以太网中交换设备安全性能主要技术分析与对策

钟代军　米利波
（重庆文理学院教育技术中心　重庆永川 402160）

摘　要　交换设备的安全特性直接影响着网络的安全稳定运行和网络的服务质量，无论是传统的交换设备还是目前广泛运用的交换设备都存在着一些安全隐患。本文分析了交换设备的安全性能和交换机数据处理过程中的缺陷和问题，提出了提高交换设备性能和加强交换设备安全的新思路。

关键词　交换机，网络安全，网络系统，体系结构

Analysis and Countermeasure on the Main Technology of Switch Facility's Security Capability in Ethernet

ZHONG Dai-Jun　MI Li-Do
(Modern Education Technology Center, Chongqing University of Arts and Sciences, Yongchuan Chongqing 402160)

Abstract　The security speciality of switch facility can influence the security, stability and the service quality of network directly. The hidden trouble exists in both the traditional switch facility and the one which is widely used nowadays. This paper analyzes the security capability of switch facility, the disfiguration and problem in data processing, then puts forward the new thoughts of improving switch facility's security capability and strengthening it's safety.

Keywords　Switch facility, Security of network, System of network, Systematic structure

1　引言

网络安全不再单纯依赖单一设备和单一技术来实现，已成为业界共识。IP网络上高度灵活性和扩展性丰富的应用，成为了IP网络的安全软肋之一。系统软件、应用软件、网络设计等方面的漏洞和错误致使病毒泛滥，攻击行为成灾。交换设备作为网络骨干设备，自然也肩负着构筑网络安全防线的重任。传统的安全保障体系和方法面对今天的网络问题显得有些苍白无力，更多的设计者、技术人员开始认识到必须完善和加强网络设备的安全性，才能真正保证网络的安全稳定运行。传统的网络交换设备存在什么问题？网络安全的关键因素是什么？如何针对这些安全因素来改进交换设备？这些问题都值得我们广泛讨论和深入研究。

1　传统交换网络设备安全性能分析

作为网络主要设备的交换机在安全方面的技术主要体现在以下两个方面。

(1)系统层面：在网络架构中实现了安全机制，即对网络管理信息进行加密、控制。这主要体现在交换设备传递信息的全过程。

(2)用户层面：采用了安全接入机制，如RADIUS/TACACST、安全套接层（SSL）、流量控制（Flow Control）、WRR(Weighted Round Robin)、带宽控制、MAC地址检验、各种类型虚网技术以及部分交换机支持的802.1X端口认证等。

但是，在以病毒和攻击行为为核心的网络安全保障体系中，传统交换机却主要依靠以下几方面来实现安全防护：ACL、QoS、RADIUS/TACACST以及802.1X端口认证。然而这些技术在实际网络实施之后我们取得的成效如何呢？

当我们启用安全体系中的核心技术ACL后，常规的策略限制访问能够实现。但是，当我们出现类似于2003年肆虐的"冲击波"病毒的情况时，就会出现网络设备由于CPU利用率过高，基本无法正常运行，频繁发生设备死机现象，用户只有通过重启交换路由设备、重新配置访问控制列表才能消除蠕虫病毒对网络设备造成的影响。再则，对于病毒和攻击的防护，即便是交换设备CPU利用率没有影响，但是多端口千兆数据转发时，根本无法达到线速，致使高带宽的内网通信也不能流畅完成。

当启用RADIUS/TACACST协议进行安全接入时，RADIUS协议本身并不十分占用带宽，并且在WAN链路上可以工作得很好。但是，在IAS服务器与域控制器（包含用于确定网络访问的用户和组）之间拥有高性能的连接很重要。而IAS服务器与域控制器却与交换设备连在一起，它们之间的线速转发也是很难实现的。

QoS的实施：但总体上，目前交换设备上QoS的实施还很粗糙，还不能完全解决IP网络中很多问题。比如，如何提供业务端到端的QoS、如何管理全网QoS策略、如何动态调整QoS等，良好的QoS实现无疑依赖于交换网络中线速转发实现的高带宽。

