



## (12) 发明专利申请

(10) 申请公布号 CN 102130919 A

(43) 申请公布日 2011.07.20

(21) 申请号 201110096111.3

代理人 蔡悦

(22) 申请日 2002.02.01

(51) Int. Cl.

(30) 优先权数据

H04L 29/06(2006.01)

60/343,307 2001.12.20 US

H04L 12/46(2006.01)

10/057,566 2002.01.25 US

(62) 分案原申请数据

02825771.5 2002.02.01

(71) 申请人 微软公司

地址 美国华盛顿州

(72) 发明人 丹尼斯·迈克尔·沃尔帕诺

(74) 专利代理机构 上海专利商标事务所有限公司 31100

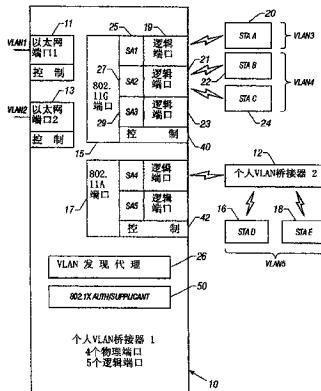
权利要求书 2 页 说明书 7 页 附图 7 页

(54) 发明名称

个人虚拟桥接局域网

(57) 摘要

一种用于分离在与桥接器相关的 STA 中的业务的机制, 这里称作个人虚拟桥接局域网 (个人 VLAN), 是基于通过利用一个 VLAN 分离业务的。 IEEE802.1Q — 1998 (虚拟桥接 LAN) 协议提供一个通过本发明扩展的机制以在理论上把一个局域网段划分为多个 VLAN。 在优选实施例中, VLAN 桥接器仅仅转发单播和群播帧到服务于帧所属的 VLAN 的端口。 本发明的一个实例扩展该标准 VLAN 桥接模型以提供一个适合于在 AP 内使用的机制。 在一个优选实施例中, 个人的 VLAN 桥接器在至少任何下列方法中扩展了标准 VLAN 桥接器 :VLAN 发现, 其中一个个人 VLAN 桥接器提供一个用于 VLAN 发现的协议 ;VLAN 扩展, 其中一个个人 VLAN 允许一个站建立一个服务于新 VLAN 的新端口, 或经由认证协议加入一个现存的 VLAN ;逻辑端口, 其中一个个人 VLAN 桥接器保持每一物理端口多于一个逻辑端口, 并且该桥接器桥接在任何种类的端口之间 ; 和加密的 VLAN 分离。



1. 一种用于在一个用于分离在多个与接入点有关的站中的业务的系统中加入由所述接入点服务的个人虚拟局域网的方法,所述方法包括:

由所述个人虚拟局域网的创建者提供一个用于请求者的认证的控制信道;

使用所述控制信道来中继所述创建者和所述请求者之间的认证协议消息;

如果所述创建者能够认证所述请求者,则所述创建者与所述请求者共享安全关联;

使用在所述个人虚拟局域网的成员之间共享的所述安全关联来标识来自所述成员的帧;

其中:如果一个接收帧载有一个空虚拟局域网 ID 或是未加标签的,则使用它的源 MAC 地址去确定一个所述接收帧的初级虚拟局域网分类;以及

如果所述接收帧载有一个虚拟局域网 ID,则取而代之地使用所述虚拟局域网 ID 作为所述初级虚拟局域网分类代替;

使用所述初级虚拟局域网分类去索引进入给出认证码密钥的安全关联表;

所述接收帧载包括认证码,所述认证码通过在帧负载上使用在认证时间由所述个人 VLAN 桥接器和所述请求者双方商定的消息摘要算法来计算,所述消息摘要算法被记载在所述安全关联表中;

所述接收帧的接收器使用所述认证码密钥在所述接收帧的所述负载上重新计算认证码;

比较所述重新计算的认证码和所述接收的认证码;其中如果所述重新计算的认证码和所述接收的认证码匹配,则所述初级的虚拟局域网分类成为最终的虚拟局域网分类;

使用所述最终的分类作为任何通信数据请求基元的虚拟局域网分类参数的值;

使用所述安全关联对所述接收帧进行解密;以及

提交所述解密帧到一个前向转发和学习过程;否则,丢弃所述接收帧。

2. 如权利要求 1 所述的方法,其特征在于,通过具有与所述接入点相关联的多个逻辑端口,所述接入点能够服务多于一个 VLAN。

3. 如权利要求 2 所述的方法,其特征在于,还包括步骤:提供在所述逻辑端口的入口过滤。

4. 如权利要求 2 所述的方法,其特征在于,所述安全关联包含至少两个密钥,一个密钥用于加密,而另一个密钥用于计算认证码,其中所述安全关联与 VLAN 相关,其中所述认证码用来限制在连接全部 VLAN 的成员的逻辑端口上的业务,其中加密用来保持除成员之外的专用业务,其中只有具有所述安全关联的站属于所述 VLAN,并且其中所有具有所述安全关联的站属于相同的广播范围。

