第 3 章　虚拟局域网

虚拟局域网(Virtual LAN,VLAN)技术是在交换式以太网基础上发展起来的一种技术。利用这种技术,可以进一步提高交换式以太网的传输效率,增强网络的安全性,降低网络的管理成本。本章将对虚拟局域网的工作原理和组网方法进行介绍和讨论。

3.1　VLAN 的提出

交换式以太网是以交换机为中心的以太网。尽管交换式以太网的工作效率比共享式以太网提高很多,但是在应用中也暴露出一些问题。

3.1.1　交换式以太网的主要问题

交换式以太网的主要问题表现为广播风暴、网络安全性和网络的可管理性。

1. 广播风暴

在交换式以太网中,交换机具有一定的处理能力,能够将一个接口收到的数据,转发至另一个接口。交换机可连接共享式以太网,以分割冲突域,减小冲突的范围和冲突概率。但是,利用交换机组网并不能减小广播帧的传播范围。即使全网采用主机直连交换机的全双工方式,不存在冲突的情况下,也不能减小广播帧的传播范围。

对于目的 MAC 地址指向一台特定主机的数据帧,交换机按照接口/MAC 地址映射表进行转发。但是,对于目的 MAC 地址为 ff-ff-ff-ff-ff-ff 广播地址的数据帧,交换机将向除接收接口之外的所有接口转发数据帧,以保证网中的所有主机都能接收到该数据帧。

广播帧能够传播的范围称为广播域。在交换式以太网中,一台主机发送的广播帧总会转发到网络中的所有结点,因此,整个以太网就是一个广播域。无论这个以太网中连接了多少主机,级联了多少交换机,分割成了多少个冲突域,它们都在一个广播域中。

图 3-1 是由 4 台交换机级联而成的以太网。按照交换机转发数据帧的规则,如果其中一台主机(如主机 A)发送广播帧,网中的所有主机都会收到,因此图中所有主机都在一个广播域中。

尽管在设计网络应用时都会对广播帧的使用进行认真的考虑,但是网络中广播帧的出现频率仍然很高,很多功能(如以后将要讨论的 ARP 功能等)需要通过发送广播帧实现。即使有些主机与这些广播帧无关,它们也需要接收并进行处理。在大规模以太网中,频繁出现的广播帧占用了网络带宽和主机的处理资源,降低了网络效率。在有些情况下,同时出现的大量广播帧会造成网络阻塞,瘫痪整个网络,这就是广播风暴。

2. 网络安全性

以太网中的主机处于一个广播域中,因此,一台主机发送的广播帧会转发到所有主机。即使主机发送的不是广播帧,交换机依据接口/MAC 地址映射表进行转发时,也有可能将数据转发给无关的主机。

在图 3-2 中,当主机 A 向主机 E 发送数据时,由于交换机 1 和交换机 2 的接口/MAC 地

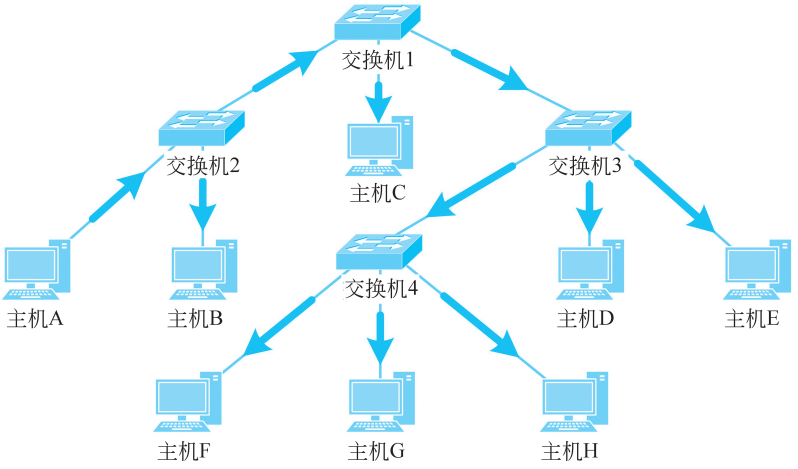
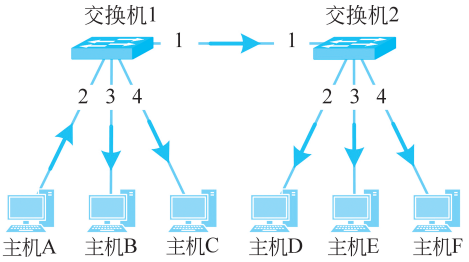


图 3-1　以太网中的广播域

址映射表中都没有关于主机 E 在哪个接口的信息，因此，交换机 1 和交换机 2 都会向接收接口之外的所有接口转发数据。主机 B、主机 C、主机 D、主机 F 都会收到该信息。

交换机1的地址映射表	
端口	MAC地址
1	52-54-4C-19-3D-03(主机D)
1	00-50-BA-27-5D-A1(主机F)
3	00-30-80-7C-F1-21(主机B)
2	00-00-B4-BF-1B-77(主机A)



交换机2的地址映射表	
端口	MAC地址
1	00-30-80-7C-F1-21(主机B)
2	52-54-4C-19-3D-03(主机D)
4	00-50-BA-27-5D-A1(主机F)
1	00-E0-4C-49-21-25(主机C)

图 3-2　无关主机接收到主机 A 发送给主机 E 的信息

如果网络中存在恶意用户，那么就可以收集和分析这些零零散散的数据，以达到自己的目的。为此，需要对不同类型的用户进行隔离，以防止网络安全问题的发生。

3. 网络的可管理性

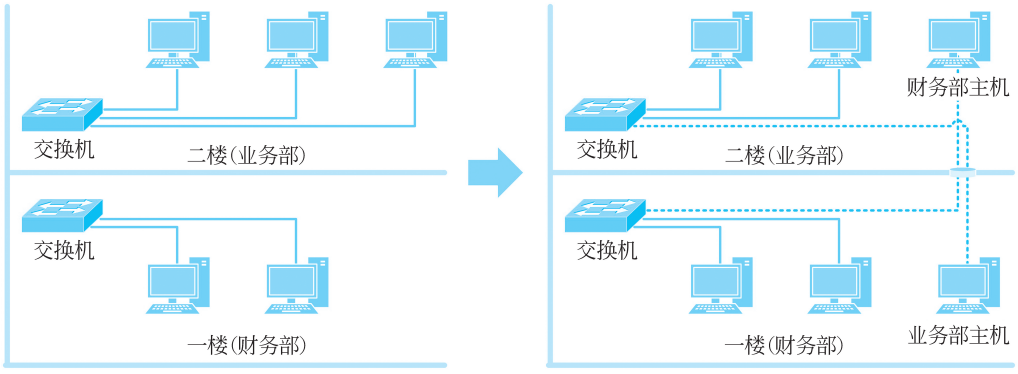
以太网的可管理性相对较差，运营和管理成本较高。例如，某单位办公楼的一层为财务部，二层为业务部。为了保证财务部的信息不外流，单位为财务部和业务部分别在一层和二层组建了以太网。这两个以太网不能相互连接，以防财务部的数据转发到业务部的主机中，如图 3-3(a)所示。如果随着业务的发展，单位在一楼为业务部分配了一个房间，那么为了将业务部的主机连入业务部网络，需要重新进行布线，即使这些计算机连入一层财务部的交换机更方便，如图 3-3(b)所示。同样，业务部的人员调入财务部，但办公位置希望不变，那么也需要重新布线，将该人员的主机连入一楼的交换机，如图 3-3(b)所示。

网络运营和管理成本的提高，增加了用户的负担。因此，需要使用新技术简化网络的管理，降低运营和管理成本。

3.1.2　认识虚拟局域网

为了解决交换式以太网的广播风暴问题、网络安全性问题和可管理性问题，人们开始使用虚拟局域网 VLAN 进行以太网组网。

现在，人们对虚拟主机的概念已经非常熟悉。一台实体主机可以运行多个虚拟主机，虚拟



(a) 按规划组建的以太网　　(b) 随业务和员工的变化重新布线

图 3-3　以太网的管理

主机之间相互隔离。人们可以像操作实体机一样操作一台虚拟主机，好像这台实体机上的其他虚拟主机不存在一样。虚拟交换机的概念与虚拟主机的概念类似，它可以在一台实体交换机上运行多个虚拟交换机，多个虚拟交换机之间相互独立。利用一个虚拟交换机组成的网络称为一个虚拟局域网。一个虚拟局域网与另一个虚拟局域网互不影响，好像它们就是用多个实体交换机组成的网络一样。

图 3-4 是一个虚拟局域网示意图。图中，一台实体交换机中虚拟了 3 台虚拟交换机。在用户看来，虚拟交换机 1、虚拟交换机 2 和虚拟交换机 3 相互独立，就好像它们是 3 台独立的实体交换机一样。主机 A 和主机 B 通过实体交换机端口 1 和端口 2 连接到虚拟交换机 1，形成虚拟局域网 VLAN1；主机 C 和主机 D 通过实体交换机端口 3 和端口 4 连接到虚拟交换机 2，形成虚拟局域网 VLAN2；主机 E 和主机 F 通过实体交换机端口 5 和端口 6 连接到虚拟交换机 3，形成虚拟局域网 VLAN3。VLAN1、VLAN2 和 VLAN3 之间互不影响，为 3 个独立的以太网。