我们要解决目前以太网中的安全问题，就得先了解作为网络主要设备交换机的数据处理方式。

2　交换机数据处理问题分析

交换机对于二层数据的处理采用硬件方式实现，一般说来在二层数处理中效率很高。但交换机在对三层数据、QoS，以及ACL和组播的处理方式，总是交换新产品更新与技术研究的一个重要领域，一次次在三层数据、QoS以及ACL和组播的数处理方式的改进，也使交换的性能得到进一步提高。

钟代军　硕士生，实验师，主要研究方向：教育技术；**米利波**　硕士生，实验师，主要研究方向：计算机网络。

这个过程简单说来经历了三个阶段。

软件式处理：这种方式是软件直接通过 CPU 实现交换的主要安全防护技术，但这种方式效率极低，每秒包转发只能达到 k 级别。在目前高密度端口，高流量的需求环境已不再适应。

基于 ASIC 芯片集中式储备和发出：由于软件式处理方式的低效率，基于 ASIC 芯片的硬件处理方式应运而生。由于三层数据转发、QoS、ACL 和组播通过单独的 ASIC 芯片来实现，交换的性能每秒包转发可以达到 M 级别。

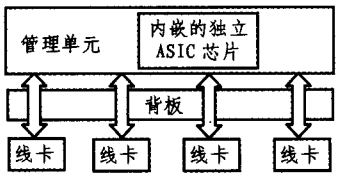

图 1

这种基于单个 ASIC 芯片的技术虽然在一定程度上提高了交换机性能，但用户流量和数据类型的复杂程度日益增加，单独的 ASIC 芯片也无法满足实际需求。

第三阶段：分布式硬件处理阶段

针对集中式硬件处理模式下整机只有单个 ASIC 芯片的设计缺点，为了提高交换机整体性能，后来发展为在每个用户线卡上都配备自己独立的 ASIC 芯片，线卡当地可以提供“统一硬件查询表”，负责自己线卡所有端口的 L2/L3/ACL/QOS/组播等功能实现，这种设计方式即为分布式硬件处理方式。这种处理方式可使交换机的性能每秒包转发可以达到 100M 级别，这是目前的交换机厂商通常采用的方式。

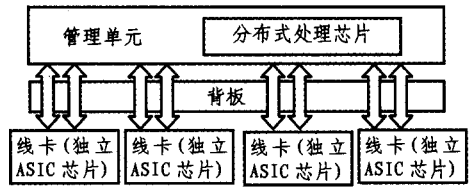

图 2

很显然这种方式虽然极大地提高了交换机性能，但对硬件的统一查询却使交换性能受到了限制。

根据以上设计的问题与弊端，可以采用以下的新思路来解决。

3 新的解决思路

3.1 针对 ACL 和 QoS 的独立处理模块

针对 ACL 和 QoS 的数据处理行为是能很明晰判断的，而基于 ACL 和 QOS 产生的数据流量是很大的，因此可以针对 ACL 和 QoS 单位增加一个快速过滤处理器。

