第4章　虚拟LAN

随着网络用户的增加，网络管理日益成为一种挑战，所以， VLAN（虚拟局域网）具有流行交换机的特点并不奇怪。VLAN可以减轻网络工程师的工作负担。VLAN还可以允许网络管理员取消过去的物理限制，并对用户的第3层网络地址进行控制，而不管它处在网络中的哪个位置。

VLAN的其他优势包括加强网络的安全性能、易于控制广播和能够分布通信量。 Cisco Catalyst交换机能够完成很多功能来加强和简化VLAN的实现。

中继线（trunking）的使用允许VLAN跨接由小型的或大型区域分开的多个交换机。Cisco也在它的许多路由产品中实施了中继特性，使得我们可以设计许多有益而有趣的网络。

4.1　VLAN定义

VLAN可以定义为“广播域”，VLAN即是广播域。第1章中，我们知道，广播域是第3层的网络。交换机可以定义一个VLAN，交换机的端口便成为VLAN中的成员。例如，在图4-1中，交换机的端口定义了两个VLAN，即会计（Accounting）和管理（Managemant）。

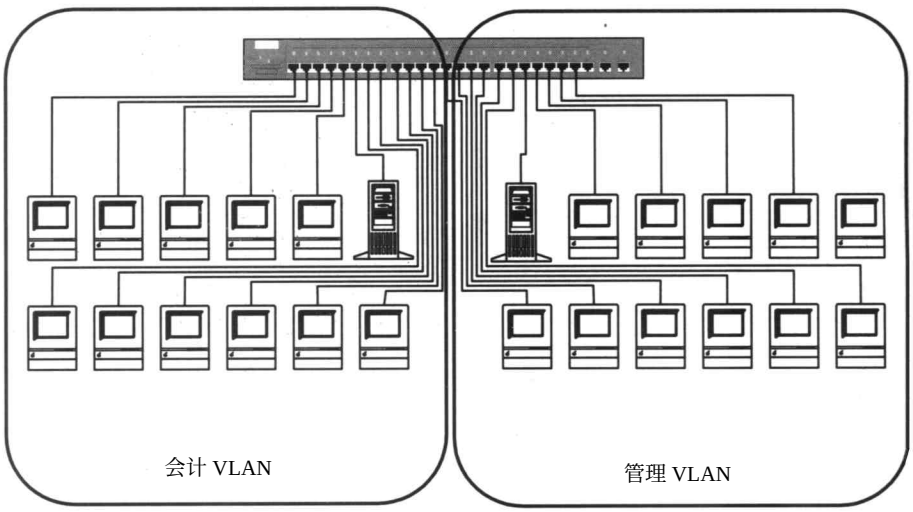


图4-1　在Catalyst 1900上的两个VLAN

图中，端口1到端口13分配给会计VLAN，端口13至端口24分配给管理VLAN。由于交换机不允许广播在VLAN之间传送，所以交换机相当于对图中的网络进行了逻辑分段（图4-2）。

如果工作站A发送一个广播，在会计VLAN上的所有工作站都接收到这个广播。但交换机不会将广播发送至管理VLAN上的任何一个端口。实际上，交换机不会从一个VLAN向另外一个的VLAN发送帧，除非它是一个多层交换机，这种交换机在本书的后面将加以讨论。现在，有人也许还在考虑第1章中所说的“路由器是唯一的能够对网络进行逻辑分段的设备”。从理论

上说，这种观点是不正确的，因为交换机也能够对网络进行逻辑分段，但在实际应用中，只使用交换机而不使用路由器对网络进行逻辑分段是非常可笑的，因为这种配置事实上不会允许信息在VLAN之间通过。所以这是一种不可靠的情况，而且也是一种讨论起来没有意义的情形。

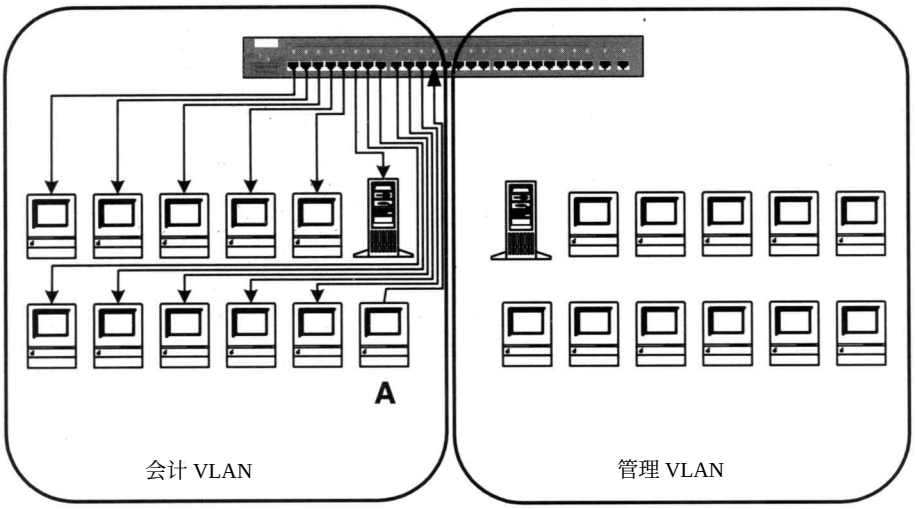


图4-2 广播限制在一个VLAN的所有端口上

在会计VLAN中的工作站将与管理VLAN中的用户处在完全不同的广播域中，所以就存在两个完全不同的IP子网、IPX网络和Applealk电缆范围。图4-3中，分配给会计VLAN的IP地址是172.16.10.0/24，IPX网络号为10，Appletalk电缆范围为10-10。分配给管理VLAN的IP子网地址为172.16.20.0/24，IPX网络号为20，Appletalk电缆范围为20-20。在这种情况下，一个VLAN的通信量将对另外一个VLAN不会产生影响，而不管它在网络中的物理位置。

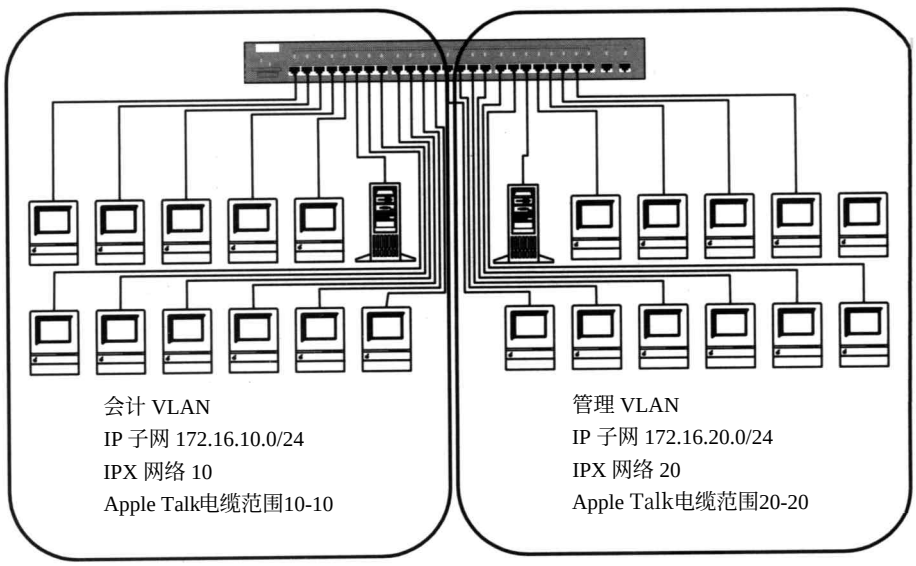


图4-3 分配给IP子网、IPX网络和Appletalk电缆范围

Cisco的VLAN实现为端口中心式。与节点相连的端口将定义它所驻留的 VLAN。怎样将端口分配给VLAN取决于Cisco Catalyst交换机。将端口分配给VLAN的方式有两种，分别是静态的和动态的。