5. 一种用于分离在与网络接入点相关联的多个终端站之间的业务的方法,所述方法包括:

所述多个终端站中的一个终端站执行一初始认证操作;

在所述终端站接收帧;如果所述接收帧载有一个空虚拟局域网 ID 或是未加标签的,则使用它的源 MAC 地址去确定一个所述接收帧的初级虚拟局域网分类;以及

如果所述接收帧载有一个虚拟局域网 ID,则取而代之地使用所述虚拟局域网 ID 作为所述初级虚拟局域网分类代替;

使用所述初级虚拟局域网分类去索引进入给出认证码密钥的安全关联表;

所述接收帧载包括加密的认证码,所述加密的认证码通过在帧负载上使用在所述初始认证操作期间确定的加密的消息摘要算法来计算,所述加密的消息摘要算法被记载在所述安全关联表中;

所述终端站使用所述认证码密钥在所述接收帧的所述负载上重新计算所述加密的认证码;

比较所述重新计算的加密的认证码和所述接收的加密的认证码;

其中如果所述重新计算的加密的认证码和所述接收的加密的认证码匹配,则:

使用所述初级虚拟局域网分类作为任何通信数据请求基元的虚拟局域网分类参数的值;

使用所述安全关联对所述接收帧进行解密;以及

提交所述解密帧到一个前向转发和学习过程;

其中如果所述重新计算的加密的认证码和所述接收的加密的认证码不匹配,则丢弃所述接收帧。

6. 如权利要求 5 所述的方法,其特征在于,所述认证码是唯一地标识业务所属的 VLAN 的加密的认证码。

7. 如权利要求 5 所述的方法,其特征在于,所述认证码是在所述初始认证期间生成的。

8. 如权利要求 5 所述的方法,其特征在于,所述初始认证操作是由所述终端站和所述接入点执行的的。

9. 如权利要求 8 所述的方法,其特征在于,所述加密的消息摘要算法是由所述接入点和所述终端站双方商定的。

## 个人虚拟桥接局域网

[0001] 本发明专利申请是国际申请号为 PCT/US2002/002905, 国际申请日为 2002 年 2 月 1 日, 进入中国国家阶段的申请号为 02825771.5, 名称为“个人虚拟桥接局域网”的发明专利申请的分案申请。

### 技术领域

[0002] 本发明涉及局域网。更特别地, 本发明涉及一种个人虚拟桥接局域网。

### 背景技术

[0003] 接入点 (AP) 是在一个或多个站 (STA) 和分布系统 (DS) 之间的链路层桥接器。参见 IEEE 802.11, 无线局域网媒体存取控制和物理层规范, ISO/IEC8802-11 :1999 (E), ANSI/IEEE Std 802.11、1999 版本。一种 DS 的实例是一个局域网段, 或一个企业内部互联网。AP 启动将经由无线发送的分组, 或者从发射站发送 (STA) 到 DS 的分组、或者从 DS 发送到 STA 的分组。因此, 接入点至少具有两个物理端口。一个是 DS 接口, 而另一个是一个无线电接口。每个具有他们自己无线接口的多个 STA 可以通过多路复用 AP 单独共享无线接口而发送分组到 DS。该无线电接口在一个特殊的频率下操作, 并且多个 STA 通过保证互相专用访问媒质的 MAC PHY 协议共享该媒质。DS 同样通过利用相同的协议发送分组。

[0004] AP 的 STA 具有一个基本服务组 ID(BSSID)。理论上它用来划分 802.11 基本服务组。每一个和 AP 相关的 STA 共享 AP 的 BSSID。去往由 AP 或 STA 接收的组地址的帧将丢弃, 假如 AP or STA 所属的 BSS 不匹配该帧的 BSSID。在这种意义上讲, 该 BSSID 起一个虚拟 LAN ID(VID) 的作用。参看 IEEE 802.1Q, 用于本地和城域网 IEEE 标准: 虚拟桥接局域网, IEEE Std 802.1Q-1998。由于和相同的 AP 相关, 因此每个站是相同的虚拟局域网 (VLAN) 的成员。

