转发,出口 PE 弹出 MPLS 标签后移除 PBB 头部,解封装成原始以太网 IEEE 802.1Q 以太网帧,然后交付给 CE。基于 PBB E-VPN 的 PE 需要执行如下功能:

- 基于标准的网桥功能通过 AC 学习本地 C-MAC 地址;
- 基于 IEEE 802.1ah 标准的网桥操作,通过数据转发平面从网络侧接收的数据流中学习远端 C-MAC 地址与 B-MAC 地址的绑定关系;
- 采用 MP-BGP 向属于同一 VPN 实例的其他 PE 通告本地 B-MAC 地址的可达性信息,注意到每个 PE 有一套用于标识本地 PE 设备的 B-MAC 地址;
- 根据接收到的 BGP 路由通告消息中的远端 B-MAC 地址、IP 地址及关联的 MPLS 标签构建转发表。

其与 E-VPN 的最大差异在于:PBB E-VPN 不需要通过 BGP 发布 C-MAC 地址。每个 PE 基于标准的网桥操作通过数据平面独立学习 C-MAC 地址,每个 PE 有一个或多个与之关联的 B-MAC 地址,这些 B-MAC 地址通过 BGP MAC 地址通告路由向 MPLS 网络边缘设备发布。这种改变解决了 E-VPN 存在的上述问题,如 MAC 地址路由通告的扩展性问题、基于 MAC 地址子网化的 C-MAC 移动性问题、C-MAC 地址学习及限制问题、每站点的策略支持问题、网络拓扑改变时避免受影响的 C-MAC 地址清除问题。PBB E-VPN 还定义了一个新的 TRILL Nickname 通告路由,以支持与 TRILL 及 IEEE 802.1aq 网络的无缝操作,因此保持了 C-MAC 地址的透明性。表 1 给出了 VPLS、E-VPN、PBB E-VPN 3 种技术对以太网 VPN 需求的满足程度。

从表 1 可以看出,PBB E-VPN 技术能够充分满足即将兴起的虚拟化数据中心以及下一代以太网技术等新的应用场景需求。由于 PBB E-VPN 是对 E-VPN 功能的增强,E-VPN 协议框架有待完善的地方在 PBB E-VPN 上依然存在,其标准化程度也将随着应用验证及广泛部署而日渐成熟。

4 以太网 VPN 技术在云 IDC 互联应用

云 IDC 指以客户为中心、以服务为导向,基于高效、低

表 1 3 种 VPN 技术对以太网 VPN 需求的满足程度

以太网 VPN 需求	VPLS	E-VPN	PBB E-VPN
基于流的多接入链路负载均衡		✓	✓
基于流的多径负载均衡		✓	✓
地理分割的 PE 冗余及灵活的 PE 冗余组		✓	✓
自动发现	✓	✓	✓
使用 P2MP 或 MP2M PLSP 构建大规模多播		✓	✓
部署的简易性		✓	✓
新业务接口		✓	✓
故障快速收敛		✓	✓
MAC 移动性的快速收敛			✓
避免 C-MAC 清除的快速收敛			✓
MAC 通告路由的扩展性			✓
C-MAC 地址学习和限制			✓
与 TRILL/IEEE 802.1aq 网络的无缝操作			✓
每站点的策略支持			✓

能耗的 IT 与网络基础架构,利用云计算技术,自动化地按需提供各类云计算服务的新一代数据中心。由于云 IDC 具有资源池化、高效智能、面向服务、按需供给、绿色低碳等特点,已率先在 Google、Facebook、亚马逊等互联网公司获得成功应用,并成为这些企业的核心竞争力之一。国内一些知名互联网企业(如百度、腾讯等)开始新建或扩展大型云 IDC,中国电信为顺应云计算时代到来的趋势,开始在多个省份建设云 IDC。云 IDC 互联是把地理分散的多个独立的云 IDC 通过大二层网络互联起来,形成一个逻辑上虚拟化的超大型数据中心。云 IDC 互联能够为企业实现数据中心整合、业务统一运营、异地容灾备份、虚拟机在线迁移、节能减排等各方面提供条件,通过更靠近用户的分布式应用及业务的连续性提升用户感知。一些互联网公司要求电信运营商网络能够为其提供多个 10 Gbit/s 甚至数百 Gbit/s 的高速带宽进行云 IDC 互联。