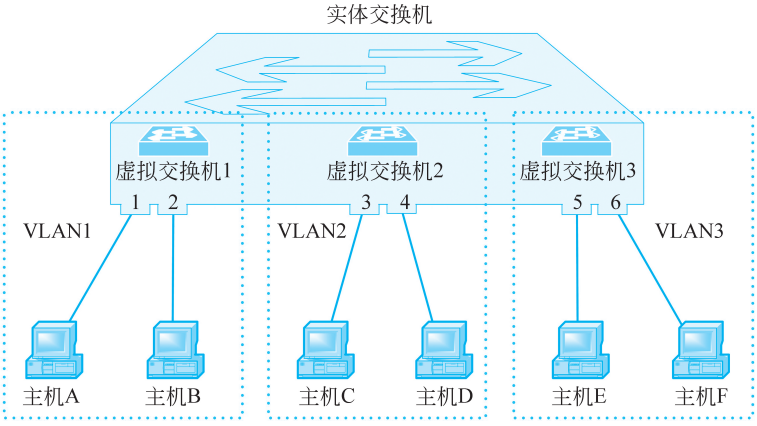


图 3-4　虚拟局域网示意图

交换机具有强大的处理能力，它可以对收到的数据帧进行处理，控制其流动的方向和路径。这种处理能力是实现虚拟局域网的基础。在图 3-4 中，如果实体交换机从端口 1 收到数据帧后不向除端口 2 之外的端口转发，从端口 2 收到数据帧后不向除端口 1 之外的端口转发，那么从用户看来，主机 A 和主机 B 就是一个独立的网络。这个网络与主机 C 和主机 D 形成

的网络、主机 E 和主机 F 形成的网络相互隔离，互不影响。

利用虚拟局域网技术，可以将连入一台实体交换机的多个主机划分成若干逻辑工作组，逻辑工作组中的主机可以根据功能、部门、应用等因素划分，无须考虑它们所处的物理位置。实体交换机通过控制数据帧的流向，保证一个逻辑工作组中的数据帧只在该工作组内部流动，不会转发到其他逻辑工作组。

虚拟局域网技术的使用，有效地解决了以太网原有的广播风暴、网络安全性、可管理性等问题，被广泛应用于以太网组网之中。

（1）VLAN 技术有效地降低了广播风暴风险：使用 VLAN 技术以后，交换机在收到广播帧后首先判断发送主机所属的 VLAN，然后向属于该 VLAN 的主机转发广播帧。在图 3-5 显示的以太网中，主机 A、主机 B 和主机 C 属于 VLAN1，主机 D 和主机 E 属于 VLAN2。当交换机收到主机 A 发送的广播帧后，只会向主机 B 和主机 C 转发。主机 D 和主机 E 不会收到该广播帧。由于一个 VLAN 中的广播帧，不会出现在其他 VLAN 中，因此一个 VLAN 就是一个广播域。在使用 VLAN 之后，原有的大广播域被分割成多个小广播域，有效地降低了广播风暴发生的风险。

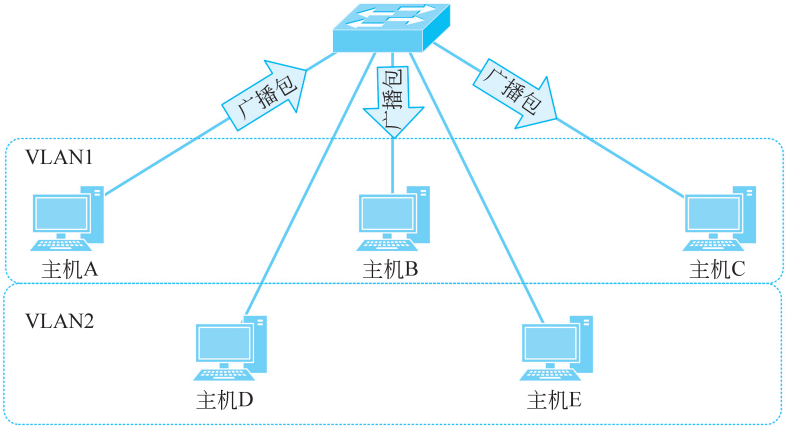


图 3-5　利用 VLAN 分割广播域

（2）VLAN 技术增强了网络的安全性：不但一个 VLAN 中的广播帧不会传播到其他 VLAN，一个 VLAN 中的其他数据帧也不会传播到其他 VLAN。不同 VLAN 之间的数据相互隔离的特性，增强了网络的安全性。

（3）VLAN 技术增强了网络的可管理性：在组网完成后，网络管理员利用 VLAN 技术通过软件就可以对用户进行工作组的划分，无须考虑他们所在的物理位置，节省了重新布线等管理和运营开销。

3.2　VLAN 的划分方法

VLAN 的划分可以根据功能、部门或应用而无须考虑主机的物理位置。属于同一个 VLAN 中的主机可以相互发送信息，共享同一个广播域，不同 VLAN 中的主机不能相互通信。

VLAN 的划分方法分为两种，一种是静态 VLAN 划分方法，另一种是动态 VLAN 划分方法。其中，动态 VLAN 划分方法又包括基于 MAC 地址、基于互联层协议、基于 IP 组播、基于

策略等多种方法。不同的划分方法有不同的特点，其区别主要表现在对 VLAN 成员的定义上。在组建以太网时，网络管理员需要按照网络应用环境的不同选择合适的划分方法。本节对基于接口的静态 VLAN 划分方法、基于 MAC 的动态 VLAN 划分方法和基于互联层协议的动态 VLAN 划分方法进行介绍。

3.2.1 基于接口的静态 VLAN 划分方法

在实际工作中，基于接口的静态 VLAN 是最实用也是最常用的一种 VLAN。静态 VLAN 通过网络管理员静态地将交换机上的接口划分给某个 VLAN，从而把主机划分为不同的部分，实现不同逻辑组之间的相互隔离。划分后的接口与 VLAN 之间一直保持这种配置关系，直到人为改变它们。

在图 3-6 所示基于接口的静态 VLAN 划分方法中，以太网交换机接口 1、2、4、6 被划分到 VLAN1，接口 3、5 被划分到 VLAN2。按照网络管理员的配置指令，交换机形成 VLAN 与其接口的对照表。从一个接口收到数据帧后，交换机首先通过接口/MAC 地址映射表查找需要转发的接口，然后再通过 VLAN 成员对照表判定需要转发的接口是否与接收接口同属一个 VLAN。如果同属一个 VLAN 则转发，否则就抛弃。这样，保证一个 VLAN 中的数据不会转发到另一个 VLAN。例如，在图 3-6 给出的示意图中，由于接口 1 属于 VLAN1，因此交换机从该接口收到的数据帧，只可能转发给 VLAN1 拥有的接口 2、4、6，其他接口（接口 3、5）不会收到该帧的任何信息。

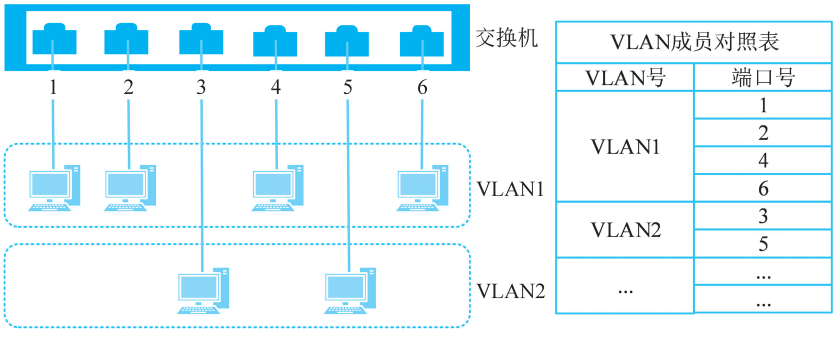


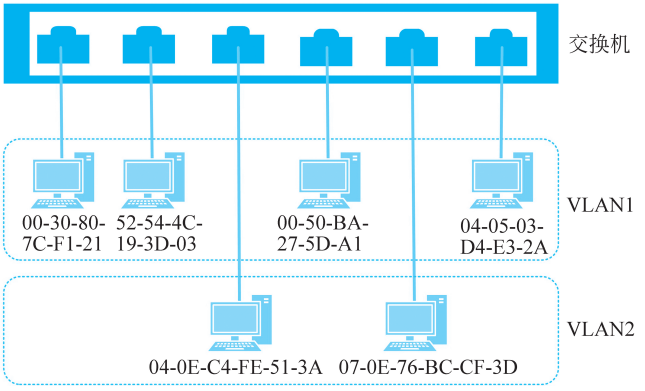
图 3-6 基于接口的静态 VLAN 划分方法

尽管静态 VLAN 划分方法需要网络管理员通过配置交换机进行更改，但这种方法安全性高，配置简单并可以直接监控，因此，很受网络管理人员的欢迎。特别是主机位置相对稳定时，应用基于接口的静态 VLAN 划分方法是一种最佳选择。

3.2.2 基于 MAC 地址的动态 VLAN 划分方法

在以 MAC 地址为基础划分 VLAN 时，网络管理员可以指定一个 VLAN 包含哪些 MAC 地址。如果一台主机的 MAC 地址与 VLAN 包含的一个 MAC 地址相同，那么这台主机就属于这个 VLAN。在图 3-7 给出的例子中，由于 VLAN1 包含的 MAC 地址为 00-30-80-7C-F1-21、52-54-4C-19-3D-03、00-50-BA-27-5D-A1 和 04-05-03-D4-E3-2A，因此拥有这些 MAC 地址的主机属于 VLAN1；由于 LAN2 包含的 MAC 地址为 04-0E-C4-FE-51-3A 和 07-0E-76-BC-CF-3D，因此拥有这两个 MAC 地址的主机属于 VLAN2。在基于 MAC 地址的动态 VLAN

中,判断一台主机属于哪个 VLAN,不是依据它所连接的交换机接口,而是根据它拥有的 MAC 地址。无论是从一个位置移动到另一个位置,还是从一个接口换到另一个接口,只要主机的 MAC 地址不变(即主机使用的网卡不变),这台主机就属于原来的 VLAN。



VLAN成员对照表	
VLAN号	MAC地址
VLAN1	00-30-80-7C-F1-21
	52-54-4C-19-3D-03
	00-50-BA-27-5D-A1
	04-05-03-D4-E3-2A
VLAN2	04-0E-C4-FE-51-3A
	07-0E-76-BC-CF-3D
...	...
	...