[0005] 然而, 在 BSS 中的每个 STA 将不会共享相同的 VLAN, 除非这些 STA 彼此信任。然而, 在公共区域配置中, 当他们之间典型地不存在信任时, 所有与 AP 有关的 STA 被请求共享相同的 VLAN。这就导致了 STA 的易受攻击, 例如一个不信任的 STA 发射地对各种链路层的攻击, 例如地址解析协议 (ARP) 高速缓冲存储器再映射。

[0006] 提供用于在与桥接器相关的多个 STA 中分离业务的机制是有益的, 因此例如一个与所述桥接器相关的不被信任的 STA 不能对与相同的桥接器相关的另一个 STA 发起链路层 (OSI 层 2) 攻击。

### 发明内容

[0007] 本发明提供用于在与桥接器相关的多个 STA 中分离业务的机制, 因此例如一个与所述桥接器相关的不被信任的 STA 不能对与相同的桥接器相关的另一个 STA 发射链路层 (OSI 层 2) 攻击。本发明是基于通过利用 VLAN 分离业务的。IEEE 802.1Q-1998 (虚拟桥接 LAN) 协议提供一个通过本发明扩展的机制以在理论上把一个的局域网段划分为多个 VLAN。在优选实施例中, VLAN 桥接器仅仅转发单播和群播帧 (unicast and group frames)

到服务于帧所属的 VLAN 端口。本发明的一个实例扩展该标准 VLAN 桥接模型以提供一个适合于在 AP 内使用的机制。

[0008] 假定 AP 附属于 DS。和 AP 相关的每个站将有机会建立一个具有它本身的新的 VLAN，并且该 DS 也作为它的成员。这样在信任和不信任的 STA 之间的业务被分离，即使他们和相同的 AP 相关。通常，假如 DS 包括多个 VLAN，则 VLAN 任何子集的成员可以是该新 VLAN 的成员。所以将有一个方法去发现现存的 VLAN。此外，将有一个加入现存 VLAN 的协议。建立一个 VLAN 和加入现存的 VLAN 都需要认证操作。IEEE 标准 802.1Q-1998VLAN 模型用于这种目的是有欠缺的，因为它不能提供这种能力。本发明的优选实施例包括一个提供这种能力的机制，在这里称为个人虚拟桥接局域网（个人 VLAN）。

[0009] 在优选实施例中，个人的 VLAN 桥接在至少任何下列方法中扩展了标准 VLAN 桥接器：

[0010] • VLAN 发现：一个个人 VLAN 提供一个用于 VLAN 发现的协议（在下文中讨论）。

[0011] • VLAN 扩展 / 建立：一个个人的 VLAN 桥接器允许一个站建立一个服务于新 VLAN 的新端口，或加入现存的 VLAN 或经由认证协议加入现存的 VLAN。

[0012] • 逻辑端口：一个个人的 VLAN 桥接可以保持每个物理端口超过一个逻辑端口。它桥接在任何种类的端口之间。一个 VLAN 的成员组按照逻辑与物理端口定义。每个逻辑端口具有通过桥接控制的生存期。

[0013] • 密码的 VLAN 分离：在一个个人的 VLAN 中，一个逻辑端口至多服务一个 VLAN。然而，因为每一物理端口可能有超过一个逻辑端口，多于一个 VLAN 就可能存在于一个物理端口上。在一个 VLAN 内的业务与在相同的物理端口上的另一个 VLAN 通过密码术分离。认证码唯一地识别业务所属的 VLAN，同时加密的另一个等级用来保持除 VLAN 的成员之外的专用业务。

[0014] • 通过路由器支持的第 2 层 VLAN：当 STA 可以漫游和再安装到在不同桥接器上的网络时，例如通过和新的 AP 相关，STA 可以通知它已经所属的 VLAN 的桥接器。该 VLAN 可能已经通过站，例如其本身，在另一个桥接器上被建立，该另一个桥接器在该桥接器上将 VLAN 连接到一个或多个逻辑或物理端口。即使新的桥接可能是位于不同的子网，STA 可以在第 2 层的 VLAN 保持它的会员资格。这些能力包含移动 IP 能力，因为移动 IP 目标是通过路由器对于站保留子网会员资格。一个子网可能相当于一个 VLAN，但通常它不是。

[0015] • 生成树维护：个人的 VLAN 桥接器允许站建立一个 VLAN，这里 STA 本身就是一个桥接器。当授予会员资格时，生成树算法消除桥接器间的循环。加入个人 VLAN 的过程执行对 VLAN 拓扑的限制，使得在新的桥接器加入 VLAN 之后重新构造一个不必要的生成树。

## 附图说明

[0016] 图 1 是一个按照本发明的框图，描述了在个人 VLAN 中的两个桥接器；

[0017] 图 2 是一个框图，示出了一个实例，其中站 A 和桥接器 1 共享 SA1；

[0018] 图 3 是一个显示实例的框图，其中站 D 和 E 均属于 VLAN5，然而不同于其它站，他们不与桥接器 1 共享安全关联，而是与个人 VLAN 桥接器 2 共享安全关联；