云 IDC 的一个基本特征是虚拟机数目巨大,虚拟机迁移频繁发生,并且要在迁移过程中保持 VLAN、IP 地址、MAC 地址等虚拟机的网络标识不能改变,从而保证业务的灵活部署和连续性,这就决定了云 IDC 互联必须采用多点到多点的二层 VPN 技术。由于云 IDC 互联需要提供足够的带宽保证和较低的时延,同时对互联网络的可靠性和可用性也提出了很高的要求,因此在实现多点互联的以太网 VPN 技术中,PBB E-VPN 是专为云数据中心互联而优化的技术,能够满足云数据中心互联环境下的应用需求。

下面分析 PBB E-VPN 在云数据中心互联应用中的技术实现。

4.1 云 IDC 多归宿接入 MPLS 网络

(1) 站点多归宿接入的情形

考虑到某个 CE 通过多归宿主链路接入 MPLS 网络中的一组 PE 节点,这组 PE 节点形成一个 PE 冗余组,为实现多归宿接入的负载分担及 AC 故障的快速收敛,需要为该 CE 接入的 PE 冗余组分配一个唯一的 B-MAC 地址。图1给出了站点多归宿接入核心网络的示例。

图 1 中,CE1 通过 Active-Active 冗余链路接入 MPLS 网络的 PE1、PE2、PE3,为 PE1、PE2、PE3 形成的冗余组分配一个唯一的 B-MAC1 地址(对于基于 LACP 捆绑的链路,PE 可从 CE 的 LACP 系统 ID 自动导出 MAC 地址作为 B-MAC 地址),PE1、PE2、PE3 分别向远端 PE_r 发送属于同一 ES 的 B-MAC1 地址的 BGP MAC 通告路由,远端 PE_r 最终生成 RIB 和 FIB。在远端 PE_r 安装的 FIB 中具有 3 个到达 B-MAC1 地址的下一跳 PE1、PE2、PE3,PE_r 基于散列算法在这 3 个下一跳实现到达与 B-MAC1 地址具有绑定关系的目的 C-MAC 地址以太网帧的负载均衡。当 PE1 与 CE1 之间的 AC 发生故障时,PE1 立即撤销 B-MAC1 地址路由,PE_r 更新 RIB 和 FIB,到达目的 C-MAC 地址以太网帧,只在下一跳 PE2 和 PE3 之间实现负载均衡。