4.2 静态VLAN

形成静态VLAN过程是将端口强制性地分配给 VLAN的过程。工程师一般按照自己的喜好来确定哪些端口属于哪些特定的 VLAN，然后将VLAN静态映射到端口。例如，在图 4-1中，将会计VLAN定义为与端口1至端口12相连接的任何节点。工程师还将输入一些合适的命令，这些命令有可能来自称为 SNMP管理工作站的交换机的 CLI（命令行接口），也有可能来自将端口1至端口12分配给会计VLAN的软件管理工具CWSI（CiscoWork Switched Internetworks）。这种方法非常耗时，因为工程师们只能对将端口映射到合适的 VLAN所必须的命令进行手工输入。不过，这是将端口映射到 VLAN的一种最通用的方法。

4.3 动态VLAN

动态的VLAN形成很简单，由端口自己决定它属于哪个 VLAN时，就形成了动态的VLAN。不过，这不是Terminator，也不是变成非小说文学的The Forbin Project，它是一个简单的映射，这个映射取决于工程师创建的数据库。分配给动态 VLAN的端口被激活后，交换机就缓存初始帧的源MAC地址（见图4-4）。

随后，交换机便向一个称为 VMPS （VLAN管理策略服务器）的外部服务器发出请求，VMPS中包含一个文本文件，文件中存有进行 VLAN映射的MAC地址。交换机对这个文件进行下载，然后对文件中的MAC地址进行校验。如果在文件列表中找到 MAC地址，交换机就将端口分配给列表中的 VLAN。如果列表中没有 MAC地址，交换机就将端口分配给默认的 VLAN（假设已经定义默认了 VLAN）。如果在列表中没有MAC地址，而且也没有定义默认的 VLAN，端口不会被激活。这是维护网络安全一种非常好的的方法。

从表面上看，动态VLAN的优势很大，但它也有致命的缺点，即创建数据库是一项非常艰苦而且非常繁琐的工作。如果网络上有数千个工作站，则有大量的输入工作要做。即使有人能胜任这项工作，也还会出现与动态的 VLAN有关的很多问题。另外，保持数据库为最新也是要随时进行的非常费时的工作。在第 6章中将对动态的VLAN做进一步讨论。

4.4 中继

前面我们已经知道，单个交换机可以定义 VLAN，那么多个交换机是怎样扩展 VLAN的呢？举个例子，图4-5给出了第1层和第2层楼上属于会计部门和管理部门的一部分节点。这两层楼的节点怎样才能属于同一个 VLAN呢？

图中，我们可以将两个交换机之间的物理连接分配给会计 VLAN，但这会限制楼层之间的通信。在交换机之间还可以形成另外一个连接，而且可以将这个连接放置在管理 VLAN中，但这种做法花费很大，特别是存在两个以上的 VLAN时。中继允许多个VLAN的信息通过同一个物理连接。例如，如果图 4-5中的两个交换机之间的连接做成一个中继连接，那么两个 VLAN都可以通过同一个物理连接进行通信。这个过程通常由一个标记完成。通过中继线进行传输的帧都将用VLAN ID进行标记。Catalyst交换机通过一个唯一的数字对每个 VLAN进行