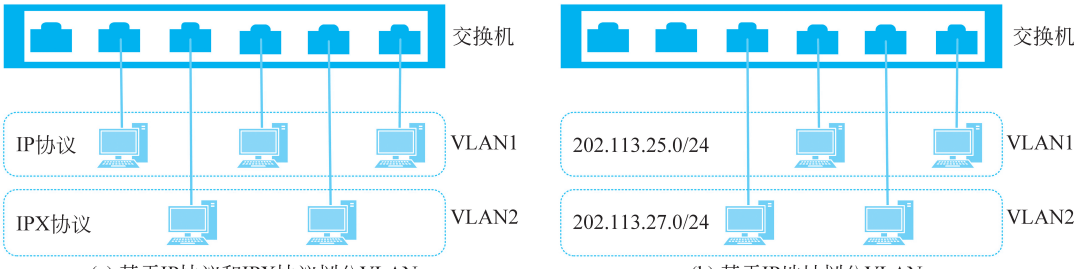
图 3-7　基于 MAC 地址的 VLAN 划分

采用这种划分方法,需要将网络中每台主机的 MAC 地址绑定到特定的 VLAN。如果网络的规模比较大,网络管理员初始的配置工作量相当大。另外,当用户的主机更换网卡后,网络管理员也需要对 VLAN 的配置进行相应的改变。

3.2.3　基于互联层的 VLAN 划分方法

基于互联层的 VLAN 划分方法根据互联层使用的协议(如 IP、IPX[①])、互联层的地址(如 IP 地址)定义 VLAN 中的成员。基于互联层的 VLAN 划分方法特别适合于针对具体应用和服务组织用户,用户可以在网络内部自由移动,而不用重新配置交换机。

图 3-8 给出了基于互联层的 VLAN 划分方法示意图。在图 3-8(a)中,使用 IP 的网络用户被划入 VLAN1,使用 IPX 协议的用户被划入 VLAN2。在图 3-8(b)中,IP 地址属于 202.113.25.0/24 的所有结点划归为 VLAN1,IP 地址属于 202.113.27.0/24 的所有结点划归为 VLAN2。



(a) 基于IP协议和IPX协议划分VLAN　　(b) 基于IP地址划分VLAN

图 3-8　基于互联层的 VLAN 划分方法

采用该 VLAN 管理策略,交换机不仅需要分析数据帧的头部信息(如源地址、目的地址等字段),而且还需要深入数据帧的数据区域读取和分析高层协议信息,因此,交换和转发速率会受到一定的影响。

① IPX 是一种与 IP 类似的网络互联协议,主要应用于 Novell 网络的应用中。本书不介绍 IPX 的详细内容。

3.3 跨越交换机的 VLAN

随着 VLAN 应用越来越广泛，人们不再满足在一台交换机上划分 VLAN，很多网络应用环境要求 VLAN 能够跨越交换机。

图 3-9 显示了一个 VLAN 跨越交换机的连网方式。实体交换机 1 和实体交换机 2 分别虚拟了 3 台虚拟交换机，交换机 1 的第 7 端口和交换机 2 的第 7 端口进行级联。其中，虚拟交换机 11 通过实体交换机 1 的端口 7 连接实体交换机 2 的端口 7，而后再连接虚拟交换机 23，形成由虚拟交换机 11 和虚拟交换机 23 构成的虚拟局域网 VLAN1；虚拟交换机 12 通过实体交换机 1 的端口 7 连接实体交换机 2 的端口 7，而后再连接虚拟交换机 22，形成由虚拟交换机 12 和虚拟交换机 22 构成的虚拟局域网 VLAN2；虚拟交换机 13 通过实体交换机 1 的端口 7 连接实体交换机 2 的端口 7，而后再连接虚拟交换机 21，形成由虚拟交换机 13 和虚拟交换机 21 构成的虚拟局域网 VLAN3。

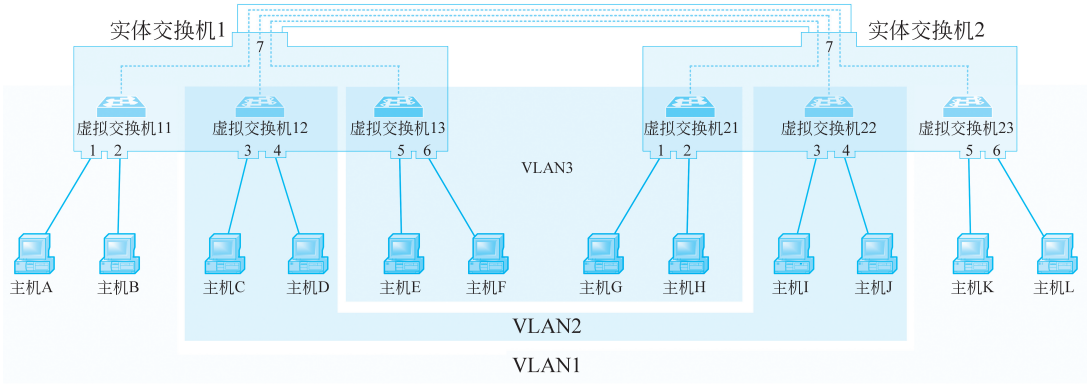


图 3-9 跨越交换机的 VLAN

图 3-9 中实体交换机 1 的端口 7 和实体交换机 2 的端口 7 被 VLAN1、VLAN2 和 VLAN3 共享。但是，这种共享不应被用户感觉到，每个 VLAN 中的用户（如 VLAN1 中的主机 A、主机 B、主机 K 和主机 L）应该觉得实体交换机之间的连接只有这个 VLAN 在使用。因此，VLAN 跨域交换机时，进行交换机级联的实体端口和实体中继线也需要虚拟，形成多个逻辑端口和逻辑中继线，以便跨越交换机的 VLAN 使用。这样，在跨域交换机时，一个 VLAN 中的数据就不会进入另一个 VLAN，实现 VLAN 之间的隔离。

下面，从 VLAN 跨越交换机时遇到的问题出发，讨论其具体的解决方法。为了讨论方便，本节以基于端口的 VLAN 划分方法为例进行介绍。

3.3.1 多交换机上的 VLAN 与 IEEE 802.1Q

与单交换机上划分 VLAN 不同，多交换机上划分 VLAN 时，交换机上存在共享端口，多个 VLAN 的数据可能在这个共享的端口上流动。共享端口的存在，使得单交换机上划分 VLAN 与多交换机上划分 VLAN 有很大的不同。解决跨越交换机 VLAN 的主要方法是在共享端口上运行 IEEE 802.1Q 协议。

1. IEEE 802.1Q 协议的提出

支持 VLAN 的交换机通常需要保存各个 VLAN 与其拥有成员的对照表，如图 3-6 所示。

在采用基于端口的 VLAN 划分方法时，VLAN 与其成员对照表包含了每个 VLAN 拥有的端口号。从一个端口收到的数据帧只可能转发到与该端口处于同一个 VLAN 中的端口上。

当 VLAN 在单一交换机上实现时，交换机接收时即可掌握接收帧的输入端口，从而可以通过 VLAN 成员对照表判定该帧所属的 VLAN 和该帧的转发去向。例如，在图 3-6 中，交换机在端口 1 接收到帧时，可以通过 VLAN 成员对照表知道该帧属于 VLAN1。这个帧只可能转发给端口 2、端口 4 或端口 6。

但是，当 VLAN 跨越两台或多台交换机时，由于连接交换机与交换机的中继线需要传递属于多个 VLAN 的数据帧，因此，仅依靠每个交换机中存储的 VLAN 成员对照表很难知道一个帧属于哪个 VLAN，一个帧应该转发到哪个端口。

例如，在图 3-10 中，VLAN1 包含了交换机 1 的端口 2 和端口 7，交换机 2 的端口 3 和端口 8；VLAN2 包含了交换机 1 的端口 5 和端口 10，交换机 2 的端口 6 和端口 11。交换机 1 的端口 12 与交换机 2 的端口 1 通过中继线相连。由于中继线上既要传输 VLAN1 的数据帧，又要传输 VLAN2 的数据帧，因此，交换机 1 的端口 12 和交换机 2 的端口 1 既属于 VLAN1，又属于 VLAN2，为 VLAN1 和 VLAN2 的共享端口。当交换机 1 收到从端口 2 到来的数据帧时，它通过查看自己的 VLAN 成员对照表，可以判定该数据帧属于 VLAN1，只可能向端口 7 和端口 12 转发。如果该帧向端口 12 转发，那么交换机 2 将在自己的端口 1 接收到该帧。由于交换机的端口 1 既属于 VLAN1，又属于 VLAN2，而收到的数据帧信息中又没有携带该帧从属于哪个 VLAN 或该帧是从交换机 1 的哪个端口接收的，因此交换机无法转发该帧。