(2) 网络多归宿接入情形

图 2 给出了以太网多归宿接入核心网络的示例。以

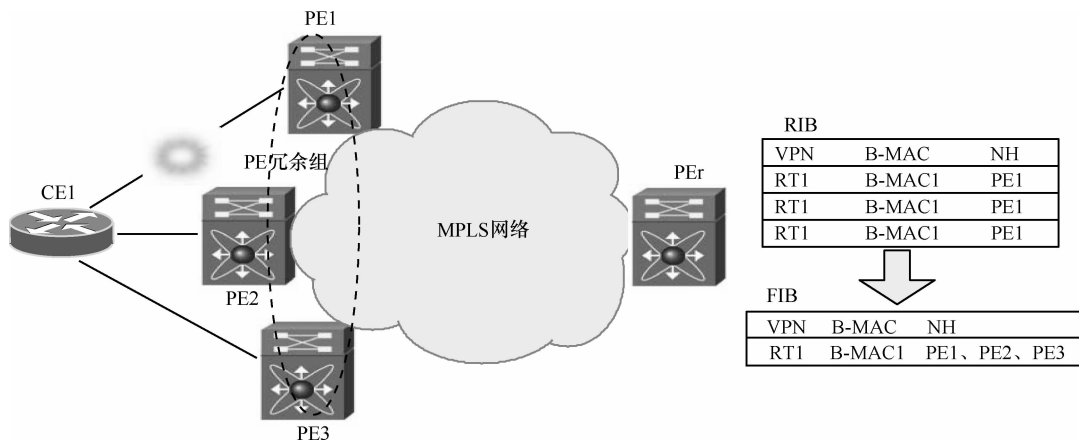


图1 站点多归宿接入核心网络示例

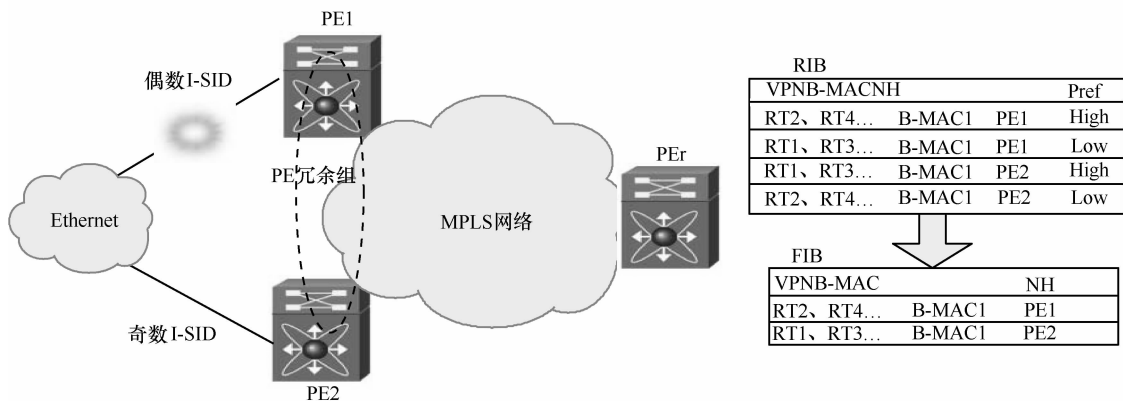


图2 网络多归宿接入核心网络示例

太网络通过 Active-Active 冗余链路接入 MPLS 网络的 PE1、PE2，为 PE1、PE2 形成的冗余组分配一个唯一的 B-MAC1 地址(PE 可通过探测多归宿以太网的 BPDU 报文并提取根桥 ID 作为 PE 的 B-MAC 地址)，正常情况下，假设 PE1 负责来自多个偶数 I-SID 以太网帧的数据转发，PE2 负责来自多个奇数 I-SID 以太网帧的数据转发。PE1 和 PE2 分别向远端 PEr 发送属于同一 ES 的 B-MAC1 地址的两条 BGP MAC 通告路由，对于 PE1，其中有一条携带标识偶数 I-SID 的 RT，并具有较高的本地优先级(local pref)属性，另一条携带标识奇数 I-SID 的 RT，并具有较低的本地优先级属性；PE2 发送的两条 BGP MAC 通告路由由携带的 RT 及 Local Pref 恰好同 PE1 相反。远端 PEr 最终生成 RIB 和 FIB，把去往偶数 I-SID 的以太网帧发送到下一跳 PE1，把去往奇数 I-SID 的以太网帧发送到下一跳 PE2，实现对来自/去往以太网络的以太网流量基于 I-SID 的负载均衡。

4.2 PBB E-VPN 在云 IDC 互联应用中的优势

(1)MAC 地址路由通告的扩展性

在 PBB E-VPN 中，MAC 通告路由的数目是站点或以太网段数量的函数关系，而不是主机/服务器数量的函数关系，换句话说，PBB E-VPN 通过 BGP 通告的是 B-MAC 地址路由而不是 C-MAC 地址路由。因此，PBB E-VPN 发布的 MAC 通告路由数目比 E-VPN 减少几个数量级，非常适合于存在上百万虚拟机的大规模云 IDC 的环境。

(2)C-MAC 地址的移动性

当 C-MAC 地址从一个以太网段 ES 迁移到另一个 ES 时，由于 PBB E-VPN 发布的 BGP MAC 通告路由中的 B-MAC 地址与 PE 节点保持一种静态的关联，并不需要通告 B-MAC 地址的变化，C-MAC 地址与 B-MAC 地址的绑定关系通过数据平面的学习自动更新，避免了 E-VPN 中需要通告大量发生虚拟机迁移时受影响的 C-MAC 地址路由。