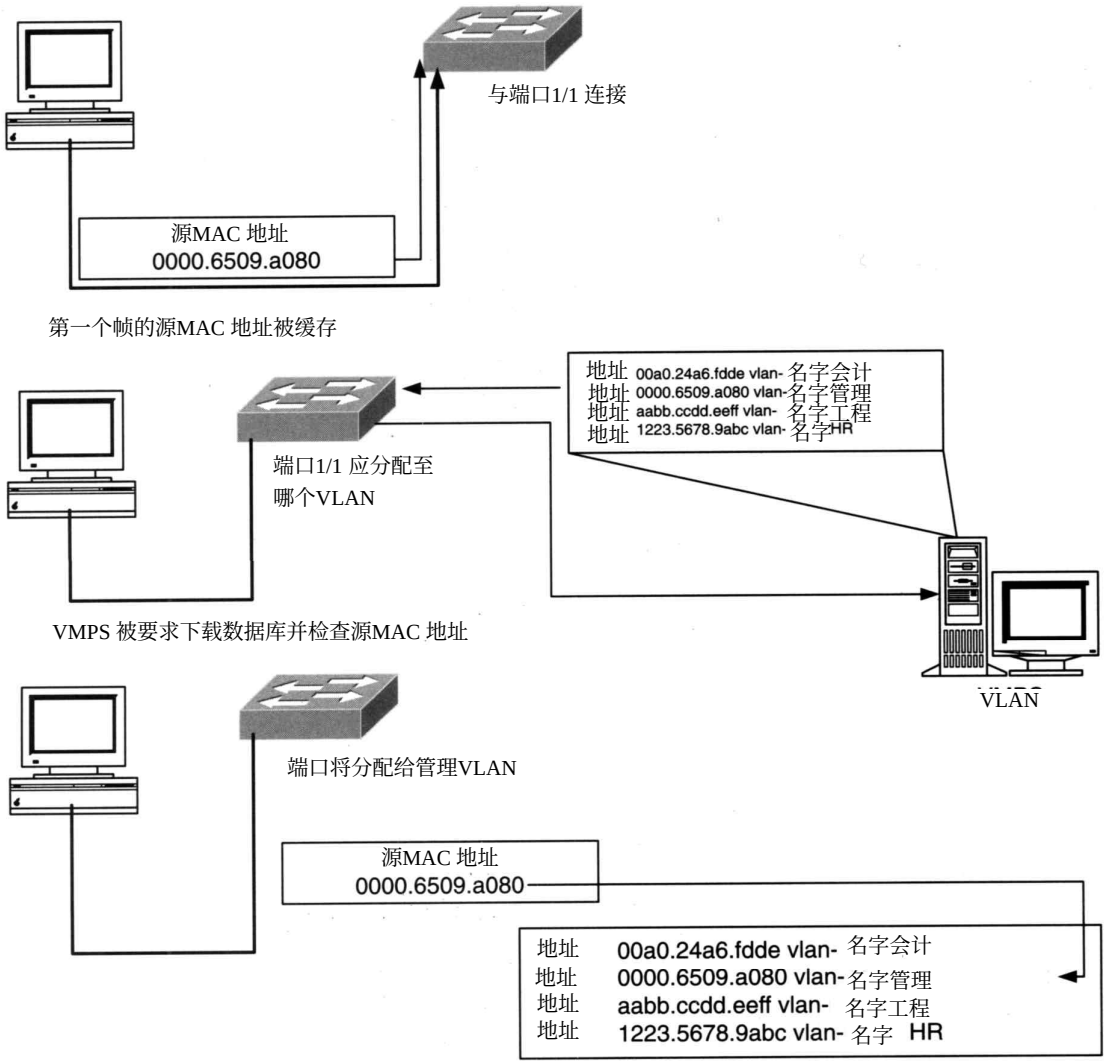


图4-4 将源MAC地址映射到管理VLAN

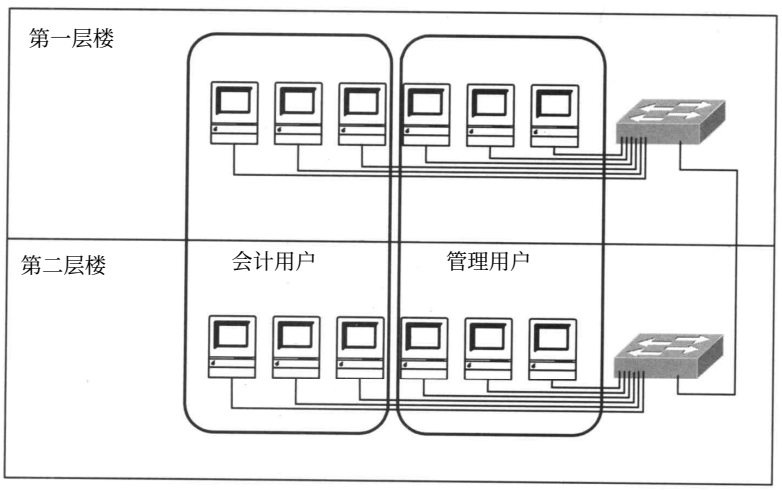


图4-5 会计用户和管理用户

识别。如果分配给会计 VLAN的VLAN号为100，那么，在中继线上进行传输的与会计 VLAN有关的所有帧都将使用VLAN 100进行标记（见图4-6）。

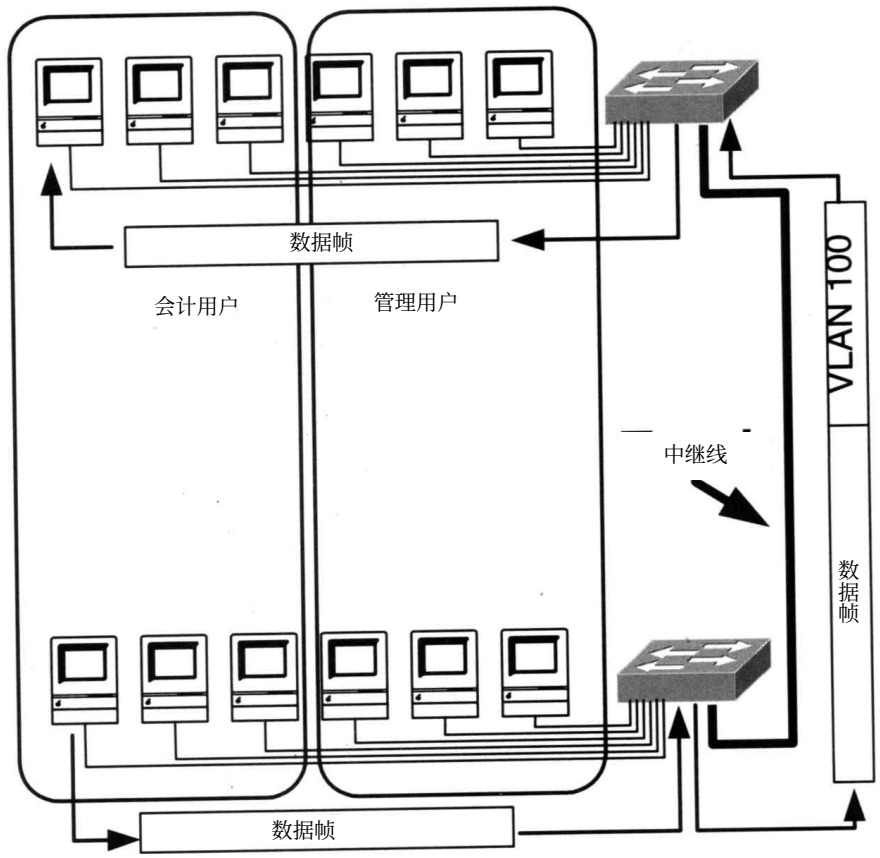


图4-6 中继标记

当第2层楼的交换机收到中继线上的帧时，它读取标记，然后便得知帧是发往会计 VLAN帧。另外，广播也将通过中继线进行传输。这一点是非常重要的，因为 VLAN也是一个广播域。由于广播能够在适当的 VLAN中继线上传播，广播域也可以通过交换机扩展。交换机通过读取来自中继线的帧上的标记，就可以将广播保留在适当的 VLAN中。

图4-7给出了一个由6层楼组成的网络，用户分散在所有的 6层楼上。由于实现了中继，所以，所有的会计用户都可以放置在同一个广播域中或同一个 VLAN 中。

图中，任一会计节点与一个 VLAN100端口进行连接，而不管这个节点位于哪个楼层。这样，所有的会计用户就可以处在同一个 IP子网、同一个IPX网络或同一个Appletalk的电缆范围中。图4-7中，我们还注意到，通过使用 VLAN，服务器不但可以定位到一起，而且仍然能够保持在它们各自的用户广播域中。