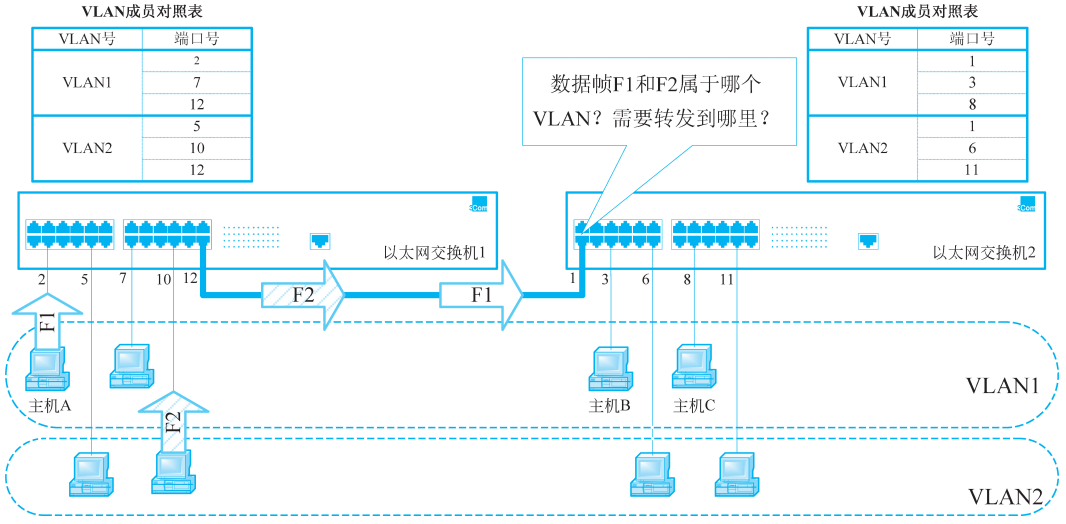


图 3-10　VLAN 跨越交换机的转发问题

为了解决交换机之间的 VLAN 信息交换问题，IEEE 推出了 IEEE 802.1Q 标准。IEEE 802.1Q 标准通过扩展标准的数据帧结构，使交换机之间转发的数据帧中携带所属的 VLAN 信息，从而使接收的交换机能够了解数据帧的转发方向。

2. 802.1Q 的主要内容

IEEE 802.1Q 是与 VLAN 相关的最重要的标准之一，主要用于在交换机和交换机之间、交换机和路由器之间、交换机和服务器之间传递 VLAN 信息和 VLAN 数据流。IEEE 802.1Q 标准是 VLAN 历史上的一块里程碑，由 IEEE 委员会 1999 年 6 月正式颁布实施。

VLAN 跨越交换机时出现问题的主要原因，是共享端口的存在使得不能分辨中继线上传输的数据属于哪个 VLAN 流。为了解决这个问题，IEEE 802.1Q 协议要求在向共享端口转发数据帧之前，需要向原有数据帧中添加携带 VLAN 信息的 802.1Q 标记，以使得另一台交换机的共享端口能够识别接收到的数据帧属于哪个 VLAN。共享端口接收到携带 802.1Q 标记的数据帧后，如果需要向本机的非共享端口转发，必须将 802.1Q 标记去掉，以保证与原来的以太网兼容。扩展 IEEE 802.1Q 标记后的数据帧格式如图 3-11 所示。

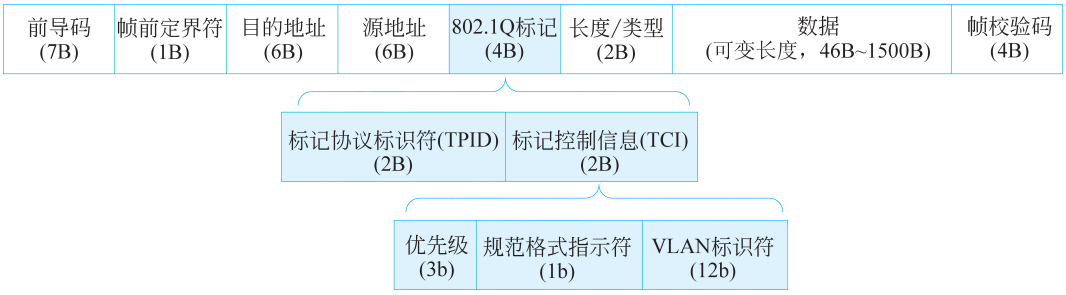


图 3-11　添加 802.1Q 标签后的数据帧格式

从图 3-11 可以看到，IEEE 802.1Q 标记添加在标准数据帧的源地址之后。IEEE 802.1Q 标记由标记协议标识符（Tag Protocol Identifier，TPID）和标记控制信息（Tag Control Information，TCI）两部分组成。

（1）标记协议标识符（TPID）占用 2B，用于指示所采用协议的协议类型，取值为 8100H。当交换机的输入端口检测到该字段为 8100H 时，就可断定该帧为携带 802.1Q 标记的数据帧。

（2）标记控制信息（TCI）中包含 VLAN 的具体信息，由用户优先级（User Priority）、规范格式指示符（Canonical Format Indicator，CFI）和 VLAN 标识符（VLAN IDentifier，VID）3 部分组成，占用 2B。其中，用户优先级占 3b，可以将用户分为 8 种不同的级别。交换机可以参考该字段值为帧转发制定不同的优先级别；规范格式指示符（CFI）长度为 1b，用于表明该帧是否符合以太网规范。在以太网交换机中，该位总被置为 0；VLAN 标识符（VID）的长度为 12b，用于标识该帧所属的 VLAN 号。由于 VID＝0 和 VID＝4095 留作他用，因此，IEEE 802.1Q 要求 VID 应该为 1～4094。

3.3.2　端口类型与帧处理规则

交换机的端口可通过命令配置为以下 3 种类型中的 1 种：①接入端口（access port）；②共享端口（trunk port，也称主干端口）；③混合端口（hybrid port）。其中，接入端口和共享端口一般交换机都可支持，而混合端口只有部分交换机可以支持。

1. 接入端口

接入类型的端口可用于连接主机等终端设备，也可用于交换机之间的级联。但是，接入类型的端口只能分配给一个 VLAN。管理员可以通过命令配置一个接入类型的端口属于哪个 VLAN。

交换机从接入类型的端口转发出去的数据帧都是不带 802.1Q 标记的数据帧，该帧一定是属于这个接入端口所属的 VLAN。即使原数据帧是带有 802.1Q 标记的数据帧，交换机在向接入类型的端口转发之前，也需要将 802.1Q 标记去掉，而后再从该接入端口发送出去。

交换机从接入类型的端口接收的数据帧都是不带 802.1Q 标记的数据帧，该帧属于这个

接入端口所属的 VLAN。如果从接入类型的端口收到了带有 802.1Q 标记的数据帧,交换机会将其丢弃。

2. 共享端口

共享类型的端口通常用于交换机之间的级联,它被多个 VLAN 共享,同时属于多个 VLAN。管理员可以通过命令配置一个共享类型的端口可以被哪些 VLAN 共享。

为了区分发送和接收数据帧所属的 VLAN,共享类型的端口上收发的数据帧需要添加 802.1Q 标记。

交换机在向共享类型的端口转发数据帧之前,需要判定该帧所属的 VLAN,进而形成带有 802.1Q 标记的数据帧。而后,再将带有 802.1Q 标记的数据帧从共享端口发送出去。

交换机从共享类型的端口接收的数据帧都是带有 802.1Q 标记的数据帧,解析该帧中 802.1Q 标记得到的 VLAN 号必须在该共享端口允许的 VLAN 范围内。如果解析出的 VLAN 号不在该共享端口允许的范围内,那么交换机会将该帧丢弃。例如,一个共享端口允许 VLAN2、VLAN3 和 VLAN5 共享,如果该端口收到一个 VID=VLAN3 的数据帧,那么交换机正常处理该帧;如果该端口收到一个 VID=VLAN4 的数据帧,那么交换机会将该帧丢弃。

3. 混合端口

混合类型的端口是接入类型和共享类型的混合,可以同时作为接入端口和共享端口。作为接入类型的端口,它可以被划分到一个 VLAN 中,传输不带 802.1Q 标记的数据帧;作为共享类型的端口,它可以被多个 VLAN 共享,传输带有 802.1Q 标记的数据帧。管理员可以通过命令配置一个混合端口属于哪个 VLAN(传送该 VLAN 的数据帧时无须携带 802.1Q 标记),同时,该端口可以被哪些 VLAN 共享(传送这些 VLAN 的数据帧时要携带 802.1Q 标记)。

交换机在从混合类型的端口发送数据帧时,需要判定该帧是否属于该混合端口所属的 VLAN。如果是,则向该端口转发不带 802.1Q 标记的数据帧;如果不是,则继续判定该帧是否属于共享该混合端口的 VLAN 范畴。如果属于共享 VLAN 的范畴,则向该端口转发带有 802.1Q 标记的数据帧;如果不属于共享 VLAN 的范畴,则丢弃该帧。例如,一个混合类型的端口被划分到 VLAN5 中,同时该端口被 VLAN2、VLAN3 和 VLAN4 共享。如果需要从该端口发送 VLAN5 的数据帧,那么不需要添加 802.1Q 标记;如果需要从该端口发送 VLAN3 的数据帧,那么需要在该数据帧中添加 VID=VLAN3 的 802.1Q 标记,然后再发送。

交换机从混合类型接收的数据帧可能不带 802.1Q 标记,也可能带有 802.1Q 标记。如果收到的帧不带 802.1Q 标记,那么该端口作为接入端口使用,收到的帧属于该混合端口所属的 VLAN。如果收到的帧带有 802.1Q 标记,那么该端口作为共享端口使用,收到的帧所属 VLAN 由 802.1Q 标记中的 VID 指定。与共享接口类似,如果收到帧所属 VLAN 不在共享该端口的 VLAN 范围之内,那么交换机也会将其丢弃。