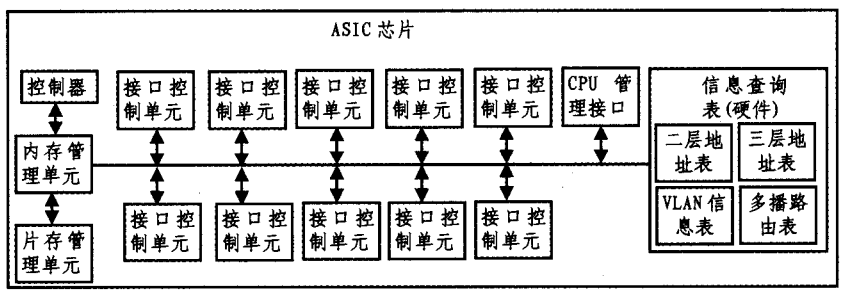

图 3 分布式硬件处理阶段线卡 ASIC 芯片

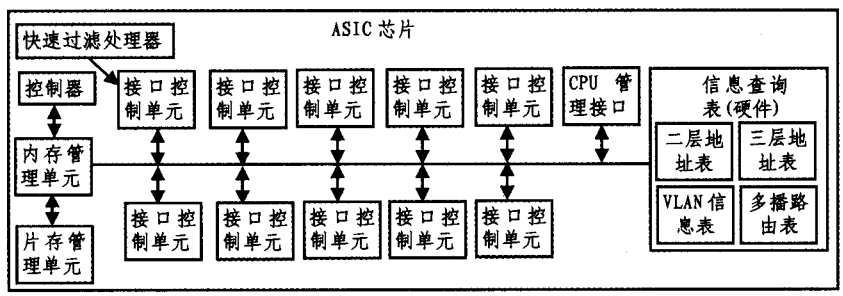

图 4 基于 ACL 和 QoS 分布式硬件处理阶段线卡 ASIC 芯片

基于 ACL 和 QoS 快速过滤处理器的设计思想，是从独立的端口角度将特殊数据单独交予快速过滤处理器处理，克服了目前大多数交换产品因病毒和攻击原因而出现的问题。基于 ACL 和 QoS 的设置，致使交换设备 CPU 负载过高而带来设备死机和网络拥塞。这种设计思想减轻了系统和线卡的压力，提高了系统稳定性，保证了整机线速的处理能力。

3.2 交换机体系结构方面

交换机的体系结构直接影响交换机的性能，目前主要有以下几种技术：

通用 CPU 具有易扩展性优点，理论上可以实现任何网络功能。但加装通用 CPU 的第三层交换机，以及基于网络处理器的系统，在实际的应用中只能完成简单的流量交换功能。如果进一步处理在网络会话建立时的数据包的内部信息，就要求能识别每个会话的每个数据包的内部，结果必然是严重的延迟和性能低下。依靠通用 CPU 的交换机体系结构，不能实时调动运算能力来完成交换任务，很快成为一个新的瓶颈，所以，在交换机的体系结构设计中，通用 CPU 一般仅用于网络设备的控制和管理。

ASIC 芯片可以将需要许多芯片完成的工作集成到一个单独的、体积更小、速度更快的模块上，以减少制造和支持费

用，同时提高了使用 ASIC 设备的速度。ASIC 技术现在已经非常先进，许多传统上需要由软件完成的功能，现在都可以迁移到 ASIC 上。但是 ASIC 芯片一经生产出来就很难再扩展，这是 ASIC 芯片最大的问题。所以 ASIC 芯片适合应用于处理网络中的各种成熟传统功能。

FPGA 的可编程特性带来了电路设计的灵活性，可以在一定程度上灵活地扩展业务处理类型。但 FPGA 能力还是非常有限的，近期推出的高处理能力的 FPGA 也没能解决大规模成熟应用。协调处理多种协议的问题，使得 FPGA 不能更广泛地应用于交换机体系结构中，所以 FPGA 一般用于简单协议扩展。

NP 网络处理器是面向数据分组处理的、具有特定电路的软件可编程器件。它将 RISC 处理器的低成本、灵活性与 ASIC 专用网络处理芯片的高性能、可扩展性很好地结合在一起，提供了适应网络发展的能力。但是 NP 需要统一标准。因为不能统一标准，所以无法使成果共享。同时，NP 技术设计实现本身很复杂，所以 NP 的广泛运用还有一段时日。

因此，采用 NP+ASIC 的体系设计结构应该说是目前最好的思路。NP+ASIC 的体系结构很好地满足了业务按需叠加、业务和性能并重的现代核心交换机设计需求。NP 针对数据分组处理，采用优化体系结构、专用指令集、硬件单元，满足高速数据分组线速处理要求；具有软件编程能力，能够迅速实现新的标准、服务、应用，满足网络业务复杂多样化需求，灵活性好；设备具有软件升级能力，满足用户设备硬件投资保护需求使用。ASIC 芯片高速处理各种传统的业务，如二层交换、三层路由、ACL、QoS 以及组播处理等等，满足核心交换机对于交换机处理性能的需求；而利用 NP 实现各种非传统或未成熟的业务，根据需要灵活支持 IPV6、Load Balancing、VPN、NAT、IDS、策略路由、MPLS、防火墙等多种业务功能，满足核心交换机对于业务按需叠加的需求；同时，NP 接近 ASIC 的高效特性，又保障了多业务提供的高性能，依然保持了核心交换机对于强大处理能力的需求。