如果有必要，所有VLAN的通信都将经过中继线进行传输，这样可以确保其他的 VLAN通过整个网络保持连通，如图 4-8所示。

在这个网络中，所有的工作站将按照部门来进行逻辑地址的分配，而不管它所处的物理位置如何。在选择中继前，工程师要想从网络的物理配置中分离出逻辑寻址模式是非常困难的。

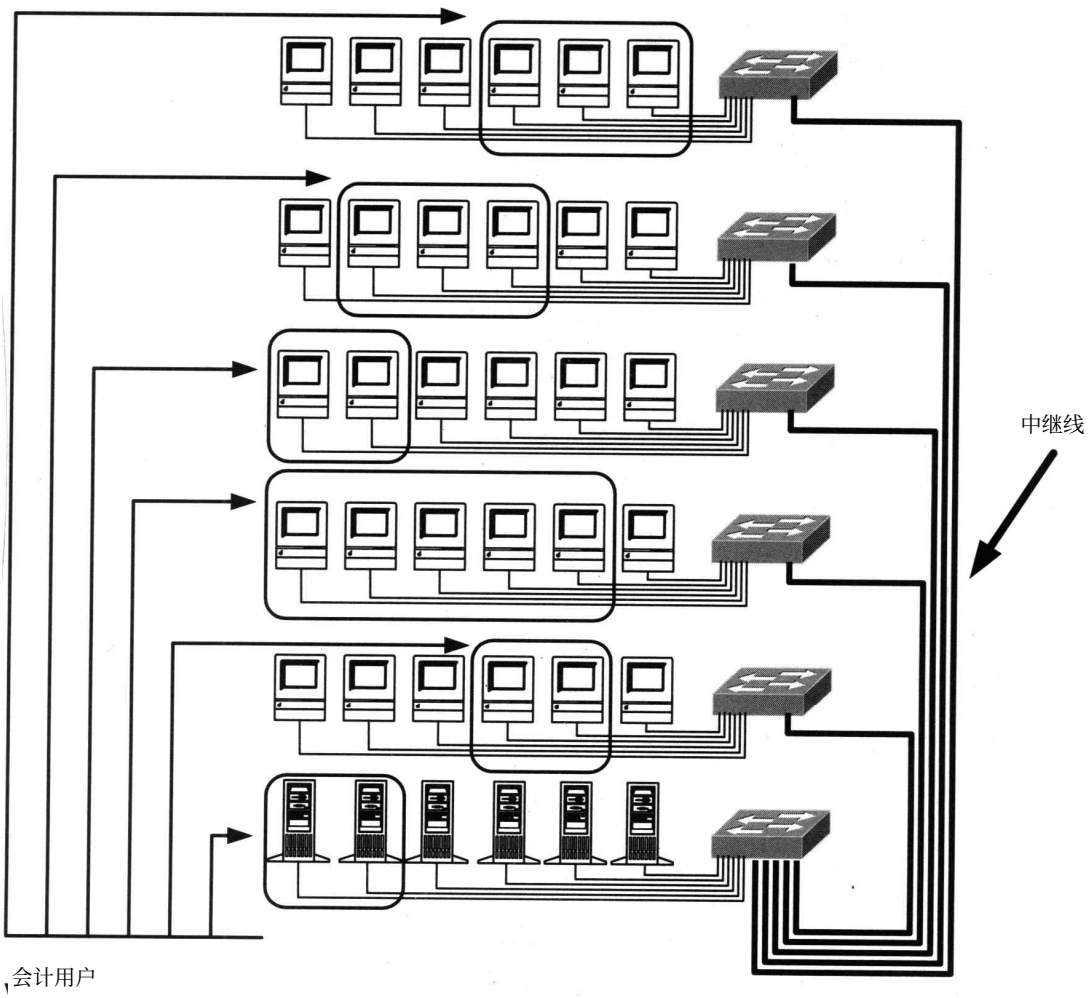


图4-7 会计VLAN

4.5 快速以太网和千兆以太网上的中继

在网络中，几乎Catalyst交换机能够支持的任何介质都可以作为中继线。其中，在快速以太网和千兆以太网上实现中继可使用下面两种类型的标记：

1) Inter-Switch 连接。

2) IEEE 802.1Q。

ISL（Inter-Switch Link，交换机间通信）标记是Cisco特有的一种标记，它主要使用在快速以太网的中继线上。 IEEE 802.1Q标记是一种标准的标记，某些（但不是所有的） Cisco Catalyst交换机线路卡可以支持它。中继可以通过线路模块上的 ASIC（application-specific integrated circuit，专用的集成电路）来实现，所以，线路模块应该包含所必须的 ASIC。由于

中继取决于硬件，所以，对Catalyst的软件进行更新并不能使中继进行更新。在不是所有的交换机都是Cisco Catalyst交换机的场合，使用IEEE 802.1Q标记。

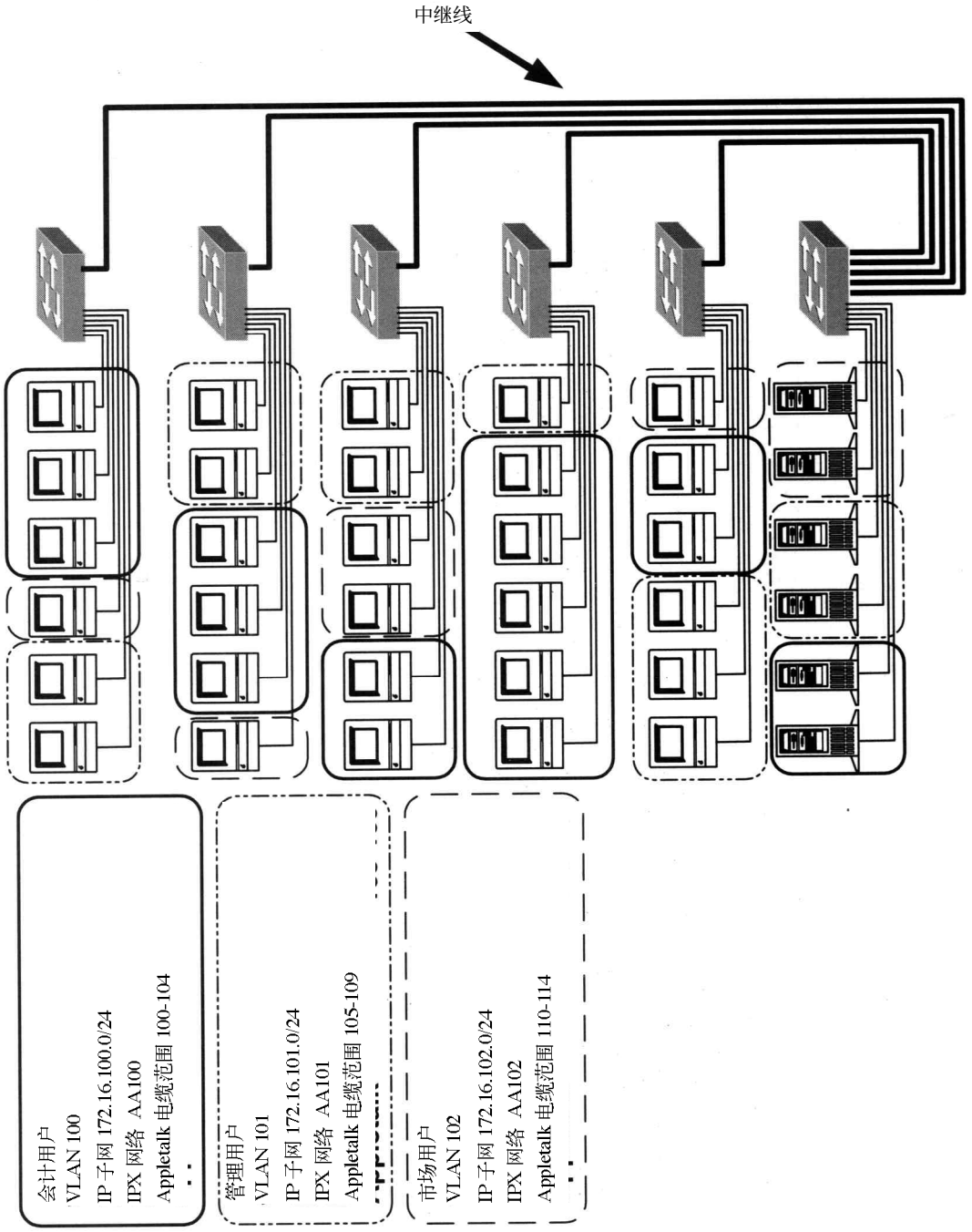


图4-8 3个VLAN的第三层寻址方案

4.5.1 ISL

主要由Cisco Catalyst 交换机构成的网络环境中的快速以太网和千兆以太网的中继线中，

通常使用ISL标记。图4-9给出了ISL标记的字段分析。

字 段	说 明	位 数
目标地址	发往中继端口的多点传送地址	40
类型	标识封装帧[以太网-0000，令牌环-0001，FDDDI-0010，ATM-0011]	4
用户	可能加到类型字段，在以太网中，可以用它定义属性	4
源地址	传输交换机的源MAC地址	48
长度	确定帧的长为，排除目标地址、类型、用户、源地址、长为和FCS字段	1 6
AAAA03	这是标准的IEEE 802.2逻辑链路控制报头	24
HSA	确定源工作站的厂商代码或OVI	24
ALAN	15位的字段，用于确定封装帧的VLAN，当前只使用了低10位，这将提供最大的1024个可能的VLAN数字	15
BPDU	确定是否封装的帧是BPDU.如果设置，还可以确定封装的帧作为一个Cisco发现信息包	1
索引	用于诊断	16
保留	用于添加信息	16
总位		208位或26字节

