

# 基于病毒遏制技术 (Virus-Throttling)的 连接速度过滤

技术摘要

简介 .....	3
当前响应的限制 .....	3
新解决方案的推出势在必行 .....	3
病毒遏制：什么是病毒遏制，它如何工作 .....	4
它是什么 .....	4
快速检测，及时阻止 .....	4
病毒遏制技术的优点 .....	4
它如何工作 .....	5
ProCurve 交换机上的连接速度过滤 .....	5
过滤选项 .....	5
灵敏度和应用选项 .....	6
ProCurve Manager Plus .....	7
配置原则 .....	7
对于相对不易受攻击的网络 .....	7
对于看起来存在较大攻击危险的网络 .....	7
ProCurve 交换机上的 ICMP 速率限制 .....	9
什么是速率限制 .....	9
ICMP 速率限制的影响 .....	9
ICMP 速率限制的操作 .....	9
网络应用 .....	9
总结 .....	10

## 简介

每一个IT经理都知道，计算机病毒的泛滥正日趋严重。2003年，SQL Slammer病毒在1分钟内感染了75,000台计算机，成为迄今为止传播速度最快的病毒，引发了全球范围内的网络中断。Nimda、Blaster、Code Red、Sasser和Welchia病毒也在持续不断地威胁着网络安全。目前，计算机用户直接面临97000多种病毒、蠕虫和特洛伊木马<sup>1</sup>的威胁。即时消息等网络应用的逐渐增加也进一步增加了感染病毒的风险。2005年第三季度，IM威胁的总数比上一年多3000% (来源于IMlogic威胁中心)。

为了防止受到计算机病毒所产生的流量冲击，很多企业不得不关闭其部分网络基础设施架构；如果他们不能尽快采取措施，病毒有可能使整个网络子网甚至整个网络瘫痪。总之，病毒使企业由于效率的降低而遭受难以估算的损失。除了使办公室或企业停止正常运转之外，计算机病毒还可能把攻击者定义的代码传播到系统上，导致更多的损害。

当信息主要通过共享软盘进行传输时，网络威胁的发展将会很缓慢，且非常容易抵御。在这种情况下，组织也有时间清理其网络，采取有效的防御措施。但是随着CPU速度的提高、带宽的增加、网络对业务发展的影响日益重要以及客户端的移动性越来越高时，网络管理员关闭操作或排除病毒感染的时间也变得越来越短。

网络病毒不仅仅导致效率的低下，而且SQL Slammer病毒还导致了为西雅图附近2个警察部门和14个火警部门服务的911应急响应中心系统的瘫痪。防止计算机病毒可能最终成为保护生命的重要措施。

### 当前响应的限制

当前阻止恶意代理程序蔓延的方法是使用签名识别避免主机受到感染，即想办法阻止病毒或蠕虫进入系统。这些方法将重点放在对病毒的物理特性的研究上——即病毒的程序代码，并使用部分代码创建独一无二的签名。进入系统的程序与这个签名进行比较，如果匹配就会被清除。

尽管这种方法在保护系统上很有效，但仍有几方面的限制，并且随着病毒数量的增加，其有效性则会随之降低。从根本上来说，这种方法属于反应式的个案处理方法，因为当每一个新病毒或变种出现时，都要为其开发新的签名。签名的开发通常由熟练人员来完成，一次只能产生一定数量的签名。而随着病毒数量的增加，首次检测与发布签名之间的时间也随之增加，同时病毒会进一步扩散。

新病毒或蠕虫进入网络与实施和分发基于签名的补丁之间的这段延迟时间就变得愈加重要。在此期间，被感染的主机所产生的异常高速流量有可能使网络瘫痪。

只要攻击以“机器速度”进行，而响应以“人的速度”实施，计算机在新的威胁前基本上只能束以待毙。随着系统不断扩大且日益复杂，这些新威胁的解决也越来越复杂。

### 新解决方案的推出势在必行

需要一个不同的解决方案。真正有弹性的基础设施架构应当包括能够自动阻止、抑制并减缓以前未知威胁攻击的解决方案，为负责基础设施架构安全的人员提供实施响应所需要的时间。

新的解决方案并非是取代当前基于签名和补丁的保护措施，而是让计算机和人分别做各自最擅长的工作，以相互补充：计算机能够比人做出快得多的响应，但在确定以前未知威胁的性质上却差强人意。而人类则擅长做出这方面的决定，但与机器比较，行动速度却较慢。新的解决方案应当在人工能够干预之前，让计算机快速行动，稳定局面。

