

xPON 系统中用户侧端口成环的破除方法

杨 柳¹, 曾 颜²

(1. 中国移动通信集团湖北有限公司 武汉分公司, 湖北 武汉 430023; 2. 烽火通信科技股份有限公司, 湖北 武汉 430073)

摘要:在以太网无源光网络/吉比特无源光网络(EPON/GPON)系统中,光网络单元(ONU)用户端口成环将会造成同一个无源光网络(PON)口下所有的业务中断。文章首先分析了 EPON/GPON 系统中造成 ONU 用户端口成环的常见原因以及成环后所带来的严重后果,然后列出了 5 种可以破除用户侧端口环路的方法,并在此基础上提出了采用“特殊报文探测法”破除用户环路。利用特殊报文的收发和比对可以自动地发现和阻止用户端口成环。

关键词:吉比特无源光网络;以太网无源光网络;用户端口成环

中图分类号:TN915.6 **文献标识码:**A **文章编号:**1005-8788(2011)02-0017-03

Solution to user ports loopbacks in xPON systems

Yang Liu¹, Zeng Yan²

(1. China Mobile Communications Group, Hubei Province, Wuhan Co., Ltd., Wuhan 430023, China;

2. FiberHome Telecommunication Technologies Co., Ltd., Wuhan 430073, China)

Abstract:In EPON/GPON systems, ONU user ports loopbacks will cause the discontinuation of all the services at the same PON user ports. This paper first analyzes the common causes for the loopbacks and the serious consequences arising from them. Then, it lists five methods that can be used to prevent the ONU's UNI ports from loopbacks and, on this basis, presents a "special message detection" method, which can be used to automatically discover and block the user port loopbacks by sending, receiving and comparing the special messages.

Key words:GPON;EPON;UNI port loopback

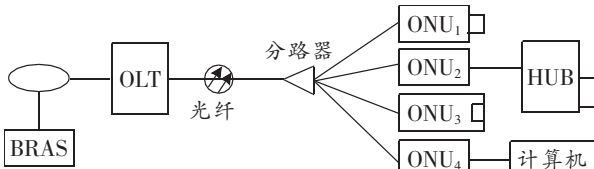
0 引 言

以太网无源光网络/吉比特无源光网络(EPON/GPON)被认为是现阶段接入网的最佳解决方案,但在实际应用中仍然面临大量的挑战。光网络单元(ONU)通常放置在用户家中或者住宅楼的楼道内,用户可以任意对 ONU 进行操作,由于用户设备级联或者误操作甚至恶意用户造成的用户端口成环将会导致同一个无源光网络(PON)口下的业务全部中断。如何防止或者及时破除用户端口的环路是运营商普遍关注的一个问题。许多设备厂家也都纷纷提出了自己的解决方案。本文首先分析可以用来破除用户端口环路的一些方案,然后在此基础上提出用“特殊报文探测法”来破除用户环路。

1 ONU 用户端口成环的可能原因

在 EPON 和 GPON 中,引起用户端口形成环路的原因有很多,其中最为常见的有以下 5 种:(1)具有多个用户端口的 ONU 由于误操作将同一个 ONU 的两个用户端口互联成环,见图 1 中的 ONU₁; (2)ONU 的一个端口下又级联一个或多个

多端口的用户设备(例如多端口的集线器(HUB)或二层交换机),用户的多端口设备成环,见图 1 中的 ONU₂; (3)由于 ONU 物理上的损坏(如雷击或者芯片老化等原因)形成环路,见图 1 中 ONU₃; (4)ONU 连接的用户计算机中毒,将接收到的报文都转发回 ONU 的端口,见图 1 中 ONU₄; (5)恶意用户故意盗取上层设备地址,并向网络中发送攻击报文。原因(4)和(5)虽然不是物理上形成真正的环路,但是其产生的后果却与物理形成环路是相似的。



注:BRAS 为宽带远程接入服务器; OLT 为光线路终端

图 1 ONU 用户端口成环示意图

2 用户侧端口成环的危害

OLT 和 ONU 的功能由 3 部分组成(见图 2):PON 核心功能、二层交换功能以及业务处理功能。其中,二层交换功能所有包的转发都是基于媒体接入控制(MAC)地址表。地址表的表项是通过学习