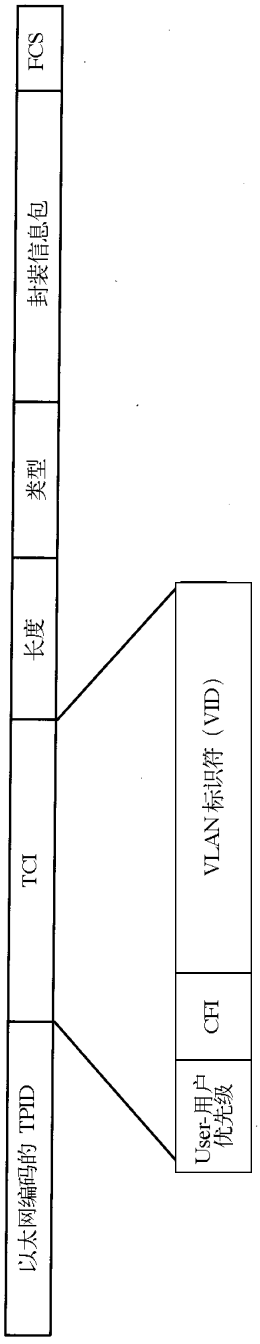
图4-9 ISL标记

在这个报头中，最重要的字段是VLAN字段。它用来标识包含封装帧的VLAN。需要注意的是，非Cisco的设备不能读取ISL标记。

4.5.2 IEEE 802.1Q

在1998的下半年，IEEE还在进行最后的IEEE 802.1 Q标准的草案设计，这时，制定标记格式的工作已经全部完成了。IEEE 802.1 Q和ISL不一样，它的格式取决于使用它的介质 。例如，ISL一般只适应快速以太网和千兆以太网，而802.1Q几乎适应所有的不同介质，其中包括FDDI和令牌环。

以太网的标记形式列在图 4-10中。



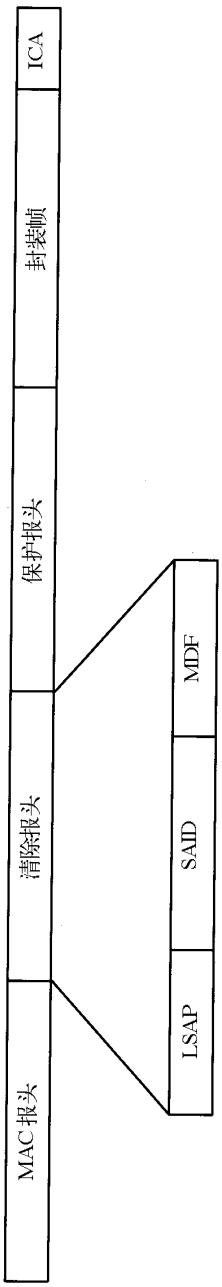
字　段	说　明	位　数
以太网编码的标记协议标识符(TPID)	用于标识此帧作为一个标记的帧。对于此字段，当前有一个可能的值，即0x8100	16
标记控制信息(TCI)	此名称给出下面列出的三个字段	16
用户优先级	根据iso/IEC 15802-3 识别压缩帧的优先级，可能的值范围为0-7	3
规范格式标识符（CFI）	确定此帧是否是规范的格式	1
VLAN标识符（VID）	唯一地标识封装的帧所属于的VLAN。此字段将提供最多有4094个VLAN	12
帧检查序列	每次一个帧是未标记的时，将进行FCS验算	

图4-10　IEEE 802.1Q以太网-编码标记报头

IEEE 802.1Q的标记报头将随使用介质的basis发生变化。按草定的IEEE 802.1Q标准，标记实际上嵌在源MAC地址和目标MAC地址后。由于这个标记要比Cisco的ISL小，所以将出现稍低的开销。Cisco通常将这种中继封装的方法称为“ dot1q ”，IEEE 802.1Q标记格式需要Catalyst IOS 4.1。

4.6 中继和FDDI

随着中继在FDDI上的实现，Cisco可以使用一种不同形式的标记。在这种情况下，Cisco



字 段	说 明	位 数
LSAP	标准802.2 LLC服务访问点，指出一个802.10 VLAN帧	24
SAID	唯一地标识封装帧的VLAN	32
管理定义的字段	此字段包含管理定义的信息	
完整性检查值	一种安全性算法，用于验证帧的完整性，与帧检查序列类似	

图4-11 对FDDI中继线，Cisco使用IEEE 802.10报头

使用IEEE 802.1Q的 SILS（共用LAN/MAN安全的LAN/MAN标准）的帧报头作为一种标记，在通过被配置成中继线的 FDDI环发送帧时使用。在 1992年末，为了维护网络的安全， Cisco研制了 802.10标准，但是这个标准很少使用。 Cisco使用 802.10报头的 SAID（security association identifer，安全关联标识符）字段作为它的 VLAN标识符，如图4-11所示。

802.10标准需要两种报头，即清除报头和保护报头。其中保护报头是一种加密的报头。源MAC地址既可以放在保护报头中，也可以放置在清除报头中。目标节点将清除报头中的MAC地址与保护报头的MAC地址进行核对。如果它发现两个地址不一样，就将帧丢弃，并作出数据被修改的假设。当 Cisco实行802.10标准时，只有LSAP和SAID字段是必要的，这样可以节省开销。

4.7 ATM和中继

在ATM中，可以通过使用一种标准的 LANE（LAN仿真）ATM过程来实现中继。不过在实现中继时，添加标记方法与快速以太网和 FDDI中所讨论的方法不一样。其实， LANE是一个很难理解的和很难实现的过程，它将在第 10章中加以讨论。

4.8 VLAN和生成树协议

当利用多个VLAN形成大型的网络时， STP（生成树协议）的随机性这一特点通常使网络形成一些并不适宜的拓扑结构。例如，在图 4-12中，网络上存在两个VLAN。以粗线表示的生