---

<sup>1</sup> <http://msnbc.msn.com/id/6679126/>; <http://msnbc.msn.com/id/4065701/?p1=0>

# 病毒遏制：什么是病毒遏制，它如何工作

基于病毒遏制技术的连接速度过滤是惠普开发的一个新的解决方案，用于克服以前的响应速度上的限制，快速控制和迁移由恶意代理产生的攻击。

## 它是什么

传统的防病毒保护以病毒的实际代码或签名为基础。与之相反，病毒遏制则建立在与正常代码之间存在差异的恶意代码的行为基础之上。病毒遏制以如下观察结果为基础：即在正常活动的情况下，计算机很少会连接新的计算机，而是比较可能有规律地连接同样一组计算机。这与快速扩散的蠕虫的基本行为正好相反，蠕虫总是试图连接新的计算机。例如，通常计算机每秒钟大约进行一次连接，而SQL Slammer病毒每秒钟则要设法感染800多台计算机。

病毒遏制技术的精髓就是对连接的新计算机施加一个速度限制，以便正常的流量保持不被感染，而试图以超过允许的速度扩散的可疑流量则被遏制。这样就会产生大量及易被检测到的积压的连接请求。病毒一经遏制并检测到之后，技术人员和系统管理员就有了进行干预所需的时间，以便将病毒从系统上清除，隔离和根除计算机受到的威胁。

这种方法和签名与补丁方法有以下三方面的不同：

1. 以病毒的网络行为为重点，防止某些类型的行为 — 尤其是每秒钟试图大量向外连接的行为。
2. 并非阻止病毒进入系统，而是限制代码离开，这一点也与其它方法有很大的区别。
3. 由于在可配置的时间段内可以阻塞超过允许速度的连接，系统容许误报，从而保证系统更为稳健。

病毒遏制技术无意取代基于签名的解决方案，而是要与其互为补充。病毒遏制填补了防病毒保护技术上的一项空白，即以前的防病毒机制不能控制没有补丁的未知病毒的破坏。应用病毒遏制后，以前未知的病毒威胁就会减轻，从而为管理员部署对付进一步攻击的签名更新和补丁争取时间。

## 快速检测、及时阻止

在英国Bristol惠普实验室<sup>2</sup>进行的病毒遏制技术测试显示，病毒遏制能够非常迅速地检测和阻止蠕虫从感染的计算机上扩散。例如，遏制技术能够在1秒钟内阻止W32/Nimda-D蠕虫扩散。

由于遏制技术阻止了随后的感染，因此对病毒全球性扩散的影响取决于在多大范围内部署病毒遏制技术。惠普实验室的测试结果表明，只需在50%的计算机上采用病毒遏制技术就可大大减少蠕虫及其变种在全球的扩散。即使被感染，被遏制的机器也不会产生任何网络流量，从而可大幅度减少由于病毒所产生的网络流量。

## 病毒遏制技术的优点

病毒遏制技术的优点包括：

- 无需对病毒有任何了解。因为它通过病毒的行为而不是通过确定病毒代码来启用的，因此无需等待签名更新即可处理未知的病毒
- 通过减慢或阻止路由流量进入具有高连接速度的主机来保护网络基础设施架构。即使受到病毒的攻击，基础设施架构也能保持正常运转
- 当发现类似蠕虫的行为时，提供事件日志和SNMP陷阱警告
- 在问题升级成灾难之前，IT人员有时间做出反应
- 如果得到广泛部署，病毒遏制将使病毒难以扩散

---

<sup>2</sup> “病毒遏制技术的实施及测试”，Jamie Twycross和Matthew M. Williamson合著，惠普实验室，2003年3月3日

