浅谈第四层交换机技术及应用[1] PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/205/2021_2022__E6_B5_85_E8_B0_88_E7_AC_AC_E5_c101_205595.htm 随着百兆、千兆，甚至万兆局域网的逐渐普及，宽带城域网，甚至宽带广域网的广泛应用，不管是Intranet、Extranet、还小区智能网，日益扩张的海量信息量，正迫使着人们对网络系统中的音频、视频、数据等信息的传输量的要求越来越高。 Internet的迅猛发展，电子商务、电子政务、电子贸易、电子期货等网络交易方式的采用，在加速物流、资金流周转的同时，也加速了信息急速骤增，给网络信息中心服务器增加了极大的压力，从而使普遍需要缓解网络核心系统压力的需求一浪高过一浪。为此，业界不得不开始考虑第四层交换概念了，以满足基于策略联网、高级QoS（Quality of Service：服务质量）以及其它服务改进的要求。巨大的市场潜力，又大大刺激了广大厂商在网络关键设备方面的重大投入，以至于在极短的时间内出现了从传统的第二层交换机，到技术先进的第三层交换机，再到近期推出的第四层，甚至第七层交换机产品的喜人局面。 第四层交换机区别时第三层交换机的是，它不仅应用了第三层交换机中的IP交换技术，更重要的是它站在更高层次上，可以查看第三层数据包头源地址和目的地址的内容，可以通过基于观察到的信息采取相应的动作，实现带宽分配、故障诊断和对TCP/IP应用程序数据流进行访问控制的关键功能。显然，第四层交换机在通过任务分配和负载均衡的同时，完全可以优化网络/服务器界面，提高服务器的可靠性和可扩充性，并提供详细的流量统计信息和记帐信息，从而在网络

应用层水平上解决网络拥塞、网络安全和网络管理等问题，使网络更具“ 智能 ”性和可管理性。 组建一个高速、宽带、稳定、可靠，且能融合安全与保密等全新需求的内外联网络系统，是当前企业网络发展的趋势。高速局域网的应用，已轻松地将语音、视频等对延时、抖动、丢包要求非常苛刻的通信类型集成在同一数据网上传输。来自企业网络内部的安全威胁，最理想的防范措施，往往是采取对不同用户的限权控制，杜绝非授权通信。勿容至疑，这些都要求我们有全新的局域网交换机支持。另外，从提高服务质量方面看，虽然我们有不断增添网络带宽这种有效而又简单的方法，但无论交换机的背板带宽有多高，无论交换机的数据包转发率有多大，无论数据传输率有多快，网络拥塞却永远存在于网络中。这从一个侧面告诉我们，没有服务质量控制，同样将意味着数据包可能丢失、延迟可能增加。 可见，工作在更高层次、支持质量服务、依靠软件运作和高层次管理的交换机，在现代企业网中具有多么重要的位置。下面我们就简单地介绍第四层交换机的相关性能、技术、应用领域和发展趋势。 一、 什么是第四层交换机 要想认识第四层交换机，先得对传统的第二层交换机和现在广泛应用的第三层交换机的基本工作原理和性能，有一些简单了解，只有通过比效，你才能真正鉴别第四层交换机。 众所周知，第二层交换机，是根据第二层数据链路层的MAC地址和通过站表选择路由来完成端到端的数据交换的。因为站表的建立与维护是由交换机自动完成，而路由器又是属于第三层设备，其寻址过程是根据IP地址寻址和通过路由表与路由协议产生的。所以，第二层交换机的最大好处是数据传输速度快，因为它只须识别数据帧中

的MAC地址，而直接根据MAC地址产生选择转发端口的算法又十分简单，非常便于采用ASIC专用芯片实现。显然，第二层交换机的解决方案，实际上是一个“处处交换”的廉价方案，虽然该方案也能划分子网、限制广播、建立VLAN，但它的控制能力较小、灵活性不够，也无法控制各信息点的流量，缺泛方便实用的路由功能。 第三层交换机，是直接根据第三层网络层IP地址来完成端到端的数据交换的。表面上看，第三层交换机是第二层交换器与路由器的合二而一，然而这种结合并非简单的物理结合，而是各取所长的逻辑结合。其重要表现是，当某一信息源的第一个数据流进行第三层交换后，其中的路由系统将会产生一个MAC地址与IP地址的映射表，并将该表存储起来，当同一信息源的后续数据流再次进入交换环境时，交换机将根据第一次产生并保存的地址映射表，直接从第二层由源地址传输到目的地址，不再经过第三路由系统处理，从而消除了路由选择时造成的网络延迟，提高了数据包的转发效率，解决了网间传输信息时路由产生的速率瓶颈。所以说，第三层交换机既可完成第二层交换机的端口交换功能，又可完成部分路由器的路由功能。即第三层交换机的交换机方案，实际上是一个能够支持多层次动态集成的解决方案，虽然这种多层次动态集成功能在某些程度上也能由传统路由器和第二层交换机搭载完成，但这种搭载方案与采用三层交换机相比，不仅需要更多的设备配置、占用更大的空间、设计更多的布线和花费更高的成本，而且数据传输性能也要差得多，因为在海量数据传输中，搭载方案中的路由器无法克服路由传输速率瓶颈。 显然，第二层交换机和第三层交换机都是基于端口地址的端到端的交换过程，