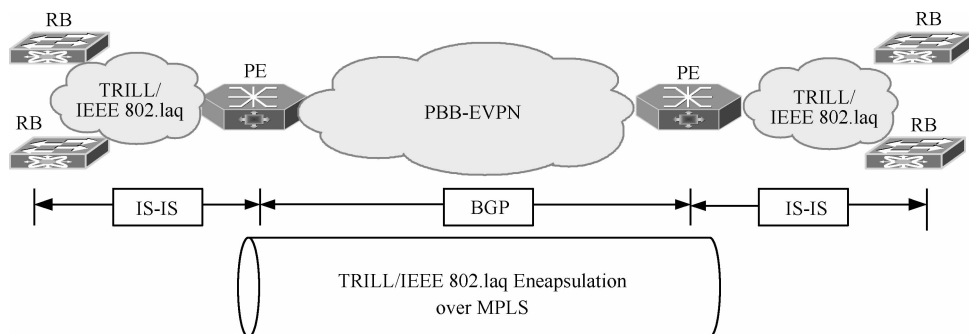


图3 PBB E-VPN 与 TRILL/IEEE 802.1aq 网络的无缝连接示意

(3) C-MAC 地址学习及限制

在 PBB E-VPN 中, C-MAC 地址的可达性是通过数据平面的学习获得的, 因此 PE 转发表中仅需保留需要通信的 C-MAC 地址; C-MAC 地址不需要通过 BGP 通告, 因此 PE 控制平面的路由表不需要维持任何 C-MAC 地址记录, 可节省大量需要记录 C-MAC 地址的存储资源。

(4) 网络出现故障时避免 C-MAC 地址清除

PBB E-VPN 可在接入链路出现故障或网络拓扑发生改变时, 避免 C-MAC 地址清除。在图 1 中, PE1、PE2、PE3 向远端 PEr 通告同一 ES 的 B-MAC1 地址路由, PEr 通过数据平面学习连接到 CE1 的主机或服务器的 C-MAC 地址与 B-MAC1 地址的绑定关系, 如果 PE1 与 CE1 之间的 AC 发生故障, PE1 只需撤销 B-MAC1 地址路由, PEr 不需要清除所有学习到的 C-MAC 地址。

(5) 每个站点的策略支持

在 PBB E-VPN 中, PE 可以通过 BGP 通告的 B-MAC 地址与客户单归宿或多归宿站点相关联, 为 E-TREE 等业务定义每个站点的转发策略。假设云 IDC 中, 某个企业客户有 100 台虚拟主机连接到同一个 CE 站点, 当需要把这 100 台虚拟主机迁移到另一个云 IDC 时, 只需要连接原 IDC 的 PE 撤销与该 CE 站点关联的 B-MAC 地址路由, 然后在连接新迁移的 IDC 的 PE 上重新发布一条该 CE 站点关联的 B-MAC 地址路由即可, 无须逐条撤销或刷新 C-MAC 地址通告路由。

(6) 与 TRILL 和 IEEE 802.1aq 网络的无缝连接

传统的二层以太网基于 STP 实现环路, 避免和以太网数据帧转发, 导致低的链路利用率和低效的数据流转发效率, 同时因 STP 引起的慢收敛等问题已不能满足虚拟环境下云 IDC 的高速数据流转发。TRILL 和 IEEE 802.1aq 作为下一代以太网桥技术试图解决传统以太网存在的问题, 有望在未来几年充当云 IDC 内部互联的大型二层网络基础

设施。PBB E-VPN 与 TRILL/IEEE 802.1aq 网络的无缝连接的示意如图 3 所示。

PBB E-VPN 能够实现 TRILL/IEEE 802.1aq 网络与 IP/MPLS 网络的无缝连接, 同时维护各自网络控制平面的独立性。连接 TRILL/IEEE 802.1aq 网络的 PE 既充当控制平面的边缘交换机, 又充当数据平面的核心交换机。PE 并不终结 TRILL/IEEE 802.1aq 的报文封装, 相反, 入口 PE 把 TRILL/IEEE 802.1aq 报文打上 MPLS 标签, 通过 MPLS 网络进行标签转发; 出口 PE 移除相应 MPLS 标签, 还原原始的 TRILL/IEEE 802.1aq 报文封装格式。这就保持了 MPLS 网络对云 IDC 中虚拟主机 MAC 地址的透明性传送, 而不需要边缘 PE 设备维护数量巨大的虚拟主机 MAC 地址表。

