第3章 交换机基础

3.1 交换机工作原理

通过集线器组织的计算机网络的数据传送方式属于共享工作模式，这是因为连接各个计算机设备的集线器是一种共享设备，当网络中的某个设备向集线器发送数据，希望通过集线器将数据发给目的设备时，由于集线器不具有识别数据中所包含目的地址的能力，数据将以广播的方式发给与集线器相连的所有其他设备，收到数据的所有设备都会通过对比数据包头中的地址信息是否为本设备的地址信息来确定是否接收数据。也就是说，在这种工作方式下，网络上在同一时刻只能传输某个设备的一个数据包，如果多个设备都需要发送数据，就会发生碰撞，这种方式就是共享网络带宽的数据传输方式。根据共享工作模式的特点，当网络中设备数量过多时，设备发送数据就会存在冲突，影响了网络的工作效率，因此，共享工作模式只适用于网络规模小的网络。对于规模较大的网络，需要采用其他合适的数据传送方式，而数据交换概念的提出改进了网络的共享工作模式，提高了网络的数据传送效率。

交换技术工作在 OSI 参考模型中的第二层，即数据链路层，因此交换操作是根据 MAC 地址进行的。在交换机内部的高速缓存中保存着 MAC 地址与端口的映射表，交换机就是通过查询该映射表来实现数据交换的。

数据交换功能的实现涉及两个子功能，即地址学习和数据包转发，下面分别介绍。

(1) 地址学习功能

地址学习功能主要完成以下内容。

① 源 MAC 地址学习。交换机通过端口接收到数据包后，会获取数据包中的源 MAC 地址，如果检查发现 MAC 地址与端口映射表中没有与该 MAC 地址相关的记录，就会在映射表中添加新的映射记录。

② 端口移动机制。交换机如果发现接收数据包的端口号不同于映射表中登记的数据包中源 MAC 地址对应的端口号，就需要修改映射表中的相应记录，将源 MAC 地址重新学习到当前接收数据包的端口，从而产生端口移动。

③ 地址老化机制。如果交换机的某个端口在规定的一段时间之内没有收到任何数据包，就会删除映射表中与该端口相关的所有记录，这样做的原因在于可以释放出映射表空间给新学到的 MAC 地址使用，被删除记录的端口在到数据包时，可以通过重新进行源 MAC 地址学习的方式将相应的映射再次添加进来。地址老化机制是交换机应对庞大的网络地址的一种行之有效的处理方法，不仅映射表降低了对交换机内存的存储量需求，也提高了映射

表的查询速度。

(2) 数据包转发功能

数据包转发功能主要完成以下内容。

① 交换机的端口控制电路收到数据包以后,如果数据包中的源 MAC 地址和目的 MAC 地址所在的交换机端口不相同,会到内存中的 MAC 地址映射表中查找数据包中的目的 MAC 地址挂接在哪个端口上。如果在映射表中找到相关记录,会通过内部交换矩阵迅速将数据包传送到映射表中指定的端口;如果在映射表中找不到相关记录,就向所有的端口广播该数据包,端口接收到回应后,交换机就将原来的目的 MAC 地址与该端口的对应记录添入内部 MAC 地址映射表中。