[0019] 图 4 是一个按照本发明示出个人 VLAN 发现的框图；

[0020] 图 5 是一个按照本发明示出请求服务用于新 VLAN 的流程图；

[0021] 图 6 是一个按照本发明的流程图,示出在桥接器上通过逻辑端口服务的 VLAN 到在桥接器上通过物理端口服务的一个或多个 VLAN 的连接。

[0022] 图 7 一个是按照本发明的流程图,示出当桥接器接收由逻辑端口服务的单个 VLAN 组成的目的地 VLAN 组的 VLAN 请求时被触发的站内认证;和

[0023] 图 8 是一个按照本发明流程图,示出入口过滤逻辑端口。

## 具体实施方式

[0024] 本发明目前的优选实施例提供用于在与桥接器相关的多个 STA 之间分离业务的机制,因此例如一个与所述桥接器相关的不信任 STA 不能用于在与相同桥接器有关的另一个 STA 上发射链路层 (OSI 层 2) 攻击。本领域有经验的技术人员将理解,于此披露的本发明可应用到各类的系统和网络,包括但不限于有线和无线网络。

### 个人 VLAN 桥接器模型

[0026] 本发明是基于通过利用 VLAN 分离业务的。IEEE 802.1Q-1998(虚拟桥接 LAN) 协议提供一个通过本发明扩展的机制以在理论上把一个的局域网段划分为多个 VLAN。在优选实施例中,VLAN 桥接器仅仅转发单播和群播帧 (unicast and group frames) 到那些服务于帧所属的 VLAN 的端口。本发明的一个实例扩展该标准 VLAN 桥接器模型以提供一个适合于在 AP 内使用的机制。

[0027] 假定 AP 附属于 DS。和 AP 相关的每个站将有机会建立一个具有其本身的新 VLAN,并且该 DS 作为它的成员。可见在信任和不信任的 STA 之间的业务能够被分离,即使他们和相同的 AP 相关。通常,假如 DS 包括多个 VLAN,则他们任何子集的成员可以是该新 VLAN 的成员。所以将有一个方法去发现现存的 VLAN。此外,将有一个用于加入现存 VLAN 的协议。建立一个 VLAN 和加入一个现存的 VLAN 都要求认证操作。IEEE 标准 802.1Q-1998VLAN 模型用于这样的目的是有欠缺的,因为它不能提供这种能力。本发明的优选实施例包括一个提供这种能力的机制,在这里称为个人虚拟桥接局域网 (个人的 VLAN)。

[0028] 本发明当前优选实施例于此结合图 1-3 进行讨论。本领域熟练的技术人员理解,图 1-3 示出的结构仅仅提供实例的目的,而不是打算限制本发明可能实践的结构。

[0029] 图 1 是描述两个桥接器 10、12 的框图。个人 VLAN 桥接器 1(10) 具有四个物理端口 11、13、15、17,其中两个 11、13 是有线以太网。有线端口分别服务于 VLAN1 和 VLAN2。其它两个端口 15、17 是无线以太网端口。这些端口中的 15 符合高速 (54Mbps) 802.11g 标准,而另外的端口 17 符合 802.11a 标准。有三个逻辑端口 19、21、23 与 802.11g 端口相关。每一个逻辑端口具有其自己的安全联合 25、27、29,以构成一个单独的 VLAN,上述的安全联合 25、27、29 通过一些数量的终端站 20、2224 共享。

[0030] 如图 2 所述,站 A20 与桥接器 110 共享 SA125。没有其它站共享 SA1,因此 STA A 在一个唯一的 VLAN 中,也就是 VLAN3 中,并通过根是桥接器 1 的生成树代表。

[0031] 另一方面,站 B 和 C22、24 属于 VLAN4,因为他们与桥接器 1 共享 SA227(见图 2)。这个 VLAN 通过 STA A 或 STA B 中的一个建立。然后其它站在通过创建者验证之后加入。这描述了加入个人 VLAN 的情况(参见下文)。VLAN4 也由具有作为根的桥接器 1 的生成树表示的。