## 它如何工作

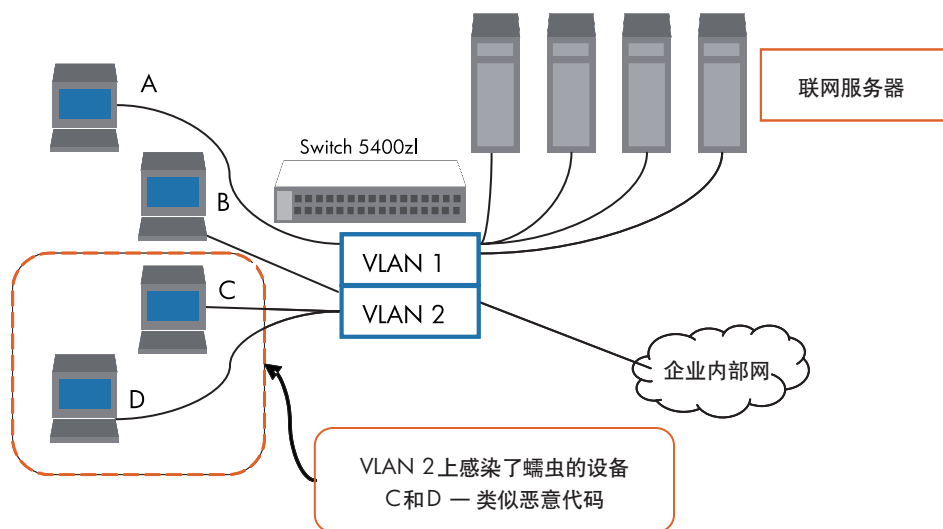
病毒遏制通过截取各种类型的 IP 连接请求，即源子网和目标地址不同的连接，发挥其作用。这种方法适用于最常见的第 4–7 层会话和应用协议，包括 TCP 连接、UDP 包、SMTP、IMAP、Web 代理、HTTP、SSL 和 DNS — 事实上正常流量看起来不像病毒扩散的任何协议。

(NetBIOS 和 WINS 等部分协议不适合病毒遏制，因为它们启动的广泛网络流量脉冲，可能会被病毒遏制技术误认为是威胁。同样，产生似乎可疑但无害的短期流量的应用程序 — 例如网络管理扫描程序、通知服务和部分点对点文件共享 — 也不适合病毒遏制。)

病毒遏制跟踪最近建立的连接数量。如果截取的新请求是面向最近建立了一个连接的目标，则正常处理这个请求。如果请求是面向最近没有连接的目标，则只在最近连接的数量低于预先设定的阈值时才处理该请求。这个阈值限定在一定时间内允许多少个连接，以此实施连接速度限制。如果超过阈值，而请求以不同寻常的高速度进入，那么它将被视为是病毒。这时，病毒遏制将停止处理请求，从而另行通知系统管理员。

在图 1 中，VLAN 2 上的设备 C 和 D 被感染，并呈现受病毒攻击的高连接速度的特征。ProCurve Switch 5400zl 系列上的病毒遏制技术可保护设备 A、B、联网服务器和企业内部网免受被感染的设备 C 和 D 的冲击。

图 1: VLAN 之间的病毒遏制步骤



## ProCurve 交换机上的连接速度过滤

在 ProCurve 系列产品中，ProCurve Switch 3500yl、5300xl、5400zl 和 6200yl 通过连接速度过滤特性来实施病毒遏制技术。这一特性可通过以上交换机上某一端口启用。但是，对于 Switch 5300xl 系列产品来说，只有当它处于路由模式时才能实施病毒遏制功能。而 Switch 3500yl、5400zl 和 6200yl 系列产品无此种限制，它们在处于路由或桥接模式时均可实施病毒遏制功能。

### 过滤选项

默认配置下禁用连接速度过滤。在某个端口上启用后，连接速度过滤监视流入的路由流量中是否有来自该端口上任何给定主机的高连接速度请求。如果主机表现出与蠕虫类似的在短时间内试图建立大量对外 IP 连接(目标地址)的行为，根据连接速度过滤的配置，交换机就会以下列方式之一做出响应：

- **只通知潜在的攻击：**当显而易见的攻击持续进行时，交换机生成确定侵入主机的源地址(SA)的事件日志通知和(如果交换机上配置了陷阱接收器)类似的 SNMP 陷阱通知
- **通知并减少扩散：**在这种情况下，交换机在“惩罚”期间内临时阻塞来自侵入主机 SA 的流入路由流量，并生成此措施的事件日志通知和(如果交换机上配置了陷阱接收器)类似的 SNMP 陷阱通知。当惩罚到期时，交换机重新评估来自该主机的路由流量，如果明显的攻击仍然持续，则继续阻塞这个流量。(在重新评估期间，允许来自该主机的路由流量。)
- **阻塞扩散：**该选项在交换机上阻塞主机流量的路由。当阻塞发生时，交换机生成事件日志通知和(如果交换机上配置了陷阱接收器)类似的 SNMP 陷阱通知。这时，系统人员必须明确地重新启用以前被阻塞的主机