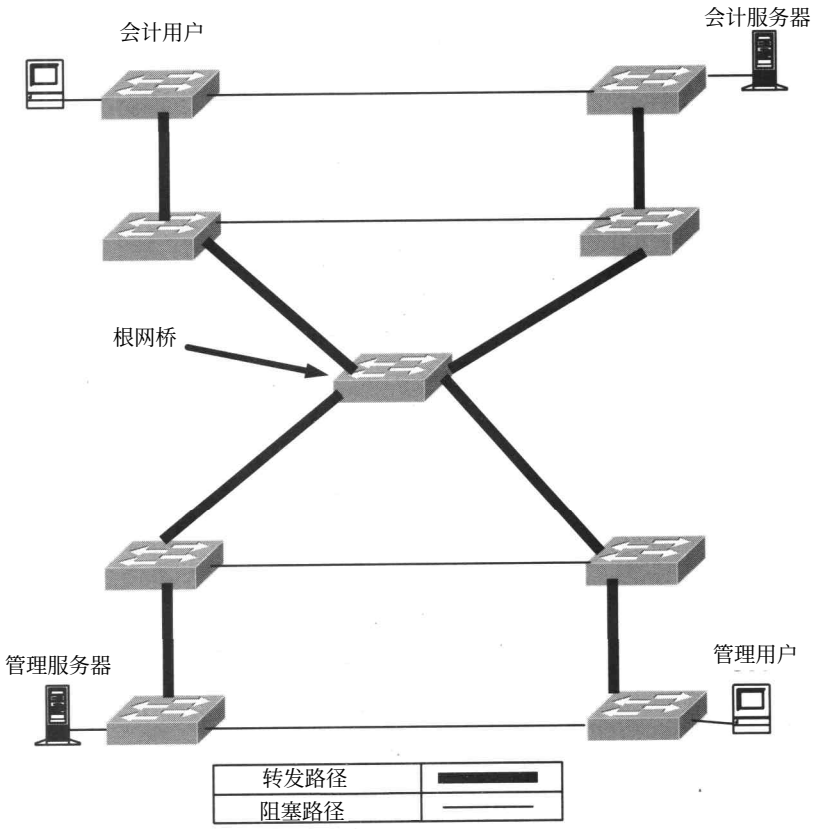


图4-12 不适宜的生成树结构

成树路径就形成了一个不适宜的网络环境。

在这种情形下，会计用户为了与会计服务器进行通信，就必须经过根网桥，同样，管理用户为了将信息传到管理服务器，也必须通过根网桥。解决的办法是使会计服务器的交换机成为根网桥。这样会确保会计用户与会计服务器进行通信时有一个更加直接路径（见图4-13）。

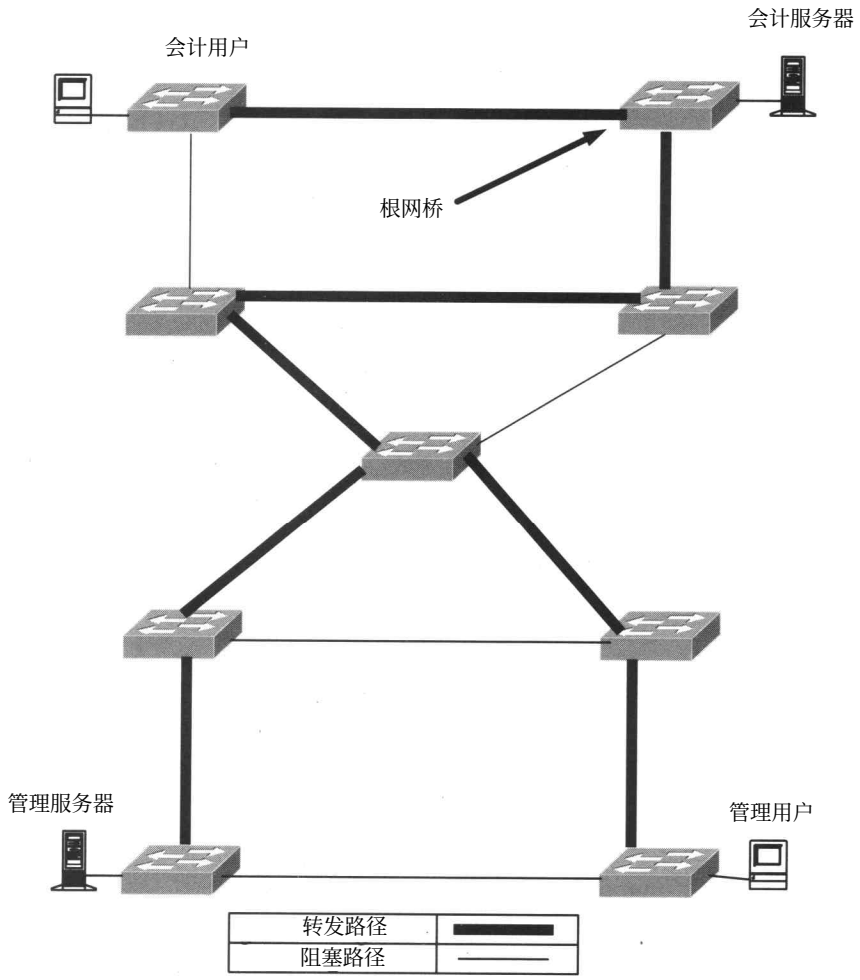


图4-13 会计用户，有直接路径；管理用户有非直接路径

但是，管理用户与管理服务器进行连接的路径仍然是间接的。Cisco可以在每个VLAN上都实现STP，这样就允许生成不同的基于VLAN的转发路径。由于每个VLAN上的STP相互独立，所以，会计VLAN可以将会计服务器交换机作为它的根网桥，反之，管理VLAN也可以将管理服务器交换机作为它的根网桥。图4-14为管理服务器作为根网桥的转发路径。

通常，转发的通信量属于哪个VLAN，它所遵循的转发路径就由哪个VLAN决定。如，会计VLAN的通信量遵循图4-13中所示的路径发送，而管理VLAN的通信量遵循图4-14所示的路径发送。需要注意的是两个不同路径的过程是同时进行的，如图4-15所示。