[0032] 站 D 16 和 E 18 属于 VLAN5。然而,与其它站不同,他们不与桥接器 1 共享安全联

合,而是与个人 VLAN 桥接器 212 共享(参见图 3)。桥接器 2 是用于 VLAN5 的生成树的根直至该树被扩展,使得桥接器 1 作为新的根。

- [0033] 在一个实例中,个人 VLAN 桥接器在至少任何下列方法中扩展标准 VLAN 桥接器:
- [0034] • VLAN 发现:一个个人的 VLAN 提供一个用于 VLAN 发现的协议(在下文中讨论)。
  - [0035] • VLAN 扩展 / 建立:一个个人的 VLAN 桥接器允许一个站建立一个服务于新 VLAN 的新端口,或加入现存的 VLAN 或经由认证协议加入现存的 VLAN。

[0036] • 逻辑端口:一个个人 VLAN 桥接器可以保持每个物理端口多于一个逻辑端口。它桥接在任何种类的两个端口之间。一个 VLAN 的成员组按照逻辑和物理端口定义。每个逻辑端口具有通过桥接器控制的使用期。

[0037] • 密码的 VLAN 分离:在个人的 VLAN 中,逻辑端口至多服务于一个 VLAN。然而,因为每一物理端口可能有超过一个逻辑端口,多于一个 VLAN 存在一个物理端口上。在一个 VLAN 内的业务与相同的物理端口上的另一个 VLAN 中的业务通过密码术分离。认证码唯一地识别业务所属的 VLAN,加密的另一个等级用来保持除 VLAN 的成员之外的专用业务。

[0038] • 通过路由器支持的第 2 层 VLAN:当 STA 可以漫游和再安装到在不同桥接器上的网络时,例如通过和新的 AP 相关,STA 可以通知它已经所属的 VLAN 的桥接器。该 VLAN 可以已经通过站,例如其本身,在另一个桥接器上被建立,该另一个桥接器在该桥接器上将 VLAN 连接到一个或多个逻辑或物理端口。即使新的桥接器可能是位于不同的子网,STA 可以在第 2 层的 VLAN 保持它的会员资格。这些能力包含移动 IP 能力,因为移动 IP 目标是通过路由器对于站保留子网会员资格。一个子网可能相当于一个 VLAN,但通常它不是。

[0039] • 生成树维护:个人的 VLAN 桥接器允许站建立一个 VLAN,这里该站本身就是一个桥接器。当授予会员资格时,生成树算法消除桥接器间的循环。加入个人 VLAN 的过程执行对 VLAN 拓扑的限制,使得在新的桥接器加入 VLAN 之后再构造一个不必要的生成树。

[0040] 如在 IEEE Std 802.1Q-1998 所述,当前优选的个人 VLAN 桥接器模型按照它的标记帧规则和按照涉及中继 MAC 帧的元件并联 VLAN 模型,确定成员 / 未标记组,IEEE 用于局域网和城域网的标准:虚拟桥接局域网,第 28 页。在个人 VLAN 桥接器中的元件扩展部分描述如下。

#### [0041] 个人 VLAN 控制信道

[0042] 每个物理端口具有一个个人 VLAN 控制信道 40、42,用于发送和接收控制帧和认证协议帧。该信道没有安全关联,并且通过帧场识别,例如以太网类型编码。认证帧更适宜使用一个诸如 EAPoL(查看 IEEE 802.1X,用于局域网和城域网的 IEEE 标准:基于网络接入控制的端口,IEEE Std 802.1x-2001) 的格式压缩,EAPoL 可以处理各种认证协议。

#### [0043] VLAN 发现

[0044] 一个个人 VLAN 桥接器分别运行服务器和客户端 VLAN 发现代理 26、28 和 30。当客户端代理发出信息请求时,服务器代理响应信息请求。这种代理的实例是服务定位协议 v2IETF RFC 2608 的客户机和服务器代理。因此,个人 VLAN 可以发现其它 VLAN,和 / 或允许该个人 VLAN 服务的多个 VLAN 被发现。发现(参见图 4)包括 VLAN-DISCOVER 帧的传输。在响应方面,VLAN-OFFER 帧被发送给该发现帧的源 MAC 地址。提供帧(offer frame)列出全部或一些桥接器服务的 VLAN 和从他们中选出来被使用的信息。响应它发送的发现帧,可能有多于一个由客户端接收的提供帧。VLAN-OFFER 帧的传输通过随机选择某些时段而被延

迟以最小化应答者间的冲突。

[0045] 服务新的 VLAN

[0046] 一个个人 VLAN 桥接器可以接收一个请求以服务新的 VLAN。该请求包含新的 VLAN 的 VID。请求是不准许的,除非请求者被授权,该请求是最新的,并且它可以通过控制信道认证。为了在桥接器服务一个新的 VLAN,请求标记桥接器用于提名 VLAN 的生成树的根。用于新 VLAN 的请求服务包括下列步骤:

[0047] • 桥接器通过某些物理端口的控制信道接收具有源 MAC 地址的请求帧。MAC 地址的持有者是该请求者(100)。

[0048] • 请求帧的接收通过控制信道(102)启动关于请求者的认证协议。

[0049] • 假如请求者不能被认证,或从该桥接器不批准请求 VLAN 服务(104),那么丢弃该请求(106)。

[0050] • 假如在使用请求的 VID 时没有冲突(105),新的逻辑端口建立并与接收请求帧的物理端口相关(108)。这是桥接器使用的逻辑端口以便服务 VLAN。否则,桥接器与请求者的 VID 协商(110)。VLAN 的过滤规则由用于请求者的政策确定。

[0051] • 端口状态信息被更新用于该逻辑端口从而包括安全关联(SA),并与请求者共享该信息,其可以有效用于通过那些端口的全部业务(112)。仅仅 SA 的持有者可以改变逻辑端口状态。

[0052] 当完成这些步骤时,新的逻辑端口存在用于服务新的 VLAN,但是该 VLAN 没有连接到桥接器服务的其它 VLAN,直到请求被做出以加入特殊的 VLAN。直到这时,新的 VLAN 不在该桥接器上工作。

[0053] 加入 VLAN

[0054] 通过桥接器服务的新 VLAN 扩展一个或多个通过该桥接器的端口服务的现存的 VLAN 将是有用的。换句话说,它必须连接一个或多个现存的 VLAN。连接通过桥接器的逻辑端口服务的 VLAN 到通过桥接器的物理端口服务的一个或多个 VLAN 通过在控制信道上发送的 join-VLAN 请求而执行。该请求不桥接由物理端口服务的多个 VLAN。更合适的,他们保持独立,但是同时新 VLAN 扩展了全部。

[0055] 加入 join-VLAN 请求包含由桥接器的逻辑端口 P' 服务的 VLAN 的 VID V',此处称作源 VLAN;和一组用于由一组物理端口 P 服务的 VLAN 的 VID 的 V,此处称作目的地 VLAN。该请求目的是连接 V' 到 V 中的每个 VLAN ID,或换句话说,目的在于允许请求者加入 V 中每个 VLAN。该请求者已经建立了 V'。桥接器采用以下步骤(参见图 6):

[0056] • 第一请求是认证(200)。这可以根据与当桥接器被要求服务 V' 时建立的 V' 相关的 SA 完成。一个简单的询问-响应策略被用于该优选实施例,虽然也可以适当的使用其它方法。假如认证失败,则丢弃该请求。

[0057] • 逻辑端口 P' 被增加到 V 中每个 VID 的成员组(202),而 P 中的每个物理端口被增加到 V' 中的成员组(204)。通过采用全部未加标签组的联合而形成用于 V' 中 VID 的 V' 的未加标签组(206)。假如该请求帧在它的标记头部包含一个空 VID,或它是未加标签的,那么 P' 被增加到 V 中每个 VID 的未加标签组(208)。

[0058] 服务于新的 VLAN 并链接它到其它 VLAN 的请求可以被合并成一个请求。因而,建立一个 VLAN 并加入另一个 VLAN 可以具体地通过一个认证过程完成,特别地,该过程需要服

务于新 VLAN。

[0059] 加入个人 VLAN

[0060] 加入个人 VLAN, 也就是由逻辑端口服务的一个要求特殊处理。个人 VLAN 桥接器不批准链接由逻辑端口服务的 VLAN, 因为它不能建立该端口, 这与它的物理端口不同。在这种情况下, 逻辑端口的创建者通过一个相互双方商定协议认证, 例如询问 - 响应。桥接器接收一个谁的目的地 VLAN 组包括单个由逻辑端口服务的 VLAN 的 join-VLAN 请求时, 站内认证(参见图 7)被触发(298)。

[0061] 有三种情况:

[0062] •源和目的地 VLAN 具有相同创建者, 并且该创建者发出 join-VLAN 请求(300)。在这种情况下, 该请求被丢弃(302)。否则, 可以在桥接地 VLAN 中产生循环。

[0063] •源和目的地 VLAN 是相同的, 并且创建者没有发出请求(304)。在这种情况下, 创建者对进入到个人 VLAN 内的请求者认证会员资格(306)。

[0064] •在全部其它情况下(308), 桥接器首先认证该请求以确信该请求者是源 VLAN 的创建者(和步骤 1一样, 用于加入仅仅由物理端口服务的 VLAN——参见上文)(310)。假如认证继续(312), 创建者对进入到目的地 VLAN 内的请求者认证会员资格(314)。