3.3.3 802.1Q 交换机的数据帧处理过程

在 VLAN 组网中,网络管理员既可以将交换机的一个端口配置为共享端口,也可以配置为接入端口、混合端口。共享端口用于交换机之间的连接,能够支持 802.1Q 标记帧的发送和处理。而接入端口用于非 802.1Q 设备(如主机)的连接,需要发送和处理不带 802.1Q 标记的

数据帧。由于混合端口只有部分交换机支持，因此本节以共享端口和接入端口为例，介绍 802.1Q 交换机的数据帧处理过程。

图 3-12 显示了较为典型的 802.1Q 交换机的数据帧处理过程。假设交换机 1 的端口 12 通过中继线与交换机 2 的端口 1 相连，交换机 1 的端口 12 和交换机 2 的端口 1 为共享端口，支持 802.1Q 标记帧的发送和处理。同时，假设主机 A 向主机 B 发送数据帧 F_{AB}。

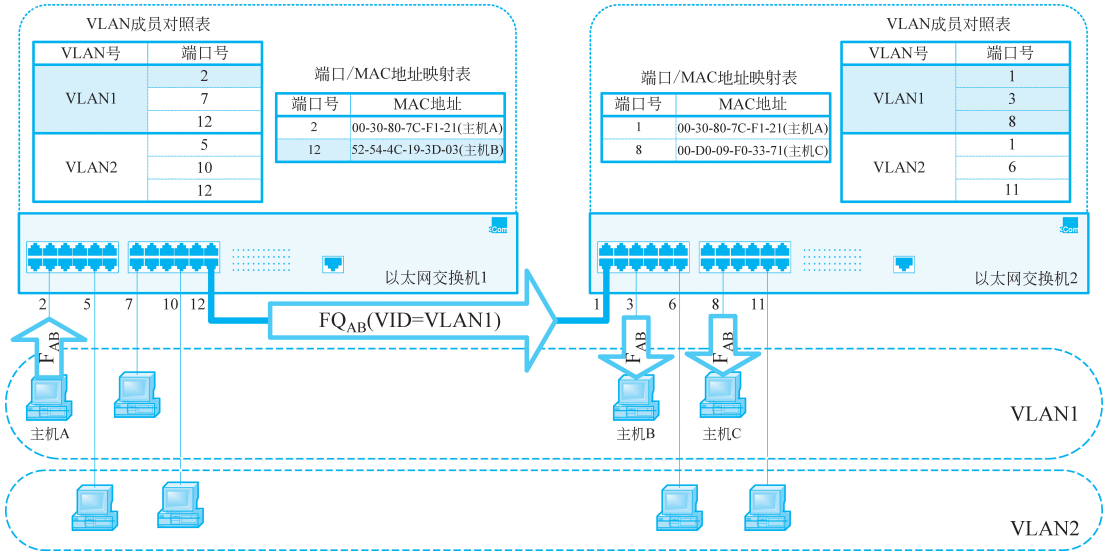


图 3-12　802.1Q 交换机的数据帧处理过程示意图

(1) 主机 A 形成数据帧 F_{AB}并开始发送，交换机 1 在端口 2 进行接收。由于主机 A 不支持 802.1Q 标准，因此，交换机 1 在端口 2 接收到的 F_{AB}没有 802.1Q 标记。

(2) 根据本地端口/MAC 地址映射表和 VLAN 成员对照表，交换机 1 决定 F_{AB}的转发去向。如果主机 B 的 MAC 地址出现在端口/MAC 地址映射表中，同时对应的端口号又为 VLAN1 的成员端口，那么交换机直接向该端口转发 F_{AB}；否则，交换机 1 需要向接收端口 2 之外的所有 VLAN1 的成员端口转发 F_{AB}。本例中，由于主机 B 的 MAC 地址对应于端口 12，而且端口 12 属于 VLAN1 的成员，因此，交换机直接将 F_{AB}转发至端口 12。

(3) 由于端口 12 为 802.1Q 共享端口，因此，交换机 1 首先在需要转发的 F_{AB}中插入 802.1Q 标记，形成新的数据帧 FQ_{AB}，其中 VID 为 VLAN1。之后，交换机 1 在端口 12 发送 FQ_{AB}。

(4) 交换机 2 在端口 1 接收 FQ_{AB}。通过分析 FQ_{AB}中的 802.1Q 标记字段，即可判定该帧属于 VLAN1。

(5) 根据本地接口/MAC 地址映射表和 VLAN 成员对照表，交换机 2 决定 FQ_{AB}的转发去向，具体过程与(2) 相似。由于主机 B 的 MAC 地址没有出现在交换机 2 的接口/MAC 地址映射表中，因此，交换机 2 向接口 1 之外的 VLAN1 成员端口(即端口 3 和端口 8)转发 FQ_{AB}。

(6) 由于接口 3 和端口 8 不是 802.1Q 共享端口，因此，交换机 2 在发送之前需要将 FQ_{AB}中的 802.1Q 标记删除，还原为数据帧 F_{AB}。

(7) 主机 B 和主机 C 接收 F_{AB}。由于 F_{AB}的目的地址与主机 C 的 MAC 地址匹配，因此，主机 C 继续处理 F_{AC}，而主机 D 将其抛弃。

3.4 实验：交换机的配置与VLAN组网

交换机可以看作一台专用的计算机。按照操作系统和软件的不同，交换机的配置命令和配置方式也不同。本实验将学习交换机配置命令的组织方式和使用方法，讨论有关的VLAN的配置命令，学习观察数据帧结构和数据帧传递过程的方法。大部分品牌的交换机(如华为交换机、思科交换机等)都可以通过控制终端以命令提示符的方式进行配置，同时多数仿真环境都提供简化的配置方法。


交换机的配置命令与技巧

3.4.1 交换机的配置命令

Cisco交换机的配置分成不同的配置模式，配置模式之间按照层次结构组织，不同配置模式中使用的命令不同。

在通过控制台进行配置时，开始处于用户模式。在用户模式下，交换机一般显示带大于号“>”的提示符(如switch>)。用户模式下只可以进行一些最基本的操作，不能对交换机进行配置。例如，可以利用show version命令查看交换机使用的操作系统版本；可以利用Ping命令测试与其他设备的连通性等。前面章节学习过的show mac-address-table命令也可以在这种模式下执行。

在用户模式下执行enable命令，交换机进入特权模式。在特权模式下，交换机一般显示带“#”的提示符(如switch#)。enable命令相当于一个登录命令，如果设置了口令，enable命令后需要跟随口令才能进入特权模式。特权模式除了包含用户模式下的一些命令外，还包含其他一些命令。例如，可以使用reload命令重启交换机；可以使用copy命令保存或调用交换机的配置等。如果希望退出特权模式，可以使用exit命令。

在特许模式下执行config terminal命令，交换机进入全局配置模式。在全局配置模式下，可以对交换机的全局信息进行配置。例如，可以使用hostname命令配置交换机使用的名称；使用enable命令设置enable登录时需要的口令等。如果希望退出全局配置模式，可以使用exit命令。

在全局配置模式下，可以使用不同的命令进入不同的子配置模式。例如，可以使用interface命令，进入接口配置模式；使用vlan命令，进入VLAN配置模式等。在子配置模式下，可以对相应的子部分进行配置。例如，在利用interface命令进入接口配置模式后，可以使用命令对相应的接口参数进行设置；在利用vlan命令进入VLAN配置模式后，可以使用命令对相应的VLAN参数进行配置。如果希望退出子配置模式，可以使用exit命令。

在子配置模式下，如果需要，还可以使用命令进入子配置模式的子配置模式。这样从用户模式开始，逐步进入更低级别的配置模式，形成了一个层次结构，如图3-13所示。

下面就Cisco交换机常用命令使用方法进行简单介绍。其他一些命令在实验遇到时再进行详细说明。

1. 使用问号“?”进行帮助

Cisco交换机的配置命令非常多，有时很难记住命令的具体形式和使用的参数。这时，可以通过输入问号“?”来使用帮助。

如果直接输入“?”，那么交换机返回该模式下可以使用的全部命令；如果输入了一部分命令后输入“?”，那么交换机返回该命令的完整形式；如果输入命令后想知道该命令可以使用的

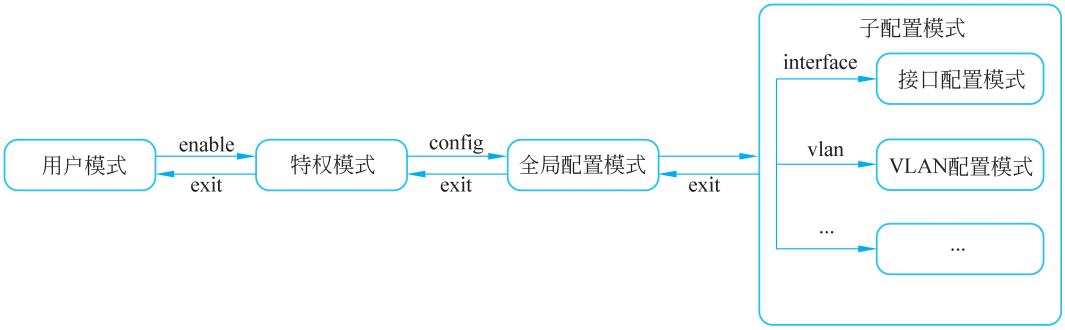


图 3-13 Cisco 交换机的配置模式

参数，那么可以在命令后输入空格，然后跟随一个“?”。

例如，在用户模式下，如果输入“?”，那么系统显示用户模式下可以使用的全部命令；如果输入“sh?”，那么系统将显示以 sh 开始的所有命令（如 show 等）；如果输入“show ?”，那么系统提示 show 命令可以使用的参数，例如显示 show 命令可以使用 version 参数、mac-address-table 参数、vlan 参数等。