当然，管理VLAN中的通信量发送所遵循的路径与会计VLAN中所遵循的路径不一样。

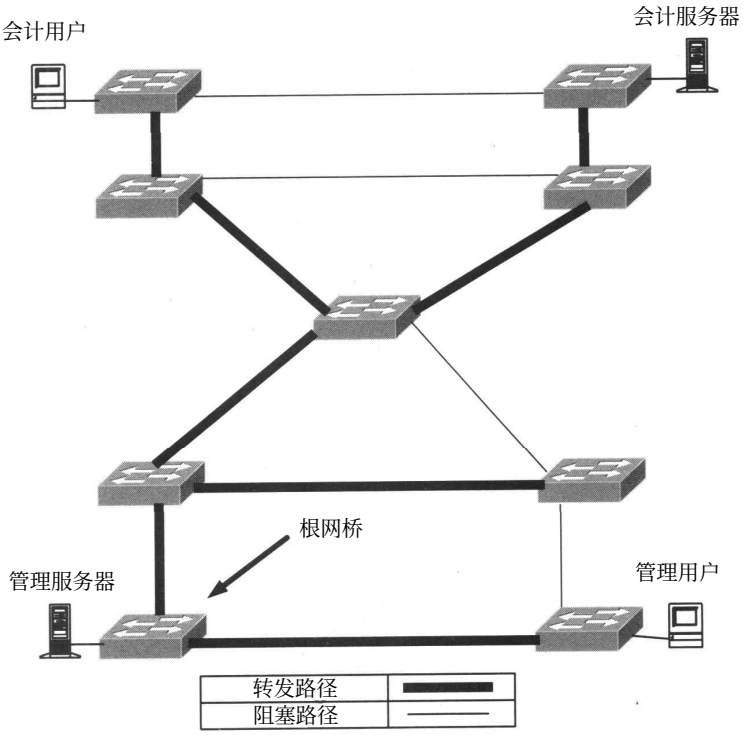


图4-14 管理服务器的交换机是管理VLAN的根网桥

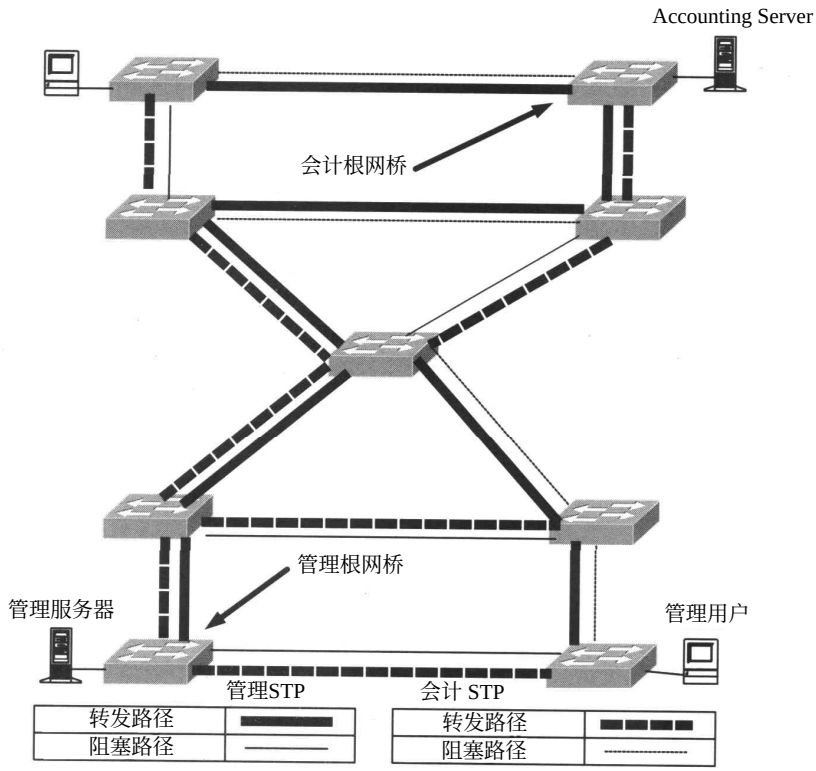


图4-15 会计和VLAN转发路径

4.9 路由器和VLAN

在前面曾提到，如果没有路由器，进行VLAN间通信是不可能的。路由器可以看作是两个广播域或VLAN之间的一个网关。每个VLAN中的接口都可以和交换机连接，如图4-16所示。

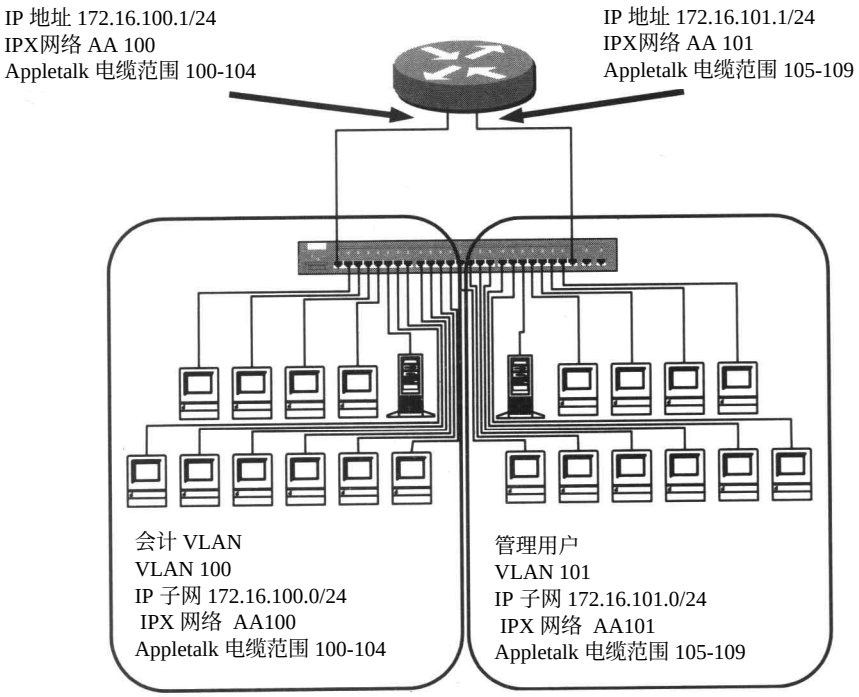


图4-16 VLAN上的独立接口

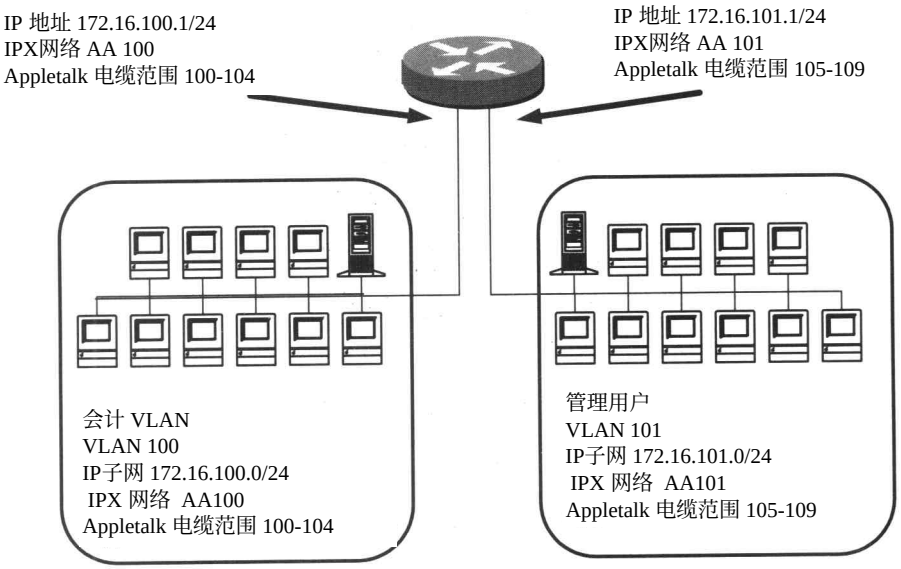


图4-17 图4-1中所示网络的逻辑配置

在这种情况下，工作站将通过路由器发送任何互连网络通信量。路由器的接口通常意识

不到它们和同一个交换机相连。它们只能监测到在网络中存在两个广播域或两个 IP子网、IPX网络和Appletalk电缆范围。图4-17中所示的路由器的配置与图 4-16中的路由器的配置完全相同。路由器只能对逻辑环境进行监测。

4.10 路由器中继

从图4-16中可以看出，为了进行路由，每个 VLAN都需要使用一个路由器接口 。所以，如果有100个VLAN，就需要100个路由器接口。很明显，这种配置有点昂贵。由于 Cisco路由器可以配置成中继线，所以它可以通过一个路由器接口对多个 VLAN进行路由。它所使用的介质决定供应商的兼容性。 Cisco路由器是唯一能够支持ISL的路由器。而且Cisco路由器也支持IEEE 802.1Q、IEEE 802.10中继方式和ATM的LANE（LAN仿真）。