[0065] 当加入个人 VLAN 时, 目的地 VLAN 组最好准确的限于一个 VLAN, 也就是源 VLAN。因此它是被强制的, 因为该请求将另外反应一种企图, 即一个站桥接一个不拥有其它多个 VLAN 的 VLAN, 某些情况下它是不批准这么做的。VLAN 的拥有者可以加入一个新的 VLAN, 从而它的所有成员站也成为新的 VLAN 的成员。

[0066] 来自创建者的请求者的认证通过桥接器的控制信道和相应的 Auth/Supplicant 模块 50、52、54 变得更为方便。桥接器使用信道转播在创建者和请求者之间的认证协议信息。控制信道和转播信息的管理可以使用例如用于局域网和城域网的 IEEE 802.1X IEEE 标准: 基于网络接入控制 IEEE Std802.1X-2001 的端口实现。在 802.1x 模式中, 请求者是 Supplicant, 而创建者是 Authenticator。假如创建者可以认证请求者, 那么当 SA 持有桥接器时, 创建者与请求者共享 SA。当 SA 持有桥接器时, 决定是否将创建者与请求者共享 SA 不是桥接器的职责。这是创建者的职责。有很多方法可以完成共享。一个方法是使用请求者的公用密钥去加密运输层安全(TLS v1.0)预主密(pre-master secret), 其中 SA 可以得自请求者的站。

[0067] 在逻辑端口的入口过滤

[0068] 一个安全关联包含至少两个密钥, 一个用于加密, 另外一个用于计算认证码, 此处称作消息完整性编码(MIC)。特别地, SA 与 VLAN 相关。认证码在逻辑端口用来限制全部的 VLAN 的成员业务, 加密用来保持除成员之外的专用业务。仅仅具有 SA 的站属于 VLAN。有单个广播区域用于每一个 SA。所有具有 SA 的站属于相同的广播范围。因此, 没有独立的加密密钥需要广播。

[0069] 根据多个逻辑端口与 VLAN 相关的优点, 物理端口可以服务多于一个 VLAN(参见图 1)。因此, 除非在这样的端口接收的帧载波一个 VID, 它的 VLAN 分类必须使用基于端口的分级之外的规则。参看 IEEE 802.1Q, IEEE 标准用于局域网和城域网: 虚拟桥接局域网 IEEE 标准 802.1Q-1998, D. 2. 2。否则, 没有办法去知道眼下哪个 VID 应该从该端口服务的多个 VLAN 中被分配。必须通过接收帧识别逻辑端口。

[0070] 结合下列论述参见图 8。假如接收帧载波一个空 VID 或是未加标签的 (400), 那么它的源 MAC 地址用来确定一个初级的 VLAN 分类 (402)。这是逻辑端口的 PVID。假如该帧载波一个 VID, 那么 VID 被用作初级分类代替 (404)。该初级分类用来索引进入给出 MIC 密钥的安全关联表 (406)。接收帧载波一个 MIC, 所述 MIC 在使用例如 HMAC-MD5 的消息摘要算法的帧负载上计算以及由桥接器和请求者在认证时间同意并记录在 SA 中。该个人 VLAN 桥接器使用它的 MIC 密钥在接收帧的负载上重新计算 MIC(408), 然后把它与接收的 MIC 相比较 (410)。如果他们匹配 (412), 那么初级的 VLAN 分类成为最终的 VLAN 分类 (414)。最终的分类被用作任何相应原始数据请求的 VLAN 分类参数值 (416)。于是使用 SA 解密帧, 然后按照 IEEE802.1Q 前向转发和学习过程 (41)。否则, 该帧被丢弃。

[0071] 在逻辑端口的出口过滤

[0072] 在 VLAN 桥接器模式下, 假如用于属于某些 VLAN 的帧的传输端口不是 VLAN 的成员组, 那么该帧被丢弃。相同的规则应用于全部逻辑传输端口。

[0073] 虽然本发明于此参照优选实施例进行了描述, 但是本领域熟练的技术人员将很容易地理解在不脱离本发明的精神和范围的情况下, 其它的申请可以代替这里的阐述。因此本发明将仅仅由下文包括的权利要求限制。