3.3 交换机与 IDS 联动

传统的 IDS 系统一直备受争议，过高的误报、漏报使 IDS 成为“网络中最大的安全隐患”，降低 IDS 误报漏报率一直成了传统 IDS 的努力方向。其本质原因在于它各种检测机制过于简单，同时不能主动防护，使得 IDS 系统效率极其低下。

在目前，智能交换机与 IDS 的联动是一个非常实际而且不会给用户带来额外投资的理想方案。IDS 与网络交换设备联动是指交换机在运行过程中，将各种数据流的信息上报给安全设备，IDS 系统可根据上报信息和数据流内容进行检测，发现网络安全事件的时候进行有针对性的动作，并将这些对安全事件作出反应的动作发送到交换机上，由交换机来实现精确端口的关闭和断开。

3.4 核心交换机的 CrossBar 技术

随着核心交换机的交换容量从几十 Gbps 发展到今天的几百 Gbps，核心交换机也从共享总线、共享内存的方式发展到今天的 CrossBar 结构。

CrossBar(即 CrossPoint)被称为交叉开关矩阵或纵横式交换矩阵，它能很好地弥补共享内存模式的一些不足。其优势表现在以下几个方面：

首先，CrossBar 的实现相对简单。共享交换架构中的线路卡到交换结构的物理连接简化为点到点连接，实现起来更加方便，从而更加容易保证大容量交换机的稳定性。

其次，CrossBar 内部无阻塞。一个 CrossBar 的示意图如图 5 所示，只要同时闭合多个交叉节点(CrossPoint)，多个不同的端口就可以同时传输数据。从这个意义上，我们认为所有的 CrossBar 在内部是无阻塞的，因为它可以支持所有端口同时线速交换数据。

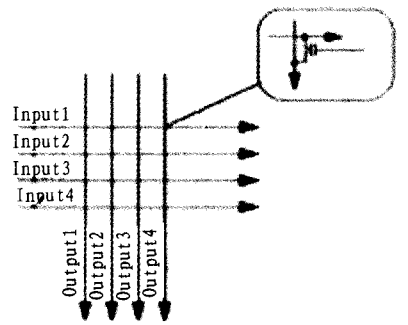

图 5

在支持 CrossBar 技术的三层交换机中，一般采用了两类三层交换芯片：一类是可以出千兆、百兆端口的交换芯片；一类是仅仅出内部高速接口(往往是 10G 以上的速率)的 CrossBar 芯片，用于各个模块之间的互联。Crossbar 交换网络在数据平面没有任何瓶颈。这正是因为 Crossbar 引入了交换矩阵这种新的交换方式，摒弃了共享带宽的交换方式，在数据交换方式上是一种革命性的变化。Crossbar 交换网的扩展能力非常强，交换容量可以做得很大，基本不受硬件条件限制。目前单颗芯片交换容量在 256G～700G 之间，多颗芯片可以构建 T 级乃至几 T 容量的大型交换网络，足以满足当前和未来几年网络对交换容量的需求。并且，随着硬件集成技术的进步，单颗 Crossbar 芯片支持的容量会更大。Crossbar 交换结构的大容量和强大的扩容能力正是高端设备首选这种结构的原因，这种交换结构极大地提高了高端设备的容量和未来的扩展能力，并且 Crossbar 交换结构具有良好的 QoS 保障机制，如仲裁、低时延、按端口按优先级的流控功能。值得一提的是，与共享缓存相比，Crossbar 的交换时延几乎可以忽略不计。图 6 为 Crossbar 交换结构图。

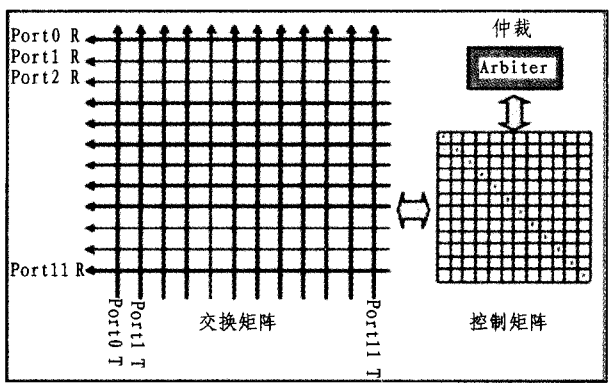

图 6

在今后的核心交换机技术发展中，分布式 Crossbar 设计应该是一个很好的方向，CPU 也采用分布式设计。设备主控板上的主 CPU 负责整机控制调度、路由表学习和下发；业务板从 CPU 主要负责本地查表、业务板状态维护工作。这就实现了分布式路由计算和分布式路由表查询，大大缓解主控板的压力，提高了交换机转发效率，这也是业务板本地转发能够