例如，在图 4-18中，路由器配置成中继线，这样可以通过同一个接口进行会计和管理VLAN通信量的传送。

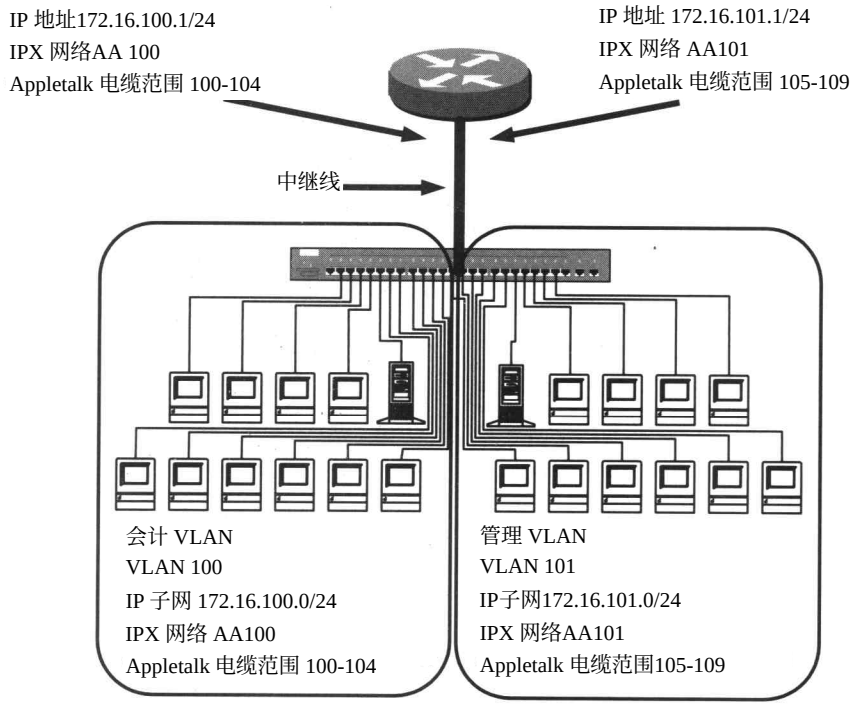


图4-18 中继到一个路由器

这种配置通常称为“ 棍子上的路由器（ router on stick）”，有时还被人们亲切地称为“ 单臂路由 ”。这种类型配置的优点是可以使用单一接口为多个 VLAN进行路由。其缺点是存在着接口不能提供足够的带宽来充分地处理 VLAN间通信量的可能性。可以通过使用以太网的子接口来对路由器进行配置，这部分内容将在第 8章中详细讨论。

4.11 服务器中继

在理想情况下，对于拥有如电子邮件服务等全局服务的服务器，如果想为每个 VLAN提供服务，那么，这个服务器就必须成为这些 VLAN的成员。如果全局服务器只存在于单一的VLAN中，那么其他VLAN必须将它们的通信量路由到全局服务器所在的 VLAN。这种情况的

出现将产生等待时间。

在图4-19中，如果邮件服务器只存在于管理 VLAN中，那么，会计用户将不得不通过中继线将通信量传送至路由器，路由器通过带有管理 VLAN标记的中继线将通信量传回。这加重

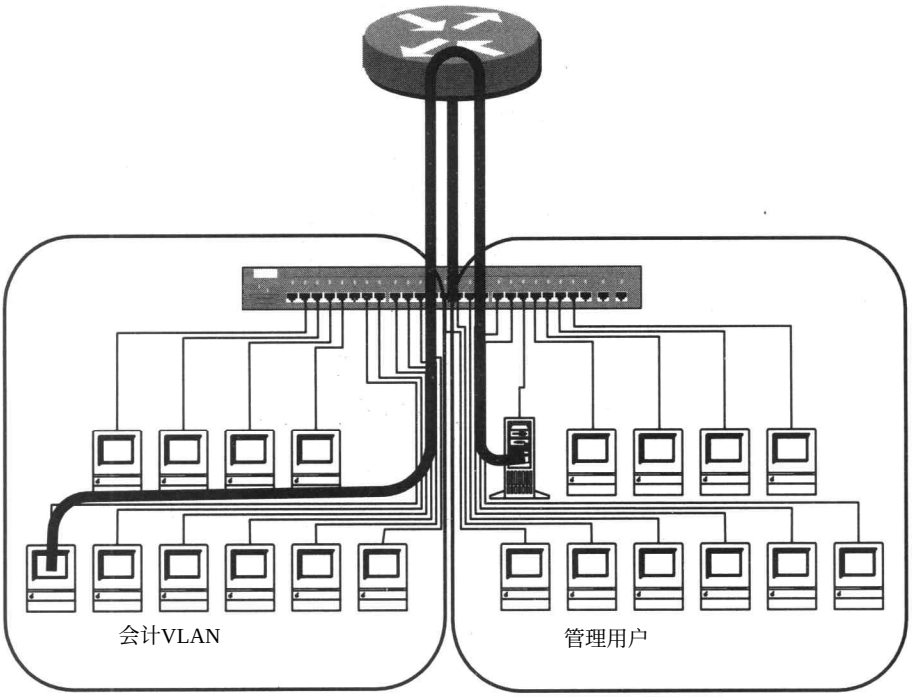


图4-19 路径通信量将从管理 VLAN送至邮件服务器

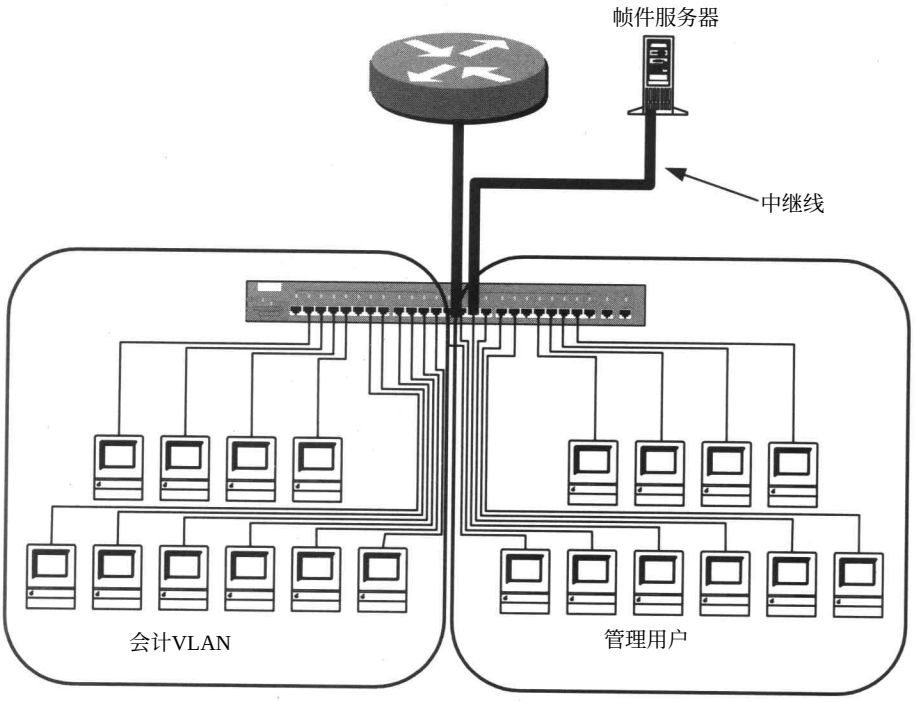


图4-20 配置邮件服务器以进行中继