2. 使用简化命令

为了方便记忆和理解命令的含义，Cisco 交换机提供的命令（或参数）有时使用较长的字符串表示。为了简化输入，Cisco 交换机允许用户只输入字符串的前面部分，只要前面部分能够与这一模式下的其他命令（或参数）区分即可。例如，在用户模式下输入 enable 命令时，只要输入 en 即可，因为 en 已经能够与用户模式下的其他命令完全区分，不会产生二义性。如果产生了二义性，系统会进行提示。这时只要再多输入几个字符即可。

3. 配置文件的保存和使用

利用命令将交换机的配置修改后，修改后的配置保存在内存中。如果关机或重启，修改后的配置就会丢失。为了使关机或重启后的交换机自动使用修改后的配置，需要将内存中的配置文件保存在交换机非易失的存储器中。要将内存中的配置存储到非易失存储器中，可以在特权模式下使用 copy running-config startup-config 命令。

另外，如果需要将修改后的配置恢复到开机时的状态，可以在特权模式下使用 copy startup-config running-config 命令。

4. 显示交换机的状态

Cisco 交换机使用 show 命令显示交换机的状态。例如，显示交换机内存中正在使用的配置文件，可以使用特权模式下的 show running-config 命令；显示非易失存储中保存的配置文件，可以使用特权模式下的 show startup-config；显示交换机当前的接口/MAC 地址映射表，可以使用特权模式或用户模式下的 show mac-address-table 命令。

5. 删除交换机的配置

Cisco 交换机使用 no 命令删除交换机的配置条目。例如，要删除编号为 10 的 VLAN，可以使用 no vlan 10。

3.4.2 VLAN 的配置

VLAN 的配置实验可以在虚拟仿真环境下进行。实验内容包括设备的连接、设备的配置和连通性测试。


VLAN 的配置

1. 网络的拓扑结构

运行 Packet Tracer 仿真软件,在设备类型和设备选择区选择交换机和主机。将选择的交换机和主机用鼠标拖入 Packet Tracer 的工作区,形成如图 3-14 所示的仿真网络拓扑。在进行主机与交换机、交换机与交换机的连接时,要注意使用的电缆类型。

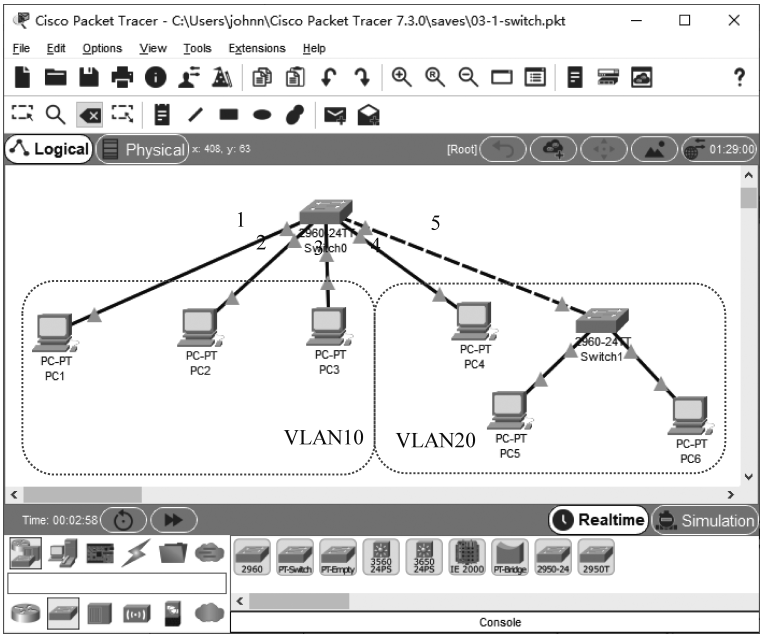


图 3-14　仿真实验中的网络拓扑结构

2. 主机 IP 地址的配置

配置图 3-14 中 PC1～PC6 的 IP 地址。主机的 IP 地址可以在 192.168.0.1～192.168.0.254 任选一个,但每台主机必须选择不同的 IP 地址。子网掩码填写 255.255.255.0 即可。由于还未划分 VLAN,因此,IP 地址配置完成后,所有主机之间都应该能够相互 Ping 通。

3. 添加终端控制台

按照第 2 章介绍的实验内容,交换机的配置需要添加一台主机作为终端控制台。在图 3-14 的工作区中增加一台主机,并使用串口线将该主机的 RS-232 串行口与交换机的 Console(控制)接口连接,如图 3-15 所示。然后,单击作为控制终端的主机 PC0,在弹出的配置界面中选择 Desktop→Terminal 启动终端控制程序。在终端控制台程序中输入常用的 enable、show running-config、show mac-address-table 等命令,观察交换机的回送信息。

4. 查看 VLAN 配置

查看交换机的 VLAN 配置可以在特权模式下使用 show vlan 命令,如图 3-16 所示。交换机返回的信息显示了当前交换机配置的 VLAN 数量、VLAN 编号、VLAN 名字、VLAN 状态以及每个 VLAN 包含的接口。

5. 添加 VLAN

按照图 3-14 的要求,需要为实验划分两个 VLAN,一个编号为 10,另一个编号为 20。每个 VLAN 都可以配置一个容易记住的名字。例如,编号为 10 的 VLAN 名字为 myVLAN10;编号为 20 的 VLAN 名字为 myVLAN20 等。

如果要添加一个编号为 10、名字为 myVLAN10 的 VLAN,那么可以按照如下步骤进行,

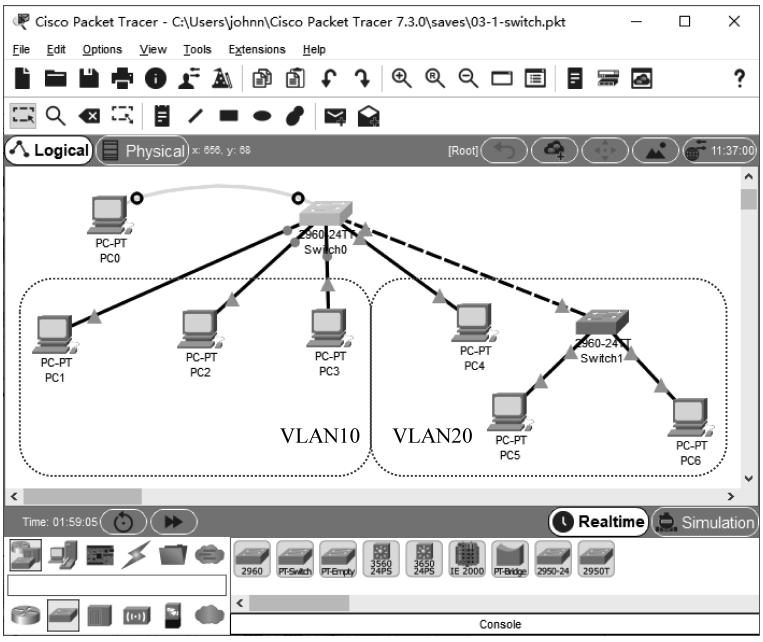


图 3-15　利用控制台对交换机进行配置

如图 3-17 所示。

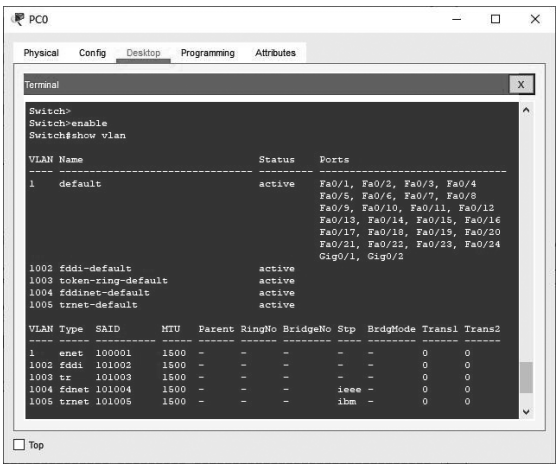


图 3-16　查看 VLAN 的配置

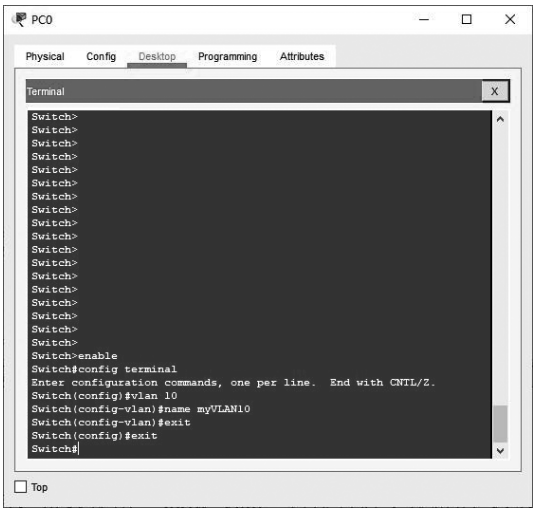


图 3-17　添加 VLAN

（1）在用户模式下利用 enable 进入特权模式。之后，再利用 config terminal 命令进入交换机的终端配置模式。

（2）利用 vlan vlanID 命令创建一个编号为 vlanID 的虚拟局域网，并进入该 VLAN 的配置模式。在图 3-17 中，vlan 10 命令创建了一个编号为 10 的虚拟局域网。在创建完成之后，系统自动进入编号为 10 的 VLAN 配置模式。