提高效率的重要原因。这种分布式 Crossbar、分布式交换的设计理念是核心网络设备设计的发展方向，保证了现在的网络核心能支撑未来海量的数据交换和灵活的多业务支持的需求。

以太网交换机实际是一个为转发数据包优化的计算机。只要是计算机，就有被攻击的可能，比如非法获取交换机的控制权，导致网络瘫痪，另一方面也会受到攻击。传统交换机主要用于数据包的快速转发，强调转发性能。随着局域网的广泛互连，加上 TCP/IP 协议本身的开放性，网络安全成为一个突出问题，网络中的敏感数据、机密信息被泄露、重要数据设备被攻击，而交换机作为网络环境中重要的转发设备，其原来的安全特性已经无法满足现在的安全需求，因此传统的交换机无论是结构体系还是软件系统都需要增加安全性。

参 考 文 献

1 楚政. 以太网交换技术及发展[J]. 电信科学，2003(5)
2 安学军，张佩珩，高文学，等. 基于 UX8 交换芯片的机群互连网络设计[J]. 微电子学与计算机，2003(7)
3 张磊. 基于消息队列的自治异构信息查询系统的研究与实现[D]. 国防科学技术大学，2003
4 毕汝超. 以太网交换机 EAPS 系统的设计[D]. 西北工业大学，2007
5 郑燕峰. 基于输入排队的可扩展交换结构调度算法的研究[D]. 中国科学院研究生院(计算技术研究所)，2006
6 荆元利. 基于片上网络的系统芯片研究[D]. 西北工业大学，2005
7 林闯，单志广，盛立杰，等. Internet 区分服务及其几个热点问题的研究[J]. 计算机学报，2000(4)

(上接第 33 页)

"变长帧"在交换前、后的分割与重组，EPFTS 直接采用以定长帧 EPF 作为基本交换单元。EPFTS 的"交换时槽"(Timeslot)为交换结构转发一个 EPF 所需时间，对输出波长的复用则以该波长上传输单个 EPF 所需的时间为"复用时槽"对该波长的传输能力进行复用，收发双方以 EPF 为基础进行异步传输，以避免频繁的时钟同步[14, 20]。图 2 为 EPF 帧格式示意图：

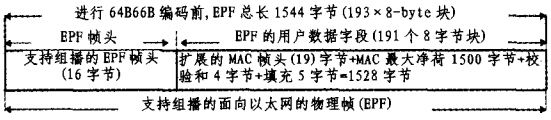

图 2 支持组播的面向以太网的物理帧格式

如图 2 所示，EPF 的载荷选择为以太网 MAC 帧的最大长度，即 1523 字节(不包括前导 7 字节)。为了适应采用 64B66B 编码以 8 字节为基础的数据块编码的需要，增加了 5 字节的填充字段，使 EPF 的用户数据字段为 1528 字节(191 个 8 字节块)。这样可以避免像 MEF 建议的 MAC in MAC 技术那样需要对被承载的 MAC 帧进行分割。EPF 的 16 字节的帧头中定义了超前交换字段、多端口组播字段以及其他控制字段。

SUPA 的 U-Platform 为用户数据提供"交换虚线路"(VSL - Virtual Switched Line)或"永久虚线路"(VPL - Virtual Permanent Line)服务[17]。对实时性要求高的单个数据流，EPFTS 可对单个数据流建立 VSL，提供可保障服务质量的 VSL"集成服务"；对服务质量要求相对较低的数据流，可为服务质量需求类似的多个数据流建立一个 VSL，为用户提供类似于"区分服务"的统计复用服务，以减少交换节点的 VSL 数量；对传统 Internet 能满足的数据传输业务(如文本业务)，可在多对边界节点对间建立若干 VLS 隧道(Tunnel)，供多个数据流共享，提供"尽其所能"的服务。VSL 是在 S&M-Platform 上通过服务质量协商协议(QoSNP)和基于 QoS 的波长路径选择算法来建立的。