② 交换机的端口控制电路收到数据包以后,如果数据包中的源 MAC 地址和目的 MAC 地址所在的交换机端口相同,则丢弃该数据包。

③ 如果交换机的端口控制电路收到的数据包是广播数据包,则交换机会向除接收端口以外的其他所有端口转发该广播数据包。

从交换机数据交换的工作原理可以得知交换机具有以下特点。

- 交换机是一种基于 MAC 地址识别、能够封装及解封数据包、能够转发数据包的网络设备,交换机能够学习 MAC 地址与端口之间的对应关系,将这种对应关系保存在内部映射表中,并在数据包的始发端口和目标端口之间建立临时的交换路径,实现将数据包从源地址转发到目的地址的目的。
- 根据交换的原理可知,交换机可以在同一时刻进行多个端口对之间的数据传输。每个端口都可以看成是独立的网段,连接在该端口上的网络设备独自享有全部带宽,不需要与其他端口上的设备竞争带宽,也就是所有同时发生的端口对之间的数据传输都有自己的虚拟连接,都享有网络的全部带宽。这就要求交换机拥有一条具有高带宽的背板交换总线,交换机的所有端口都挂接在这条背板总线上。如果交换机有 N 个端口,每个端口的带宽是 M,交换机背板交换总线的带宽只有在超过 $N \times M$ 时,交换机才能够实现线速转发数据。
- 交换机一般都含有专门用于处理数据包转发的内部交换矩阵,因此转发速度可以非常快。
- 交换机通过地址老化机制来降低 MAC 地址与端口映射表对交换机内存的需求,但是在一定程度上影响了数据的转发速度,因此,MAC 地址与端口映射表的大小将影响交换机的接入容量。
- 通过交换机可以把网络分段,交换机通过查找 MAC 映射表,只在端口间转发数据,而不会将数据转发给不相关的端口,也就是只允许必要的网络流量通过交换机,这样,通过交换机的过滤和转发,就可以有效地隔离广播风暴,避免了共享冲突。

3.2 交换机的分类

根据交换机的不同分类标准,交换机可以分成如下五类。

(1) 根据交换机的网络连接覆盖范围可分为局域网交换机和广域网交换机。

局域网交换机工作在局域网中,主要用于连接网络中的终端设备,比如,网络共享打印

机、工作站、服务器等，局域网交换机在这些设备之间提供独立的高速通信通道，单个局域网交换机只能管理一个局域网。广域网交换机主要工作在城域网互联、互联网接入等的广域网中，它提供通信用的基础平台，广域网交换机的背板带宽要大大高于局域网交换机。广域网交换机支持路由功能、内置安全机制、带有计费功能，并且广域网交换机可以管理多个局域网。

(2) 根据交换机在网络中的工作层次的不同，交换机可分为接入层交换机、汇聚层交换机和核心层交换机。其中，接入层交换机基本上采用以 10/100Mbps 为主的固定端口式架构，并且以扩展槽方式或固定式端口提供 1000BASE-T 的上连端口。汇聚层交换机具有固定端口式和机箱式两种架构，它不仅能够提供多个 1000BASE-T 端口，也能够提供 1000BASE-X 等端口。核心层交换机全部采用机箱式模块化架构，基本上都配备了 1000BASE-T 模块。

(3) 根据交换机的传输速度以及使用的传输介质的不同，交换机可以分为以太网交换机、快速以太网交换机、千兆以太网交换机、万兆以太网交换机、ATM 交换机、FDDI 交换机和令牌环交换机等。其中，以太网交换机是指带宽在 100Mbps 以下的应用于以太网的交换机；快速以太网是一种在光纤上或普通双绞线上实现 100Mbps 传输带宽的网络技术，快速以太网交换机就是应用于 100Mbps 快速以太网的交换机；千兆以太网的带宽可以达到 1000Mbps，一般用于大型网络的骨干网段，采用光纤或双绞线作为传输介质，千兆以太网交换机就是应用于千兆以太网的交换机。

(4) 根据交换机工作在 OSI 参考模型的不同层次，交换机可以分为第二层交换机、第三层交换机和第四层交换机等，一直可以到第七层交换机。其中，第二层交换机对应于 OSI 参考模型的第二层，它只工作在 OSI 参考模型的第二层，即数据链路层，该交换机根据链路层消息中的 MAC 地址进行交换机不同端口之间的线速数据交换，主要功能包括物理编址、帧序列、数据流控制和错误校验。第三层交换机对应于 OSI 参考模型的第三层，它工作在 OSI 参考模型的第三层，即网络层，它比第二层交换机具有更强的网络通信功能，该交换机根据网络层消息中的 IP 地址选择经过不同网络的传输路由，实现数据在不同网络间的传送。第四层以上的交换机称为内容型交换机，它们工作在 OSI 参考模型的第四层以上，主要用于互联网数据中心。

(5) 根据交换机是否支持 SNMP(Simple Network Management Protocol，简单网络管理协议)或 RMON(Remote Network Monitoring，远端网络监控)等网络管理协议，交换机可以分为非可管理型交换机和可管理型交换机。网络管理服务器可以监控可管理型交换机，而无法监控非可管理型交换机。

3.3 二层交换

3.3.1 二层交换工作原理

二层交换工作在 OSI 七层参考模型的第二层，即数据链路层，它的操作对象是数据帧。它是根据数据帧中的 MAC 地址对数据帧进行交换和过滤，从而实现 LAN 内主机之间的互连。