图 2 OLT/ONU 功能模块

接收到的以太网包的源 MAC 地址得到的。当交换机在某一个端口上接收到一个以太网包后,就会学习这个包的源 MAC 地址,并且在 MAC 地址表中记录源 MAC 地址与接收端口的对应关系。在转发报文时,根据报文的的目的 MAC 地址来查找 MAC 地址表,找到对应端口后将报文从这个端口转发出去。正常情况下上游设备(例如 BRAS/SR(SR 为业务路由器)或者网关)的源 MAC 地址只能在 OLT 或者 ONU 的上联端口上学习到,因此用户发往上游设备的报文都会从 ONU 和 OLT 的上联口正确地转发出去。但是如果用户侧端口成环,上游设备的 MAC 地址会在 OLT 的 PON 侧端口和 ONU 的用户侧端口上学习到,导致 OLT 和 ONU 在转发报文时的混乱。

当 OLT 和 ONU 的 MAC 地址表设置了老化时间后,上游设备的 MAC 地址将会时而在 OLT 或者 ONU 的上联口学习到,时而在 OLT 的 PON 侧端口或 ONU 的用户侧端口上学习到。因此用户发送给上游设备的报文时会而会正确转发,时而又会被错误地转发到产生环回的用户侧端口。这个 PON 口下的所有业务时断时通,非常不稳定。若 OLT 或 ONU 的 MAC 地址表的老化功能被禁用(即设置成不老化),则会出现整个 OLT PON 口下所有 ONU 的业务长时间中断的严重故障。

ONU 端口业务成环还有一个危害就是会造成整个 PON 口下的广播风暴,导致 ONU 所在的所有业务瘫痪。这个在原因(2)造成的用户端口成环中是很容易产生的。

3 阻止用户端口形成环路的方法

常见的用于破除用户端口环路的方法可以分为两大类,一类是利用生成树协议/快速生成树协议(STP/RSTP)算法来计算网络拓扑从而消除环路;另一大类就是利用二层交换芯片本身提供的访问控制列表(ACL)功能或者是 MAC 地址表的学习功能来防止在用户侧端口上学习到上游设备的 MAC 地址,主要包括 ACL 静态配置法、禁止站点移位方法和 MAC 地址表探测法等。这些破坏方案主要在 ONU 上实现。每一种方法的具体实现原理和优缺点如下:

点如下:

(1) STP/RSTP 算法。STP/RSTP 是一个成熟的协议,它通过在交换机之间传递特殊的协议报文来确定网络的拓扑结构。如果某台交换机能够从两个以上的端口接收到协议报文,则说明存在环路,此时交换机根据端口的配置选出一个端口并把其他的端口阻塞从而消除循环。在多端口 ONU 上运行 RSTP,可以防止原因(2)产生的用户端口成环,并且能阻止广播风暴的产生,在故障解除后能够自动恢复。但是,RSTP 方式需要对端的以太网交换机也支持 RSTP,并且它无法破除其他原因产生的用户侧端口环回。

(2) ACL 静态配置法。利用 ONU 设备二层交换芯片的 ACL 功能,在 ONU 的用户侧端口将 BRAS 或网关等上游设备的 MAC 地址过滤掉,不允许用户侧方向学习到上游设备的 MAC 地址。这种方式要在所有 ONU 的所有用户端口上都配置 ACL 规则,工作量非常大而且不灵活,当 ONU 数量较多时,这种方法几乎不能使用。虽然这种方法可以防止包转发上的混乱,但是它无法防止成环后形成的广播风暴。

(3) 禁止站点移位(station movement)法。所谓站点移位就是同一个 MAC 地址在交换芯片的不同端口上学习到。普通的交换芯片是无法阻止站点移位的。目前新推出的中高档交换芯片可以通过配置寄存器来禁止站点移位,即某一个 MAC 地址只能在第 1 次接收到的端口上学习,其他端口将会丢弃具有相同源 MAC 地址的报文,而且也不会学习。可见,启用了禁止站点移位功能后,ONU 只能在上联端口上学习到上游设备的 MAC 地址,来自用户侧的环回报文都会被丢弃,从而保证了到上游设备的报文能够正确转发。但是,这种方法同样只能避免转发上的混乱,无法解决因环路形成的广播风暴问题。

(4) MAC 地址表探测法。这种方法与禁止站点移位方法的原理类似。不同的是,禁止站点移位一般是依赖交换芯片的功能,而 MAC 地址表探测则由 ONU 设备上的 CPU 来完成。ONU 上的 CPU 通过与交换芯片相连接的串行接口或者并行接口将交换芯片中的 MAC 地址表读取到 CPU 的内存中进行分析,由于 CPU 的处理速度限制,不会对交换芯片所有端口都进行对比,而是重点关注上联口上学习到的 MAC 地址是否在用户侧端口上出现。若发现用户端口出现环路,就将这个用户侧端