物理层的 VSL 配合组播功能，很容易被用来构建虚拟专用网(VPN)，有助于提高 SUPANET 用户平台的安全性。

结束语 有关 NGI 和 NGN 的研究是一个长期的探索过程。尽管有关 SUPA 和 EPFTS 的研究工作仍处于前期阶段，但我们的仿真实验结果初步表明这一研究路线具有较强的可行性和进一步研究的价值。由于充分考虑了保护在 Internet 上的投资问题，较容易实现从 Internet 向 SUPANET 的平滑过渡。

参 考 文 献

1 GENI Design Documents (GDD), 2005 -2007. http://www.geni.net/documents.php
2 RFC 2205 - Resource Reservation Protocol (RSVP) - Version 1 Functional Specification, IETF, Sep. 1997
3 RFC 3031 - Multiprotocol Label Switching Architecture, IETF, Jan. 2001
4 ZENG Huaxin, et al. Replace MPLS with EPFTS to Build a SUPANET. In: 2005 IEEE International Workshop on High Performance Switching and Routing (HPSR'05), Hong Kong, May 2005
5 ITU-T SG15, Recommendation G: 8110/Y. 1370: MPLS layer network architecture, Transport MPLS, February 2006
6 Chadha H. Capitalizing on the Evolution of Metro Nets: Understanding Multidimensional Ethernet, February 2006. http://www.convergedigest.com/bp-me/bp1.asp? ID=388&ctgy=
7 Bottorff P. PBT/D1.0 - General Discussion of Provider Backbone Transport in 802.1ah Networks, May 2006. http://www.ieee802.org/1/files/public/docs2006/ah-bottorff-pbt-v1-0506.pdf
8 Clark D, Wroclawski J, Sollins K, et al. Tussle in cyberspace-defining tomorrow's Internet. In: Proc. of SIGCOMM, 2002
9 Clark D, Sollins K, Wroclawski J, et al. Addressing reality: An architectural response to real-world demands on the evolving Internet. ACM SIGCOMM Computer Communication Review, 2003, 33(4): 247～257
10 Clark D. FARA: Reorganizing the addressing architecture. In: Proc. of the ACM SIGCOMM, 2003. 313～321
11 ZENG J Z, XU J, WU Y, et al. Service Unit based Network Architecture. In: Fan Pingzhi, Shen Hong, eds. Proc. of PDCAT2003. IEEE Press, 2003. 12～16
12 曾家智，徐洁，吴跃，等. 服务元网络体系结构和微通信元系统构架. 电子学报，2004, 32(5): 745～749
13 GDD-05-01—GDD-05-06, GDD-06-07—GDD-06-041. available at http://www.geni.net/
14 Zeng Huaxin, Dou Jun, Xu Dengyuan. Single physical layer U-plane Architecture (SUPA) for next Generation Internet. In: Comprehensive Report on VoIP and enhanced IP Communications Services. IEC Publications, 2004. 197～227
15 Zeng Huaxin, Xu Dengyuan, Dou Jun. Promotion of Physical Frame Timeslot Switching (PFTS) over DWDM. In: Annual Review of Communications by IEC Publications, 2004, 57: 809～826
16 王慧. SUPANET 节点内部访问接口(IAI)研究:[学位论文]. 西南交通大学，2006
17 DOU Jun, ZENG Huaxin, WANG Haiying. Single User-Plane Architecture and its QoS Provisioning Mechanisms in Signaling and Management (S&M) Planes. In: Proceedings of 5th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT2004), Singapore, December 2004. 429～440
18 赵君，高雨. SUPANET 中 QoS 协商流程的研究. 计算机科学，2004, 31(增刊)
19 王金兰. SUPANET 中基于服务质量的波长路径选择技术研究:[学位论文]. 西南交通大学，2006.5
20 XU Dengyuan, ZENG Huaxin, Li Ji, et al. Physical Frame Timeslot Switching (PFTS) in the Single User-Plane Architecture Network (SUPANET). In: Proceedings of 5th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT2004), Singapore, December 2004. 383～395