产生二层交换的原因是为了解决局域网在运行中遇到的问题，下面以最常见的局域网技术，也就是以太网技术为例。

早期以太网采用的是总线拓扑结构，为了保证网络传输介质有序、高效地为网络上所有主机提供传输服务，也就是解决网络上所有主机共享传输介质的问题，以太网的介质访问控制协议采用了CSMA/CD(Carrier Sense Multiple Access/Collision Detect，载波监听多路访问/冲突检测)机制。由于总线是网络上所有主机的唯一的、共享的通信通道，该机制在总线上允许在某一时刻只能有一个主机在发送数据，而其他主机在该时刻只能监听总线的忙闲状态，从而知道本机何时可以发送数据。当有两个主机或多个主机在同一时刻都想要向总线发送数据时，就产生了冲突，发生冲突的主机都会通过该机制的退避算法确定发送延时，由于各个主机的延时时长不一致，从而避免了下次发送数据时的冲突。但是这种机制也会带来问题，当挂在总线上的主机数量增多时，产生冲突的概率也就增大，退避算法的实现实际上降低了主机通信的速度，也降低了网络带宽的利用率。为了提高主机通信速度以及提高网络带宽的利用率，只有降低冲突发生的概率。

第二层交换可以将一个较大的网络划分为若干个较小的物理网段，各个网段不共享带宽，从而有效地增加了各个网段的带宽和吞吐量，将原来没有网段的共享带宽变成了各个网段的独占带宽，有效地分割了冲突域，减少了冲突的发生，大大提高了网络带宽的利用率。

二层交换机采用了多物理端口以及数据帧的MAC转发机制实现了分割冲突域的目的，交换机端口的功能是接收或转发与其相连的LAN上的数据帧，端口的状态有转发、学习、监听、阻塞和禁止状态，MAC转发功能主要实现交换机的不同端口之间的内部通信。

二层交换机保存各个端口的工作状态并维护一个MAC与端口映射表，通过该表来实现MAC层的路由。二层交换机具有MAC地址学习能力，可以将主机的MAC地址与该主机所连接的端口等信息记录在MAC与端口映射表中。

当从某个端口接收到数据帧时，交换机会检测数据帧中包含的源MAC地址和目的MAC地址，并将数据帧中的源MAC地址与端口号一起保存在MAC与端口映射表中。经过一段时间，交换机就会自动学习到所在网络的所有主机的MAC地址信息。同时，交换机也会根据数据帧中包含的目的MAC地址，在MAC与端口映射表中查找与该MAC地址相关的记录，并根据查找结果的不同，进行不同的处理。

(1) 如果成功找到与目的MAC地址相关的记录，会首先判断记录中指定的目的端口的工作状态，如果目的端口没有被阻塞，就将该数据帧到目的端口转发出去，实现了数据帧从源端口到目的端口的交换。

(2) 如果没有找到与目的MAC地址相关的记录，就将该数据帧广播发送到除其进入交换机的端口以外的所有其他端口。

(3) 如果通过查表发现，目的MAC地址对应的端口就是该数据帧进入交换机的端口，交换机将丢弃该数据帧。

为了保证数据帧的高转发速度，二层交换机采用ASIC(Application Specific Integrated Circuit，专用集成电路)技术，通过硬件实现协议解析和数据帧转发技术，从而达到数据帧从源端口到目的端口的点到点的线速交换。

3.3.2 二层交换主要特点

- 通过二层交换机可以连接具有不同速率的网段而构成具有混合速率的局域网。比如，10Mbps 网段与 100Mbps 网段或者 100Mbps 网段与 1000Mbps 网段都可以通过交换机互连。
- 扩展局域网覆盖的区域。由于共享冲突，单个冲突域不能包含过多的主机，而交换机分隔了冲突域，多个冲突域可以通过交换机构成更大的网络，从而扩大了网络覆盖范围。
- 可以支持过滤功能。根据应用或安全等方面的限制，通过配置数据帧的过滤规则，限制数据帧可以转发的端口，这样，不仅消除了多余的网络流量，还满足了某些应用的需求和安全需求。
- 可以支持 QoS 功能。通过使用优先级，能够以更快的速度转发对时间敏感的、优先级较高的数据帧。
- 可以支持 VLAN(Virtual Local Area Network)，通过 VLAN 技术能够将相互通信的、共享数据的、物理上分散的主机逻辑分组。
- 可以通过包含简单网络管理协议(SNMP)和远程监控协议(RMON)来支持远程网络监测和管理。
- 数据转发速度快。二层交换工作在 OSI 参考模型的数据链路层，对于网络层以上的高层协议来说是透明的，也就是它不处理网络层的 IP 地址，不处理诸如 TCP、UDP 的端口地址，它只是按照所收到数据帧中的目的 MAC 地址来进行转发，并且依靠硬件实现数据转发，因此交换机的数据转发速度相当快。