（3）如果希望为创建的 VLAN 设置一个好记的名字，可以在该 VLAN 的配置模式下使用 name vlanName 命令。在图 3-17 中，name myVLAN10 将编号为 10 的 VLAN 命名为 myVLAN10。

(4) 执行 exit 命令退出 VLAN 配置模式,再执行 exit 命令退出全局配置模式。

添加 VLAN 之后,可以在特权模式下使用 show vlan 命令再次查看交换机的 VLAN 配置,以确认新的 VLAN 已经添加成功。

请按照同样的方式,添加编号为 20 的 VLAN。

6. 为 VLAN 分配端口

以太网交换机通过把某些端口分配给一个特定的 VLAN 以建立静态虚拟局域网。将某一端口(如 Fa0/1 端口)分配给某一个 VLAN 的过程如图 3-18 所示。

(1) 在特权模式下执行 configure terminal 命令进入交换机的终端配置模式。

(2) 利用 interface ifID 进入指定的 ifID 端口的配置模式。例如,利用 interface Fa0/1 命令进入 Fa0/1 端口的配置模式。

(3) 交换的接口既可以配置成接入(access)端口,也可以配置成共享(trunk)端口。接入端口用于连接主机等终端设备;共享端口用于交换机等设备的级联,在转发数据时会添加 802.1Q 标记信息。由于本实验无须在两台交换机之间传输 VLAN 信息,因此,所有端口需要设置为接入端口。在端口配置模式下,使用 switchport mode access 命令把配置的端口设置为接入模式,然后再使用 switchport access vlan vlanID 命令把端口分配给编号为 vlanID 的虚拟局域网。在图 3-18 中,switchport mode access 命令和 switchport access vlan 10 命令将配置的端口(Fa0/1 端口)设置为接入模式,并将其分配给编号为 10 的虚拟局域网。

(4) 执行 exit 命令退出端口配置模式,再执行 exit 命令退出终端配置模式。

按照图 3-14 的要求,将交换机 Switch0 的 Fa0/1～Fa0/3 分配给编号为 10 的 VLAN,将 Fa0/4～Fa0/5 分配给编号为 20 的 VLAN。之后,利用 show vlan 命令显示交换机的 VLAN 配置信息,确认 Fa0/1～Fa0/3 位于 VLAN10 中,Fa0/4～Fa0/5 位于 VLAN20 中,如图 3-19 所示。

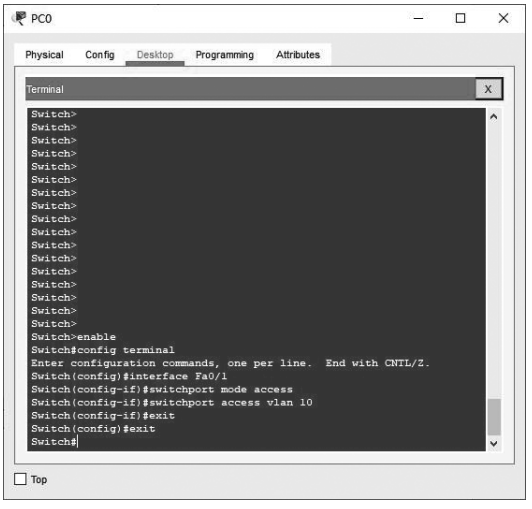


图 3-18 为 VLAN 分配接口

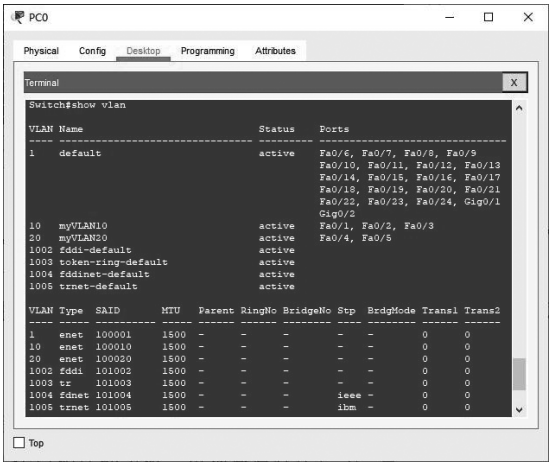


图 3-19 用 show vlan 命令确认 VLAN 包含的接口号

使用主机 PC1 分别去 Ping 主机 PC2～PC6,观察会有什么现象发生,并对其进行解释。同时思考用于连接 Switch1 的 Fa0/5 端口为何无须设置为共享端口。

7. 删除 VLAN

当一个 VLAN 的存在没有任何意义时,可以将它删除。删除 VLAN 的步骤如图 3-20 所示。

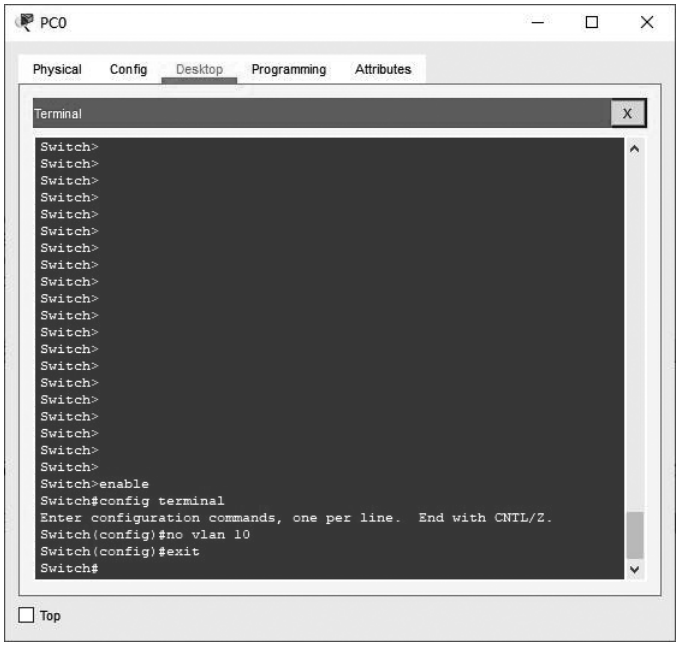


图 3-20 删除 VLAN

(1) 在特权模式下利用 config terminal 命令进入交换机的终端配置模式。

(2) 执行 no vlan vlanID 命令将编号为 vlanID 的 VLAN 删除。例如,命令 no vlan 10 将删除编号为 10 的 VLAN 虚拟局域网。

(3) 执行 exit 命令退出终端配置模式。

注意,在删除一个 VLAN 后,原来分配给这个 VLAN 的端口将处于非激活状态。交换机不会将这些端口自动归入另一个现存的 VLAN。当再次分配给一个 VLAN 时,这些端口就会被重新激活。

3.4.3 仿真环境中的简化配置方法


仿真环境下的简易配置方法

在真实环境下,通过终端控制台对交换机进行配置是最基本的配置方法。包括交换机在内的多数网络设备都可以通过这种方式进行配置。如果 Packet Tracer 工作区中每个网络设备都连接一个终端控制台,那么工作区界面就会显得非常凌乱,特别是网络拓扑中含有多个网络设备的情况下。

为了解决这个问题,Packet Tracer 提供了两种简化的配置方法。一种配置方法利用设备配置界面的命令行界面(Command Line Interface,CLI)对交换机进行配置,另一种配置方法利用设备配置界面的 Config 对交换机进行配置。这两种配置方法都可以在不添加终端控制台的情况下对交换机进行配置,使 Packet Tracer 的工作界面更加简洁。但是需要注意,这两种简化的配置方式在真实环境中并不存在。如果在真实环境中配置网络设备,终端控制台必不可少。

(1) 利用设备配置界面的 CLI 对交换机进行配置。在 Packet Tracer 工作区中单击需要配置的交换机等网络设备,在弹出的配置界面中选择 CLI 标签,然后就可以像在终端控制台一样配置该设备,如图 3-21 所示。与连接终端控制台方式相同,在 CLI 中可以运行 show

mac-address-table、config terminal、show vlan 等命令。注意,这种配置方式只是在仿真环境下省略了连接终端控制台的过程,但在真实环境中,连接控制终端是必不可少的。

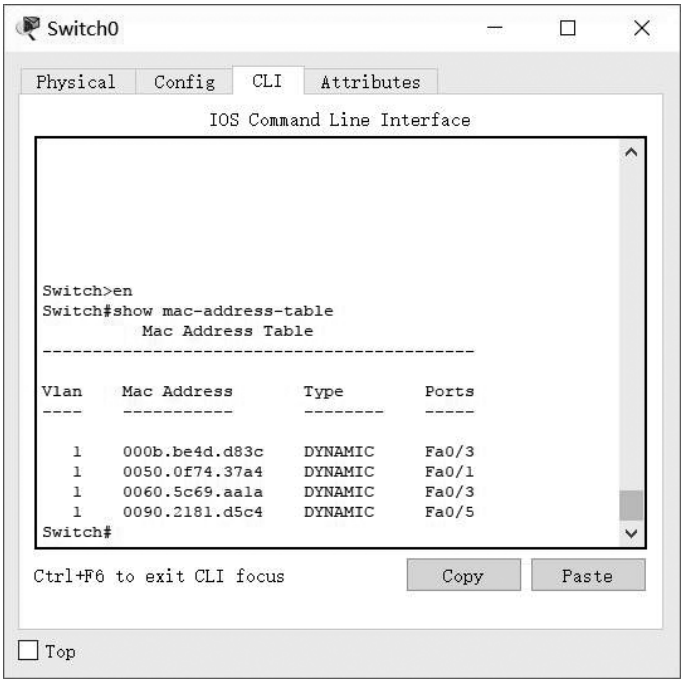


图 3-21　交换机的 CLI 界面

(2) 利用设备配置界面的 Config 对交换机进行配置。这是一种类似图形化的配置界面。单击需要配置的网络设备,在弹出的配置界面中选择 Config 标签即可进入配置界面,如图 3-22 所示。例如,单击图 3-22 中的 VLAN Database 选项,界面的右侧就会出现 VLAN 配置界面。