### 灵敏度和应用选项

所有支持病毒遏制技术的 ProCurve 交换机均包含一个全局灵敏度设置，用以调整连接速度过滤的能力，进而检测来自给定源地址的相对高连接速度实例。

一般而言，正常的网络流量与恶意代理程序产生的流量截然不同。但是当合法的网络主机在短时间内产生多个连接时，连接速度过滤可能产生“误报”，并将该主机作为被感染的客户机处理。降低灵敏度或改变过滤模式可以减少误报的数量。反之，降低过滤和灵敏度配置级别则会削弱交换机在攻击早期检测蠕虫产生流量的能力，因而应当对此进行认真的调查和规划，以确保不产生易受攻击的危险。另外，系统管理员还可以使用连接速度 ACL (访问控制列表)或有选择地启用允许高速度的合法流量。

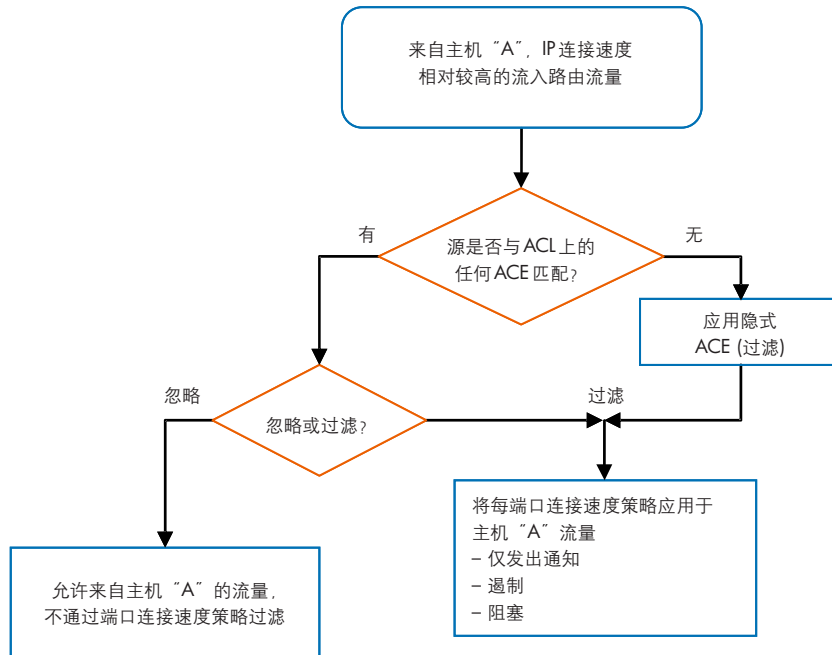
**选择性启用。**该选项只将连接速度过滤应用于存在很大攻击风险的端口。对于一定程度上不容易受到攻击的端口，配置连接速度过滤可能没有多大的用处。

**连接速度 ACL。**如上所述，基本的连接速度过滤策略按端口配置为仅发出通知、遏制和阻塞。连接速度 ACL 由一系列访问控制项(ACE)组成，并通过为各个主机、主机组或整个子网创建特殊的规则，来为该端口策略创建例外。因此，系统管理员可以调整连接速度过滤策略，创建并应用在 VLAN 端口上已配置过滤器的例外。

如果系统管理员需要从连接速度过滤策略中排除合法的高速度流入流量，那么连接速度 ACL 则可派上用场。例如，响应网络需求的服务器可能会发送数量相对高的合法连接请求。其行为就与蠕虫的连接速度升高行为一样，从而可能产生误报。连接速度 ACL 对此服务器应用例外的处理将允许管理员从连接速度过滤中排除这台可信服务器，从而使该服务器能够持续运行。

图2所示为支持病毒遏制技术的ProCurve将ACE列表应用于高速度流入流量，以确定是否忽略它并允许其进入VLAN，或者是否过滤并实施连接速度过滤与通知、遏制或阻塞(按照管理员的预先设置)时采用的逻辑程序。除非专门排除，否则作为一项新的安全性措施，与经过核准的ACE匹配的事件流量将被隐式过滤。