3.4 三层交换

3.4.1 三层交换的引出及发展

最初的第二层交换机只能分割网络的冲突域，而无法分割网络的广播域。如果交换机的某个端口收到目的地址是广播地址的数据包时会向所有端口转发。这样的话，当网络的规模较大时，广播包的数量就会增多，大量的广播包将充斥着整个网络，从而造成网络的性能下降，严重时还可能引起广播风暴。

针对这个问题，二层交换机引入了 VLAN 技术，该技术将同一物理局域网内的不同主机从逻辑上划分成一个个网段，形成多个虚拟工作组，也就是多个 VLAN，具有相同工作需求的主机属于同一个 VLAN。由于是从逻辑上划分，而不是从物理上划分，一个 VLAN 内的各个主机可以位于不同的物理网段，这个逻辑上的 VLAN 与物理上形成的 LAN 具有相同的属性，从而划分出不同的广播域，一个 VLAN 内部的广播和单播流量都被限制在 VLAN 的内部，而不会转发到其他 VLAN 中。通过 VLAN 技术，二层交换网络的广播域得到分割，网络的广播风暴得到了控制，同时网络的安全性也得到了提高。

但是，VLAN 技术在隔离 VLAN 之间的广播风暴的同时，也隔离了各个 VLAN 之间的

通信，这使得 VLAN 之间的通信必须经过网络层的路由才能完成。

在早期，网络层路由只能靠路由器来完成。路由器具有丰富的网络功能，可以处理大量跨越子网的报文，但是路由器的路由选择及报文转发功能的实现依赖于协议栈软件的运行。因此，报文的转发速度较慢，转发效率要比二层交换低。如果 VLAN 之间的通信依靠路由器转发，路由器将会成为整个网络的瓶颈。由此，结合了效率高的二层转发与三层路由处理的三层交换技术就诞生了。

相对于传统交换概念，1997 年出现了一种新的交换技术，它就是三层交换技术，也被称为 IP 交换技术，它是将交换功能和路由功能集成于一体的技术。

第三层交换机在传统的第二层交换机的基础上增加了路由功能。由软件实现第三层交换机的路由学习功能，而由硬件来实现 IP 数据包的转发功能。这样，第三层交换机在学习到路由以后，就可以按照报文中的 IP 地址由硬件直接转发数据包，从而大大提高了 VLAN 之间通信的速度。三层交换技术的出现，解决了局域网中 VLAN 划分之后，VLAN 之间必须依赖路由器进行通信的局限，同时也解决了传统路由器低速数据包转发造成的网络瓶颈问题。

目前，随着第三层交换技术越来越成熟，第三层交换机的应用地点也从网络的骨干范围扩展到网络的边缘范围，它的应用领域也扩大到企业局域网、校园网、宽带网等领域。

随着交换技术的发展，目前出现了第四层交换技术和第七层交换技术。

第四层交换技术可以根据第四层的代表不同业务协议的 TCP、UDP 端口号以及第三层的 IP 地址等第四层与第三层的信息来分析数据包的业务类型，并做出向何处转发会话传输流的决定。第四层交换的交换域是由源 IP 地址、目的 IP 地址以及 TCP 端口/UDP 端口共同决定的，第四层交换机成为一种基于会话的交换机，可以在会话级别控制网络流量和会话的服务质量。

除了第四层交换技术以外，也出现了 OSI 参考模型中的第七层的交换技术，第七层交换技术更具有智能交换的特征。第七层交换技术具有对应用层内容的认知功能，它可以通过分析数据流中的应用层的内容，根据应用的类型、应用的内容来控制数据交换转发行为，这样的处理更具有智能性，交换的是内容。因此，第七层交换机是一种基于应用的交换机，可以在应用级别实现有效的数据流优化和智能负载均衡。