5 结束语

以太网 VPN 技术能够适应企业多点互联的需求, 具有广泛的应用前景, 为电信运营商及设备制造商所关注, 以太网 VPN 技术及标准化程度也将随着其在运营商网络的广泛部署而日渐成熟。在实现多点二层互联的以太网 VPN 技术中, VPLS 作为一种标准化程度较好并广泛部署的 VPN 技术, 已被广大用户所接受, 同时也存在一些问题。E-VPN 和 PBB E-VPN 实际上是对 VPLS 的功能增强, 更能满足现有业务及新的应用需求以及下一代以太网技术发展的需要。

云 IDC 利用云计算技术, 自动化地按需提供各类云计算服务, 将对传统 IDC 产生巨大的冲击和深远的影响, 传统 IDC 向新一代云 IDC 的演进是一个必然的过程。云 IDC 互联能够为企业实现数据中心整合、业务统一运营、异地容灾备份、虚拟机在线迁移、节能减排等各方面提供条件, 并能提升用户感知。同时, 云 IDC 互联对承载网络提出了更高的要求。PBB E-VPN 是专为云 IDC 互联而优化的以



太网 VPN 技术,能够满足云 IDC 互联环境下的应用需求,并随着应用的广泛推进而日趋完善。

参考文献

- 1 RFC4761. Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling, 2007
- 2 RFC4762. Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling, 2007
- 3 Kothari B, Kompella K, Henderickx W, *et al.* BGP Based Multi-Homing in Virtual Private LAN Service. IETF Draft, Work in Progress, 2011
- 4 Aggarwal R, Kamite Y, Fang L. Multicast in VPLS. IETF Draft, Work in Progress, 2012
- 5 Sajassi A, Aggarwal R, Nabil Bitar, *et al.* Requirements for Ethernet VPN (E-VPN). IETF Draft, Work in Progress, 2012
- 6 Aggarwal R, Sajassi A, Henderickx W, *et al.* BGP MPLS Based Ethernet VPN. IETF Draft, Work in Progress, 2012
- 7 Sajassi A, Salam S, Boutros S, *et al.* PBB E-VPN. IETF Draft, Work in Progress, 2012
- 8 Touch J, Perlman R. Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement. RFC 5556, 2009
- 9 Perlman R. Routing Bridges (Rbridges): Base Protocol Specification. RFC 6325, 2011
- 10 唐宏, 陈楠. 云数据中心演进思路剖析. 电信科学, 2011, 27(10)

[作者简介] 何晓明,博士,主要从事数据通信研究,已发表论文 20 余篇,申请专利 15 个;唐宏,中国电信股份有限公司广东研究院数据通信研究部部长,主要从事下一代互联网和云计算方面的研究;刘志华,硕士,主要从事数据通信研究及网络支撑工作;樊勇兵,博士,主要从事互联网、云计算和 IDC 的研究工作。

Investigation on the Applications of Ethernet VPN in Cloud Data Center Interconnection

He Xiaoming, Tang Hong, Liu Zhihua, Fan Yongbing

(Guangdong Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China)

Abstract The problems existing in the current VPLS services and new requirements for ethernet VPN are summarized, and the technical characteristics of E-VPN and PBB E-VPN newly presented by IETF are introduced and analyzed. Furthermore, integrated with the actual application requirements of the cloud data center interconnection, the applications of ethernet VPN in cloud data center interconnection are investigated.

Key words ethernet VPN, E-VPN, PBB E-VPN, cloud data center interconnection

(收稿日期:2012-05-09)

·简讯·

PMC 荣获浪潮“2011 年最佳质量奖”

PMC 公司日前宣布其荣获国内服务器领导厂商——浪潮集团授予的“2011 年最佳质量奖”(2011 Best Quality Award)。

PMC 公司中国区销售副总裁张纲先生表示:“PMC 很荣幸能够从浪潮获得这个奖项,它肯定了我们出色的技术和技术支持以及产品的稳定性和高性能。对于

现运行于浪潮中高端服务器中的 Adaptec by PMC 产品已获得广泛认可,我们深感自豪,并期待着不断巩固与浪潮的合作。”

PMC 是半导体解决方案的创新领导者,致力于推动网络升级为连接、传送以及存储大数据的网络。秉持长久以来累积的技术优势,PMC 在存储、光网络以及移动网络领域持续创新。PMC 高集成度解决方案可提升效能,加速网络升级以实现下一代网络服务。