图2：通过给定端口将连接速度ACL应用于流量



## ProCurve Manager Plus

ProCurve Manager Plus是ProCurve最重要的“中心命令”网络管理软件，也是ProCurve Networking 适应性边缘架构™的一个重要组件。管理员可以使用ProCurve Manager Plus软件接收来自ProCurve交换机连接速度过滤器的报警，并实施关闭端口的决定以对检测到的威胁做出响应。ProCurve Manager Plus采用病毒遏制技术使其可以继续成为网络管理的一体化命令中心，正如管理员将病毒遏制技术加入企业安全库一样。此外，ProCurve Manager Plus提供的病毒遏制响应还超过了ProCurve交换机单独所能实现的水平，包括关闭攻击端口的功能。

### 配置原则

ProCurve交换机如要应用连接速度过滤器，就必须首先配置IP路由和有成员端口的多个VLAN。系统管理员可以对相对不受攻击的网络采用一种方法，而对高风险网络则采用另外一种方法。下面总结了管理员配置交换机进行连接速度过滤的步骤。

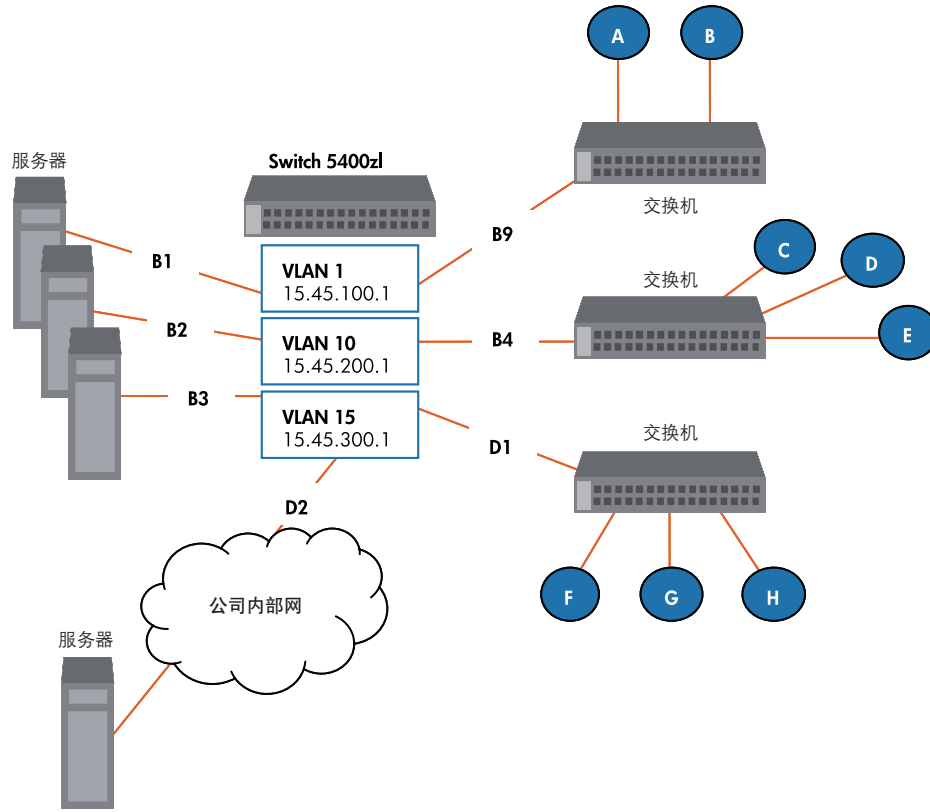
#### 对于相对不易受攻击的网络

当网络相对不易受攻击时，网络管理员可以将ProCurve交换机连接速度过滤器上的全局灵敏度设置为低级。通过监视事件日志和SNMP陷阱接收器(如果可用)，管理员可以确定连接速度高的主机。如果这个高速度行为是合法活动——例如高负荷使用的服务器——那么管理员可以配置连接速度ACL，为可信主机建立策略例外处理规则。这时，连接速度过滤器的灵敏度可以提高到中级，再次对网络进行监视。

### 对于看起来存在较大攻击危险的网络

对于有可能受到攻击威胁的网络，连接速度过滤步骤包括管理具有高连接速度的主机。这样可以使未受感染的主机获得较高的网络性能，同时帮助确定可能需要更新或补丁，以消除恶意代码的主机。例如，建议管理员将所有端口的连接速度过滤设为“遏制”，全局灵敏度设为中级。应当按上面的说明监视事件日志和SNMP陷阱，以确定具有高连接速度的主机。如果要立即停止来自特定主机或子网的攻击，管理员应在相应的端口上使用端口阻塞模式。在情况得到控制之后，管理员可以使用连接速度ACL更有选择性地管理流量，允许接受来自可靠主机的正常路由流量。