3.4.2 三层交换工作原理

第三层交换技术是将路由技术与交换技术合二为一的技术。通过在交换机中增加网络层的功能，以交换机的性能来完成路由器的路由功能，这样的设备称为第三层交换机。第三层交换机将路由学习与数据包转发功能相分离，其中，路由学习功能由路由协议来实现，而数据包转发功能则采用交换的思想由硬件来实现，从而在网络层实现了数据包的线速转发。下面简要介绍路由功能与转发功能在第三层交换机中结合使用的过程。

三层交换机在收到业务数据流中的第一个 IP 数据包后，会根据 IP 包中目的 IP 地址选择路由，路由选择成功后，也就确定了该 IP 数据包从交换机中转发出去的输出端口。然后将在 MAC 地址与 IP 地址映射表中增加该 IP 数据包在交换机的输出端口的 MAC 地址与该目的 IP 地址的映射记录，当三层交换机收到该业务数据流的后续 IP 数据包时，不再需要选择路由的过程，而是根据目的 IP 地址从 MAC 地址与 IP 地址映射表中查出对应的输出

端口的 MAC 地址，直接在数据链路层将 IP 数据包转发出去。这样的话，相当于在三层交换机中打通了一条从源 IP 地址到目的 IP 地址的通路，有了这条通路，三层交换机就不必每次都对收到的 IP 数据包进行解封操作并判断路由了，而是直接将 IP 数据包交由数据链路层的交换模块来完成数据包的转发。这就是通常所说的，一次路由，多次转发。

可见，三层交换机集路由功能与交换功能于一体，在交换机内部实现了路由，这样做的结果是，提高了数据包转发效率，消除了路由器进行路由选择而造成的网络延迟，消除了路由器可能产生的网络瓶颈问题，提高了网络的整体性能。

三层交换机和路由器具有以下三点不同：

(1) 三层交换机的端口基本上都是以太网端口，它不如路由器的端口类型丰富；

(2) 三层交换机不仅可以工作在 OSI 参考模型的第三层，也可以工作在第二层，可以直接交换不需要路由的数据包，而路由器不能工作在第二层，只能工作在第三层；

(3) 路由器基于软件处理来转发报文，而三层交换机是通过 ASIC 硬件来转发报文，因此两者之间的性能差别很大。

3.5 虚拟局域网

3.5.1 VLAN 的基本原理

根据交换机的数据转发原理，交换机在它的源端口与目的端口之间提供了直接的点到点连接，不仅解决了共享式局域网的共享冲突问题，而且还提高了网络带宽的利用率。但是，交换机无法有效隔离广播域，它对广播帧的处理方式是向交换机的所有端口转发。随着网络规模越来越大，广播帧的数量也会越来越多，极大地消耗了网络带宽。广播帧所占用的带宽影响了其他数据的传输，严重时会产生广播风暴，造成数据传输时延增长，网络性能迅速地下降，甚至造成全网阻塞以致瘫痪。这样，交换机组成的网络就陷入网络规模与网络性能之间的对立。为了解决网络规模与网络性能之间的矛盾，一个有效的解决方法就是构造较小的交换网，限制广播范围。而早期单个局域网的物理网络与逻辑网络的个数都是一个，并且是一一对应的，单一的物理网络对应的广播域个数也是一个。因此，具有不同共享数据域的主机也被束缚在同一个物理网络中，而不能根据需要将不同主机划分至不同的逻辑子网中，这样的网络结构缺乏灵活性，效率低和安全性差。解决的办法就是在统一的物理网络上，划分出不同的逻辑网段，这些逻辑网段是互相隔离的，是一个广播域，与用户的物理位置无关。

为了解决上述问题，虚拟局域网 VLAN 技术应运而生。VLAN 是 IEEE 802.1Q 中定义的一个标准，在 IEEE 802.1Q 中，VLAN 是在数据链路层实现的。VLAN 技术就是在交换局域网的基础上，在同一物理网络中将单一逻辑网络划分成多个逻辑子网的技术，它是一种将局域网内的主机逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的技术。它将局域网设备从逻辑上划分成一个个网段，网络中的任何主机都可以根据特定的逻辑子网划分方法而灵活地加入到不同的逻辑子网中，这些逻辑子网被称为虚拟局域网 VLAN。一个 VLAN 组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个主机，允许位于不同地理位置的主机加入到一个逻辑子网中。VLAN 和普通局域网一样，覆盖了一个广播包能够