口禁止掉,不允许其继续转发任何报文,同时向网管上报告警。该方案与禁止站点移位方案相比优势在于:MAC 地址表探测法可以发现上文列出的所有 5 种原因造成的用户侧端口环回,而且由于成环的端口被禁用了,还能防止产生广播风暴导致的整个 PON 口瘫痪。网管上产生告警也可以及时通知维护人员排除故障。站点移位功能只有新推出的几款中高档交换芯片才具备,从成本上来考虑,ONU 不可能采用这些交换芯片,因此 MAC 地址表探测法还具有成本上的优势。但是由于该方法需要 CPU 来读取 MAC 地址表并且进行分析,若 MAC 地址表深度过大,处理速度将会非常慢,处理的及时性将会达不到要求。因此对 CPU 的性能要求比较高。

(5) 简化的 MAC 地址表探测法。MAC 地址表探测法受到 ONU 交换芯片地址表规模的限制,且对 CPU 的处理能力提出了较高的要求。简化的 MAC 地址表探测法就是通过网管将上游设备的 MAC 地址配置给 ONU 的 CPU。ONU CPU 只按一定的周期检查用户侧端口的 MAC 地址表项,看是否出现网管上配置的上游设备的 MAC 地址。这种方法虽然和 ACL 静态配置法一样要通过网管配置上游设备的 MAC 地址,但是只需要配置一次即可,不需要在每一个 ONU 端口上都绑定 ACL 规则。因此工作量比 ACL 静态配置法的工作量要小得多。这种方法的主要问题还是在读取 MAC 地址表的速度上。若 MAC 地址表深度非常大,那么检测的性能还是会受到影响。

4 特殊报文探测法

上面介绍的 5 种破除用户端口环路的方法都存在一些缺陷,例如不能消除所有原因导致的环路,或者是配置量大,不灵活,还有就是对交换芯片的功能或者对 CPU 性能有较高要求从而增加了设备成本。

本文参考了 RSTP、站点移位和 MAC 地址表探测等方法的原理,并在此基础上加以改进提出了一种特殊报文探测法,具体如下:ONU 的 CPU 会定期发送一个特定内容的以太网报文,正常情况下这些特殊报文不会在 ONU 用户侧端口的上行接收到,并且这些特殊报文具有特别的源 MAC 地址(如 MACA)。同时,在 ONU 交换芯片的用户侧端口上设置一个规则,只要接收到的以太网包的源 MAC 地址等于 MACA,就将这个报文转发到 CPU 上。

这里要注意,不要将这个特定报文的源 MAC 地址设置成 CPU 的 MAC 地址,否则遇到恶意用户时容易遭到攻击。如果 ONU 具有多个用户端口,CPU 还要在特殊报文的净荷中定义一个端口区分字段用于区分每一个用户端口,通常端口区分字段的值可以定义为用户端口序号。如果 CPU 接收到自己发出去的报文,就表示用户侧的端口出现了环回,CPU 通过特殊报文中端口区分字段的内容判断出现环路的端口的序号,将这个成环的端口禁止,阻止其继续转发报文,同时向网管发出告警。维护人员看到告警后到 ONU 侧分析原因处理故障,如果是原因(1)和原因(2)造成的环回,则拆除成环的设备或者网线即可。如果是电脑中毒,则告知用户杀毒。当消除了成环的原因后,后续的操作可以分为人工恢复和自动恢复两种,即可以采用人工恢复和自动恢复两种方法来启用被禁用的端口。人工恢复就是维护人员在网管上将禁止掉的端口重新打开。自动恢复就是 CPU 定期将被禁用的端口试探性的启用,同时发出探测报文,观察该报文是否会返回到 CPU。如果没有异常,就认为故障消除了,该端口将会一直启用;如果发现从该端口发出去的特定报文又被环回到 CPU,则表示故障仍然存在,该端口将会再一次被禁用。

5 结束语

特殊报文探测法借用了 RSTP 报文的思路,但是并不需要复杂的算法。通过收发和比对具有特殊源 MAC 地址和端口区分字段的特殊报文,就能动态地发现并阻断所有原因形成的用户端口环路,防止广播风暴的产生,无需运维人员的配置操作。由于该方法并没有复杂的算法,对交换芯片的功能和 CPU 处理能力要求都不高,处理的及时性也能够达到要求,因此特殊报文探测法是一种比较好的用户端口成环检测和破坏的方法。

参考文献:

- [1] 唐勇. 交换机端口环路检测功能的有效性研究 [J]. 重庆工商大学学报(自然科学版), 2010, (03): 267-270.
- [2] 蔡建波. EPON+LAN 环路风暴的预防 [J]. 中国有线电视, 2010, (01): 25-27.
- [3] 洪增斌. 局域网中广播风暴产生原因及解决方法之分析 [J]. 办公自动化, 2010, (10): 44-45.