图 3: 基本网络配置



例如在上面的图 3 中，管理员可以选择

- 遏制来自 B1-3 端口、有可能存在恶意的高速度流量
- 对于连接 B4 的比较安全的源 C、D 和 E 的高速流量，仅发出通知响应
- 立即阻塞来自具有潜在高风险地点的高速度流量，例如公司内部网，通过端口 D2 进入 VLAN
- 使用 ACL 允许从源 F、G 和 H 发起的已知合法的高速度流量进入端口为 D1 的 VLAN

# ProCurve 交换机上的 ICMP 速率限制

## 什么是速率限制

网络威胁并不经常以病毒或蠕虫的方式出现。例如，其他具有危险性的威胁——称之为“拒绝服务(DoS)”——就不是病毒，而是攻击者所采用的一种方法，用于防止(拒绝)合法的用户访问网络或主机。实施DoS攻击的有效方法之一是利用ICMP流量。在IP网络中，ICMP消息是为响应路由和诊断功能的查询或请求而生成的。这些消息定向到发起这些查询的应用。在异常情况下，如果这些消息是为了让网络线路过载而快速生成的话，就有可能威胁到网络的可用性，导致拒绝服务。

这一问题在Smurf攻击等DoS攻击中更为明显，攻击者向IP广播地址发送大量ping包(ICMP回应请求)，它们拥有受害者的侦听源地址。当广播域上所有主机以指向这个受害主机的ICMP回应响应这个ping请求时，可能导致拒绝服务。ICMP流量还可能被病毒和蠕虫利用，作为发现目标网络上活动主机的起点。W32.Welchia.蠕虫<sup>3</sup>是通过ICMP回应请求发现活动主机的典型病毒代表。

在ProCurve Switch 3500yl、5300xl、5400zl和6200yl系列产品中，用于传输ICMP流量的带宽可通过ICMP速率限制功能加以控制。这一功能允许用户将ICMP流量限制在不影响所需功能的水平，并遏制由于基于ICMP的DoS攻击或蠕虫或病毒而引起的过量ICMP流量，从而减缓蠕虫或病毒的蔓延，降低其负面影响。此外，它还为非ICMP流量保留带宽。

## ICMP 速率限制的影响

ICMP速率限制仅允许端口上的一部分入站带宽用于传输ICMP流量。因此，它可为非ICMP流量保留入站带宽，而端口或链路汇聚将遏制任何由于蠕虫或病毒攻击(或其他原因)而产生的大量入站ICMP流量。注意，ICMP速率限制并不遏制非ICMP流量。当您需要遏制特定端口上的ICMP流量和其他所有入站流量时，您可以配置ICMP速率限制和所有流量速率限制功能。

## ICMP 速率限制的操作

ICMP速率限制在接口(每个端口或每个链路汇聚)上运行，应将其配置成允许预期的最高合法入站ICMP流量。如果某个接口的入站ICMP流量超过配置的极限，交换机就会遏制该流量，并生成日志消息和SNMP陷阱(如果配置了SNMP陷阱接收器)。例如，如果100 Mbps端口协商出一条100Mbps的交换机链路，ICMP速率限制配置为5%，则通过该端口的入站ICMP流量限制为5 Mbps，其它任何额外ICMP流量都将被遏制。