虽然这种基于MAC地址和IP地址的交换机技术，能够极大地提高各节点之间的数据传输率，但却无法根据端口主机的应用需求来自主确定或动态限制端口的交换过程和数据流量，即缺乏第四层智能应用交换需求。第四层交换机不仅可以完成端到端交换，还能根据端口主机的应用特点，确定或限制它的交换流量。简单地说，第四层交换机是基于传输层数据包的交换过程的，是一类基于TCP/IP协议应用层的用户应用交换需求的新型局域网交换机。第四层交换机支持TCP/UDP第四层以下的所有协议，可识别至少80个字节的数据包包头长度，可根据TCP/UDP端口号来区分数据包的应用类型，从而实现应用层的访问控制和服务质量保证。所以，与其说第四层交换机是硬件网络设备，还不如说它是软件网络管理系统。也就是说，第四层交换机是一类以软件技术为主，以硬件技术为辅的网络管理交换设备。 最后值得指出的是，某些人在不同程度上还存在一些模糊概念，认为所谓第四层交换机实际上就是在第三层交换机上增加了具有通过辨别第四层协议端口的能力，仅在第三层交换机上增加了一些增值软件罢了，因而并非工作在传输层，而是仍然在第三层上进行交换操作，只不过是对第三层交换更加敏感而已，从根本上否定第四层交换的关键技术与作用。我们知道，数据包的第二层IEEE802.1P字段或第三层IP ToS字段可以用于区分数据包本身的优先级，我们说第四层交换机基于第四层数据包交换，这是说它可以根据第四层TCP/UDP端口号来分析数据包应用类型，即第四层交换机不仅完全具备第三层交换机的所有交换功能和性能，还能支持第三层交换机不可能拥有的网络流量和服务质量控制的智能型功能。 二、第四层交换机支持哪

些重要技术 如上所述，第二层交换设备是依赖于MAC地址和802.1Q协议的VLAN标签信息来完成链路层交换过程的，第三层交换/路由设备则是将IP地址信息用于网络路径选择来完成交换过程的，第四层交换设备则是用传输层数据包的包头信息来帮助信息交换和传输处理的。也就是说，第四层交换机的交换信息所描述的具体内容，实质上是一个包含在每个IP包中的所有协议或进程，如用于Web传输的HTTP，用于文件传输的FTP，用于终端通信的Telnet，用于安全通信的SSL等协议。这样，在一个IP网络里，普遍使用的第四层交换协议，其实就是TCP（用于基于连接的对话，例如FTP）和UDP（用基于无连接的通信，例如SNMP或SMTP）这两个协议。由于TCP和UDP数据包的包头不仅包括了“ 端口号 ”这个域，它还指明了正在传输的数据包是什么类型的网络数据，使用这种与特定应用有关的信息（端口号），就可以完成大量与网络数据及信息传输和交换相关的质量服务，其中最值得说明的是如下五项重要应用技术，因为它们是第四层交换机普遍采用的主要技术。⑴包过滤/安全控制：在大多数路由器上，采用第四层信息去定义过滤规则已经成为默认标准，所以有许多路由器被用作包过滤防火墙，在这种防火墙上不仅能够配置允许或禁止IP子网间的连接，还可以控制指定TCP/UDP端口的通信。和传统的基于软件的路由器不一样，第四层交换区别于第三层交换的主要不同之处，就是在于这种过滤能力是在ASIC专用高速芯片中实现的，从而使这种安全过滤控制机制可以全线速地进行，极大地提高了包过滤速率。⑵服务质量：在网络系统的层次结构中，TCP/UDP第四层信息，往往用于建立应用级通信优先权限。如果没有第

四层交换概念，服务质量/服务级别就必然受制于第二层和第三层提供的信息，例如MAC地址，交换端口，IP子网或VLAN等。显然，在信息通信中，因缺乏第四层信息而受到妨碍时，紧急应用的优先权就无从谈起，这将大大阻止紧急应用在网络上的迅速传输。第四层交换机允许用基于目的地址、目的端口号（应用服务）的组合来区分优先级，于是紧急应用就可以获得网络的高级别服务。⑶服务器负载均衡：在相似服务内容的多台服务器间提供平衡流量负载支持时，第四层信息是至关重要的。因此，第四层交换机在核心网络系统中，担负服务器间负载均衡是一项非常重要的应用。第四层交换机所支持的服务器负载均衡方式，是将附加有负载均衡服务的IP地址，通过不同的物理服务器组成一个集，共同提供相同的服务，并将其定义为一个单独的虚拟服务器。这个虚拟服务器是一个有单独IP地址的逻辑服务器，用户数据流只需指向虚拟服务器的IP地址，而不直接和物理服务器的真实IP地址进行通信。只有通过交换机执行的网络地址转换（NAT）后，未被注册IP地址的服务器才能获得被访问的能力。这种定义虚拟服务器的另一好处是，在隐藏服务器的实际IP地址后，可以有效地防止非授权访问。 虚拟服务器是基于应用服务（第四层TCP/UDP端口号）定义的，这样，独立服务器便可以是虚拟服务器的成员。而使用第四层对话标志信息，第四层交换机则可以使用许多负载均衡方法，在虚拟服务器组里转换通信流量，其中OSPF、RIP和VRRP等协议与线速交换和负载均衡是一致的。第四层交换机还可以利用被称之为TRL（Transaction Rate Limiting）功能所提供的复杂机制，针对流量特性来遏制或拒绝不同应用类型服务。可

以借助CRL（Connections Rate Limiting）功能，使网络管理员指定在给定的时间内所允许的连接数，保障QoS.或者借助SYN-Guard功能，确保那些满足TCP协议的合法连接才可查询网络服务。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com