到达的主机范围，同一 VLAN 中的成员可以共享广播，而不同 VLAN 之间广播信息是相互隔离的，这样，整个网络的单一广播域被分割成多个不同的广播域。绝大多数的网络流量都限制在同一 VLAN 之内，一个 VLAN 中的成员看不到另一个 VLAN 中的成员，属于不同 VLAN 的主机就如同被物理分割到不同网络一样，即位于不同 VLAN 的主机之间不能直接通信。从使用效果上看，这与独立的网络没有差别。

VLAN 通过在数据帧中增加 VLAN ID(VLAN Identifier)的方式将网络分割开来，一个大的广播域被划分为若干小的广播域，这样就可以限制广播范围。

VLAN 是建立在物理网络上的一种逻辑子网，建立 VLAN 需要支持 VLAN 技术的网络设备。当网络中的不同 VLAN 间进行相互通信时，由于需要路由的支持，就需要增加路由设备，路由器或三层交换机都可以完成路由功能。

3.5.2 VLAN 的划分方法

VLAN 的划分标准主要包括以下几种，分别是基于端口划分、基于 MAC 地址划分、基于 IP 地址划分以及基于网络层协议划分等。

(1) 基于端口划分

基于端口的 VLAN 划分方法是最常用、最简单的 VLAN 划分方法，几乎所有的交换机都支持该划分方法。该方法从逻辑上把交换机上的物理端口分成若干个 VLAN，这些交换机端口可以在同一个交换机上也可以跨越多个交换机。该方法不允许同一个交换机端口出现在多个 VLAN 内，从而把网络从逻辑上划分成相对独立的，在功能上模拟传统局域网的不同 VLAN。

这种划分方法的特点是挂在属于同一个 VLAN 的各个端口上的所有主机都在一个广播域中，从一个端口发出的广播，可以直接发送到 VLAN 内的其他端口，它们相互可以直接通信，而不同 VLAN 之间的通信需要经过路由来进行。

这种基于交换机端口来划分 VLAN 的方法的优点是简单，容易实现。但其主要缺点是如果 VLAN 中的主机离开了原来的端口，移动到另一个端口，那么就必须对 VLAN 成员重新配置。

(2) 基于 MAC 地址划分

所谓基于 MAC 地址的 VLAN 划分就是根据交换机所在网络中的所有主机的 MAC 地址来划分 VLAN，由于主机上的每一个网卡上都有一个全球唯一的 MAC 地址，因此，这种划分方法就是配置每一个主机属于哪一个 VLAN。

这种划分 VLAN 的方法的最大优点就是当主机在交换机间或交换机各端口间进行物理位置移动时，主机上的 MAC 地址没有发生改变，该主机在原有的 VLAN 中的成员资格没有发生改变，因此，VLAN 不用重新配置。对于主机需要经常移动办公的网络而言，这种划分方法大大减少了网络管理员的日常维护工作量。

这种划分方法的缺点是网络中的所有主机必须被明确的分配到一个 VLAN 中。这样，在一个大规模网络中，配置工作量会相当大；另外，任何时候增加主机或者更换网卡，都需要调整 VLAN 的配置；而且，这种划分方法也会降低交换机的工作效率，因为在交换机的每一个端口上都有可能挂着很多个属于不同 VLAN 的成员，VLAN 内主机间的通信会受到影响，同时在这种情况下，无法限制 VLAN 之间的广播包。

(3) 基于 IP 地址划分

这种划分方法是人为地将属于不同 IP 地址范围的主机划分为不同 VLAN。

这种划分方法的优点是当某一主机的 IP 地址发生改变时,交换机能够自动识别,并重新定义 VLAN,而不需要网络管理员干预。这种划分方法的缺点是由于主机的 IP 地址可以人为的、不受约束的自由设置,因此这种 VLAN 划分方法会带来安全上的隐患。另外,该 VLAN 划分方法需要检查每一个数据包的网络层地址,因此增加了处理时间,造成效率低下。

(4) 基于网络层协议划分

VLAN 按网络层协议来划分,可分为多个具有不同网络层协议的 VLAN,具有相同协议的主机划分为一个 VLAN。在具体操作中,交换机会检查数据帧的帧头,帧头中包含网络层协议的类型。如果该协议的 VLAN 已经存在,那么就将该源端口加入到该 VLAN 中,否则,就创建一个与该协议相对应的新 VLAN。

基于网络层协议组成 VLAN 的方法的优点如下:

- 大大减少了 VLAN 配置的工作量;
- 不同网段上的主机可以属于同一个 VLAN,而不同 VLAN 上的主机也可以位于同一物理网段上;
- 可以使广播域跨越多个交换机;
- 非常适用于针对具体应用和服务来组织用户的场景;
- 主机在网络内的物理位置发生了改变不会影响其所在 VLAN 的成员身份,主机可以自由地增加、移动和修改,而不需要重新配置其所属的 VLAN。

3.5.3 VLAN 遵循的技术标准

目前业界普遍遵循的 VLAN 技术规范是 IEEE 提出的 VLAN 国际标准 IEEE 802.1Q,这个标准规定了 VLAN 的实现方法,它主要定义了在数据链路层的数据帧上添加带有 VLAN 成员信息的方法,也规定了 VLAN 定义、VLAN 运行以及管理 VLAN 拓扑结构等的操作,此外 IEEE 802.1Q 标准还提供更高的网络段间安全性。

在数据帧中增加 VLAN 标签是实现 VLAN 的关键,一个包含 VLAN 信息的标签字段可以插入到数据帧中。可以配置支持 IEEE 802.1Q 的交换机端口是传输标签帧还是传输无标签帧。如果支持 IEEE 802.1Q 的设备(比如,交换机)通过端口相连,那么 VLAN 标签帧就可以在交换机之间传送 VLAN 成员信息,这样的话,VLAN 就可以跨越多台交换机。但是,如果在某个支持 IEEE 802.1Q 的交换机端口上连接的设备不支持 IEEE 802.1Q,就必须确保该端口可以传输无标签帧。否则,如果不支持 IEEE 802.1Q 的设备收到含有 VLAN 标签的数据帧,就会由于不能识别 VLAN 标签而丢弃整个数据帧。

VLAN 的体系结构表明,IEEE 802.1Q 标准是为不同设备厂商所生产的不同设备使用 VLAN 而制定的数据帧方面的标准。IEEE 802.1Q 标准完善了 VLAN 的体系结构,统一了 VLAN 帧格式。IEEE 802.1Q 标准的出现打破了 VLAN 技术依赖于单一厂商的局面,确保了不同厂商产品的互通,该标准在业界获得了广泛的推广,也推动了 VLAN 技术的迅速发展。

3.5.4 VLAN 的优点

VLAN 技术的出现使网络结构变得灵活，广播风暴得到了控制，网络安全性得到了提高，并且提高了网络管理效率、网络连接的灵活性以及网络性能。

1. 控制了广播风暴

VLAN 技术实际上是一种网络分段技术，一个以太网可以基于不同的方式划分为多个 VLAN 子网，一个 VLAN 就是一个逻辑广播域，整个网络被逻辑地分割成多个广播域，通过对 VLAN 的创建，隔离了广播，缩小了广播范围。在一个 VLAN 子网中，由 VLAN 成员所发送的信息帧或数据包仅在 VLAN 内的成员之间传送，而不是向网上的所有主机发送。在一个 VLAN 子网中，由一个主机发出的广播信息只能发送到具有相同 VLAN ID 号的其他主机，其他 VLAN 的成员收不到这些信息的广播，在一个 VLAN 中的广播不会发送到 VLAN 之外，它可以将广播风暴限制在一个 VLAN 内部，使得一个 VLAN 的广播风暴不会影响其他 VLAN 的性能。

VLAN 的子网划分有效地控制了网络上的广播风暴，VLAN 能够更加有效地利用带宽。这样可减少主干网的流量，提高网络速度。

2. 提高了网络安全性

由于工作或业务原因，局域网用户会在网上传送一些关键性的、保密的数据，由于 LAN 上主机属于一个共享域，因此，LAN 上的所有用户都能监测到流经的数据，这必然会产生安全性问题。

要解决 LAN 数据传输的安全问题，可以采用多种方法，其中一种方法是可以对保密数据的访问进行控制，另一个有效的、方便的方法是将原来的局域网分段从而形成多个 VLAN。由于一个 VLAN 就是一个单独的广播域，从而将原来的单一广播域划分成多个小广播域。VLAN 的特性是 VLAN 之间相互隔离广播，可以将敏感数据的传播限制在安全的范围之内。另外，可以根据工作或业务的需要，限制不同 VLAN 中用户的数量、控制某个广播域的大小，从而将对 VLAN 中数据或应用的访问限制在一定的范围之内。这样，通过采用 VLAN 提供的安全机制，大大提高了网络的安全性。