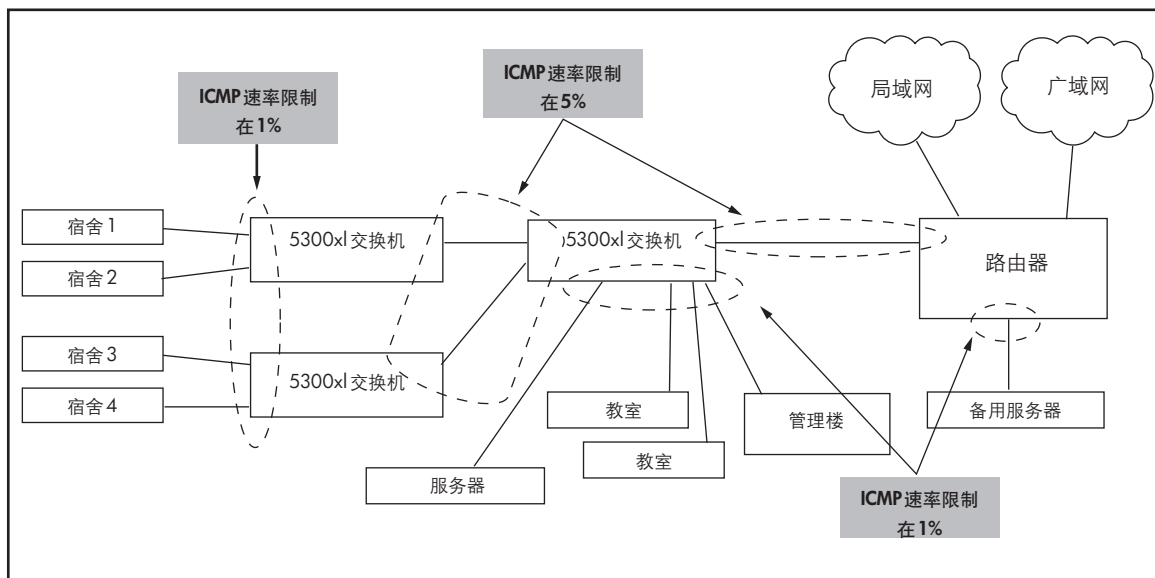
## 网络应用

在交换机的所有已连接端口上应用ICMP速率限制，用于有效遏制来自任何源的过量ICMP消息。在边缘端口上，ICMP流量应为最少，它的阈值应为可用带宽的1%，这对大多数应用来说已足够。在中心端口上，如交换机到交换机和交换机到路由器，5%的最大阈值对正常的ICMP流量来说已足够。(“正常”ICMP流量应为网络重启时的最大ICMP流量)

---

<sup>3</sup> <http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html>

图 4: ICMP 速率限制



## 总结

传统的病毒、蠕虫及其它恶意代码的处理方法依靠签名和补丁。因此，在编写并部署保护代码前，系统易于遭受以前未知的病毒威胁。当病毒的扩散速度超过以往，产生的流量经常导致网络瘫痪时，这种方法很显然就会失效。

与此形成鲜明对照的是，惠普实验室开发的病毒遏制技术将重点放在恶意代码的行为，而非其内容上，从而可以确定并响应以前未知的威胁。该项技术主要是阻止此类代码在 VLAN 上扩散，从而可以消除巨大的网络流量，而这样的流量正是此类代码最具破坏性的方面之一。病毒遏制非常有效，例如在测试中，能够在 1 秒钟之内阻止 W32/Nimda-D 病毒的扩散。

目前，ProCurve Switch 3500yl, 5300xl, 5400zl 和 6200yl 系列产品都实施了基于病毒遏制技术的连接速度过滤。系统管理员可以对该项技术进行配置，遏制(减缓)或完全阻塞可疑流量，或者只是通知管理员存在潜在的威胁。他们可以有选择地应用 ACL，允许共享恶意代码的高速度配置文件的已知合法流量正常地通过基础设施架构。在任何情况下，管理员都可以配置该技术，通过人工来决定阻塞哪些流量、允许哪些流量通过。连接速度过滤通过减缓或阻塞可疑流量使管理员有时间采取措施，为保护当前的网络提供了一个重要的工具。

欲了解有关 ProCurve Networking  
产品和解决方案的更多信息，  
请访问：

[www.hp.com.cn/network](http://www.hp.com.cn/network)

欲知详情，请电话垂询当地惠普销售办事处或离您最近的惠普授权经销商。

惠普售前支持热线： 800-820-2255  
惠普售后支持热线： 800-810-3888  
惠普客户反馈/投诉热线： 800-810-0039

或请访问：[www.hp.com.cn](http://www.hp.com.cn)  
[www.hp.com.cn/network](http://www.hp.com.cn/network)



© 2007 Hewlett-Packard Development Company, L.P. 本文所含信息如有更改，恕不另行通知。  
惠普产品与服务的全部保修条款在此类产品和服务附带的保修声明中均已列明。本文中的任何信息均不构成额外的保修条款。惠普对于本文中所包含的技术或编辑错误、遗漏概不负责。

P/N: 4AA0-0662CHP, 2007年6月中国印刷