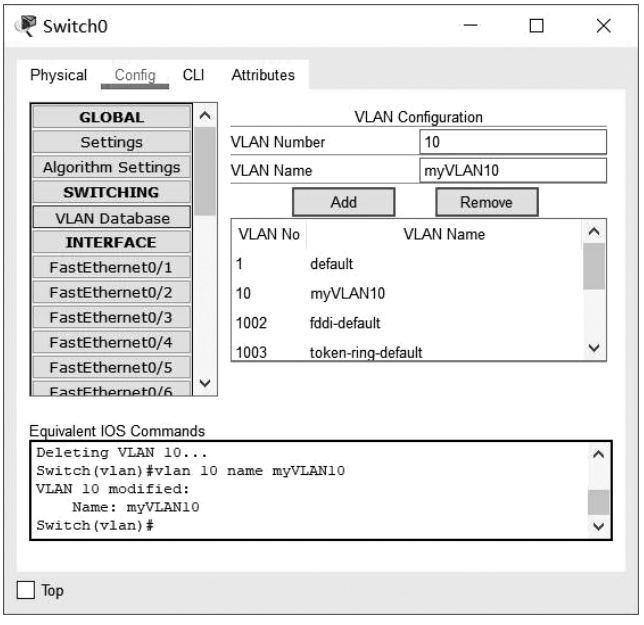


图 3-22　交换机的 Config 界面

只要输入 VLAN 号和 VLAN 名，就可以通过单击 Add 或 Remove 按钮增加 VLAN 或删除 VLAN。同时，在单击 Add 或 Remove 按钮后，界面的下方还会给出这次操作执行的相应命令和响应。虽然这种配置方式简单、直观，但是这种配置方式只能配置界面列出的一些项目，适用于对交换机配置命令不熟悉的新手。注意，这种配置方式只是在仿真环境下将一些配置命令进行了图形化，真实环境中还是要连接终端控制台进行网络设备配置。

3.4.4 在模拟模式下观察数据包的收发过程

Packet Tracer 提供了两种仿真模式，一种是实时(Realtime)模式，一种是模拟(Simulation)模式。

实时模式是一种默认模式，Packet Tracer 启动后默认在实时模式下运行。实时模式下的操作方式与真实环境非常相似，Ping 命令会在很短时间内完成并显示。但是实时模式中不能观察数据分组一步一步地传递过程。为了更形象、具体地展示数据分组的传递过程和设备的处理过程，可以使用 Packet Tracer 提供的模拟模式。

实时模式和模拟模式的转换按钮在 Packet Tracer 界面的右下角。在选中模拟模式后，系统的界面如图 3-23 所示。

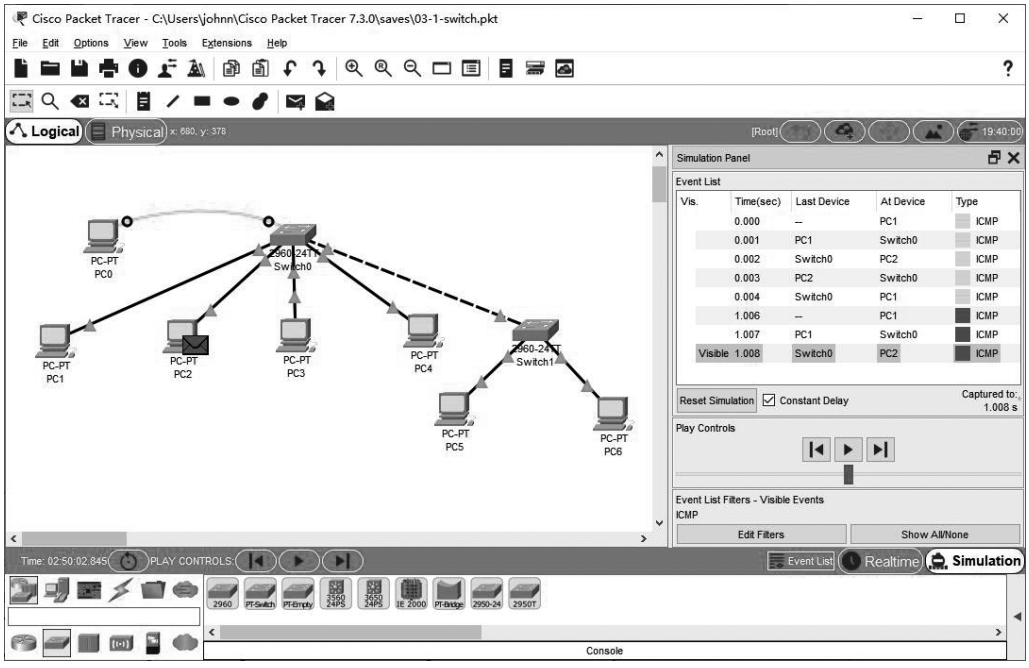


图 3-23 Packet Tracer 的模拟模式界面

图 3-23 的右部包括了 Play Controls(播放控制)、Event List Filters(事件过滤器)、Event List(事件列表)等内容。在运行中，左部的网络拓扑图上会以动画形式展示数据分组的传递过程。

- Play Controls(播放控制)：播放控制中拥有▶|(前进)、|◀(后退)、▶(自动)等按钮，控制单步或自动运行。
- Event List Filters(事件过滤器)：网络中传输的数据分组分为很多种，如后续章节将会介绍的 IP、ICMP、ARP 等。在模拟方式下，可以过滤出关心分组类型。只有这些关心

的分组类型,才会在网络拓扑图中以动画的形式显示,并且在事件列表中列出来。如果希望设置关心的分组类型,可以单击 Edit Filters 按钮在弹出的对话框中进行选择,如图 3-24 所示。由于 Ping 命令发送的分组类型为 ICMP,因此,本实验需要将 ICMP 类型选为关心的分组类型。

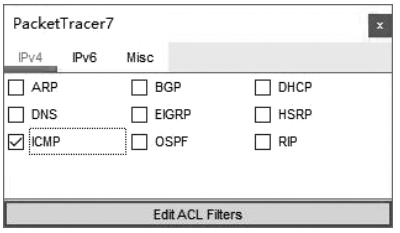


图 3-24　选择关心的分组类型

- Event List(事件列表):事件列表展示关心分组的发送设备、接收设备和分组类型。单击事件列表中的数据分组,还可以看到该分组封装的具体内容和设备对它的处理过程,如图 3-25 所示。

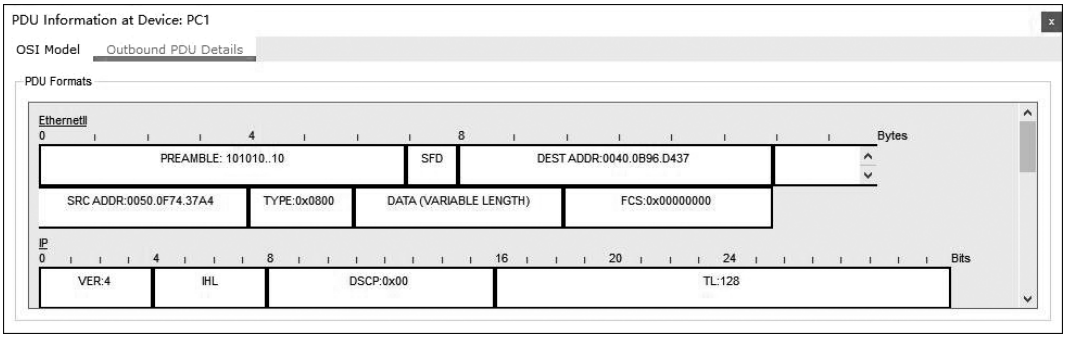


图 3-25　模拟模式下显示的数据帧的封装内容

学习以上内容后,请在模拟模式下通过 Ping 命令测试网络的连通性,利用▶|、|◀和▶按钮控制数据分组的发送进度,观察数据分组的发送过程,查看数据分组中的封装内容。

练习与思考

一、填空题

(1) VLAN 的划分方法通常分为两种,它们是_____和_____。

(2) 802.1Q 协议的主要功能是_____。

(3) 如果交换机的一个端口用于连接主机,那么通常将其配置成_____端口类型。

(4) 在 Cisco 交换机的特权模式下,进入全局配置模式使用的命令为_____。

二、单项选择题

(1) 在 IEEE 802.1Q 中,VID 由 12 位组成。其有效的 VLAN 号范围为(　　)。

a) 0～4095　　b) 1～4095　　c) 1～4094　　d) 0～4094

(2) 802.1Q 协议规定的 VID 位数为(　　)。

a) 8 位　　b) 12 位　　c) 16 位　　d) 32 位

(3) 在 Cisco 交换机中,如果希望删除编号为 100 的 VLAN,那么可以使用的命令是(　　)。

a) del vlan 100　　b) del 100 vlan　　c) no vlan 100　　d) no 100 vlan

(4) 以下关于 VLAN 的描述中,错误的是(　　)。

a) 一个 VLAN 是一个广播域　　b) VLAN 提高了以太网的工作效率

c) VLAN 使管理以太网更加方便　　d) 静态 VLAN 已经过时