3. 增强了网络管理

VLAN 是基于逻辑连接而不是物理连接，这样，子网的划分就不再局限于各个主机的物理连接，构成 VLAN 的主机的地理位置也可以不相邻，VLAN 的定义和划分与主机的物理位置和物理连接没有任何必然联系，但是，VLAN 内部主机之间可以像在同一个本地局域网上那样进行通信。

采用 VLAN 技术，网络管理员可以根据不同的需求，灵活地建立和配置 VLAN，能够借助于 VLAN 技术更方便地实现网络的管理。

传统局域网中的各个主机一般具有相近的地理位置和物理连接，当基于工作或业务的需要，在局域网中增加、删除和移动网络主机的时候，往往需要重新布线，需要采用一条新的物理链路把该主机连到原来的局域网中。这样，当网络达到一定的规模时，因为网络成员的

变化所带来的开销往往会成为网络管理员的沉重负担。而 VLAN 技术的出现减少了由于网络成员变化所带来的开销，可以非常轻松自如地增加、删除和移动主机，使得主机可以非常方便地在网络中改变自己的位置，而不必从物理上进行调整。在一个交换网络中，VLAN 提供了网段和机构的弹性组合机制。

还可以为每个 VLAN 分配它所需要的带宽，当链路拥挤时，能够重新分配业务，从而可以迅速、有效地平衡负载流量。

利用 VLAN 技术，大大减轻了网络管理和维护工作的负担，降低了网络维护费用，增强了网络管理能力。

4. 增加了网络连接的灵活性

VLAN 技术的初衷和目标之一是组建虚拟组织，特别是虚拟工作组。

借助 VLAN 技术，能够将位于不同地点或不同网络的主机组合成一个虚拟的网络环境，VLAN 内的主机就像在本地 LAN 一样可以方便、灵活、高效地互通。在实际应用中，经常需要组建具有短期工作性质的工作组。采用了 VLAN 技术以后，在工作组建立前后，都不需要搬移工作组中主机的地理位置，也不需要改变各个主机的设置，只需修改 VLAN 的配置就可以了。这样，采用 VLAN 技术就可以降低改变主机的地理位置所需要的费用。

利用 VLAN 技术，大大增加了网络连接的灵活性。

5. 提高了网络性能

利用 VLAN 技术提高网络性能的原因如下。

(1) 利用 VLAN 技术，可以将交换机上的端口逻辑上分成多组，分组后，VLAN 内的数据流只能在属于该 VLAN 的端口之间传送，VLAN 内的广播数据也只能限制在各个 VLAN 之内，VLAN 内的主机不会收到来自 VLAN 之外的广播数据，就不会受到其他 VLAN 内部的广播数据的影响，从而大大减少了 VLAN 之间的信息干扰，同时也减少了不必要的信息流量和网络上无用的信息流量，提高了网络的带宽利用率，从而提高了网络性能。

(2) 采用了 VLAN 技术以后，可以使用交换机代替路由器来分隔广播域。由于路由器在处理数据时要比交换机慢，而减少路由器的使用，会相应地提高网络的性能。

本 章 小 结

本章介绍了交换机工作原理、交换机的分类、二层交换原理、三层交换原理、虚拟局域网原理等五个部分，交换机是计算机网络中最重要的网络设备之一，了解交换机的工作原理是学习网络管理工作原理的重要基础之一。

在教学上，本章的教学目的是让学生掌握交换机的交换原理、二层交换原理，了解三层交换以及 VLAN，本章重点是二层交换原理、三层交换原理以及 VLAN 工作原理，本章难点是二层交换原理和三层交换原理。

习　　题

1. 简答题

(1) 数据交换功能中的地址学习功能的主要内容是什么?

(2) 数据交换功能中的数据包转发功能的主要内容是什么?

(3) 简述二层交换的工作原理。

(4) 简述三层交换的工作原理。

(5) 简述 VLAN 的优点。

2. 填空题

(1) 数据交换功能的实现涉及两个子功能,分别是(　　)和(　　)。

(2) 第三层交换技术是将(　　)与(　　)合二为一的技术。

(3) VLAN 的划分方法有基于(　　)划分、基于(　　)划分、基于(　　)划分等。