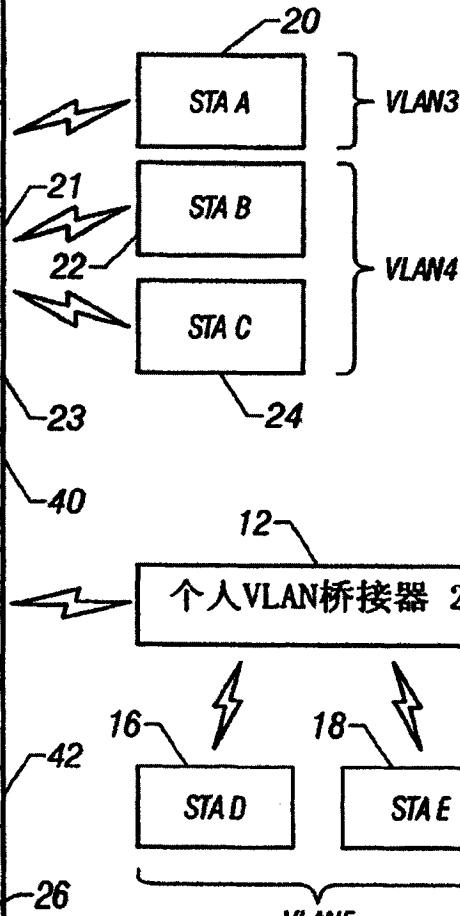
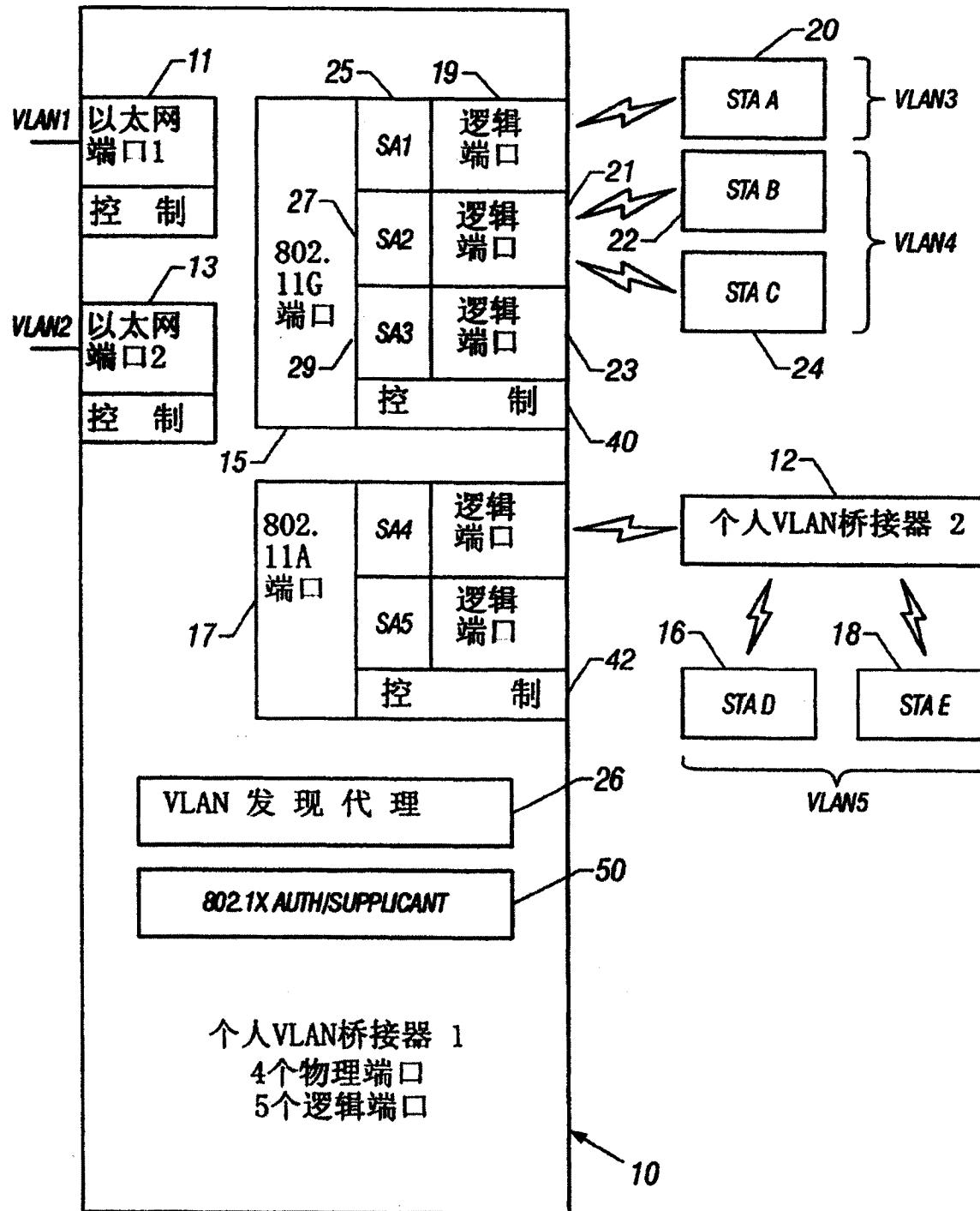


图 1

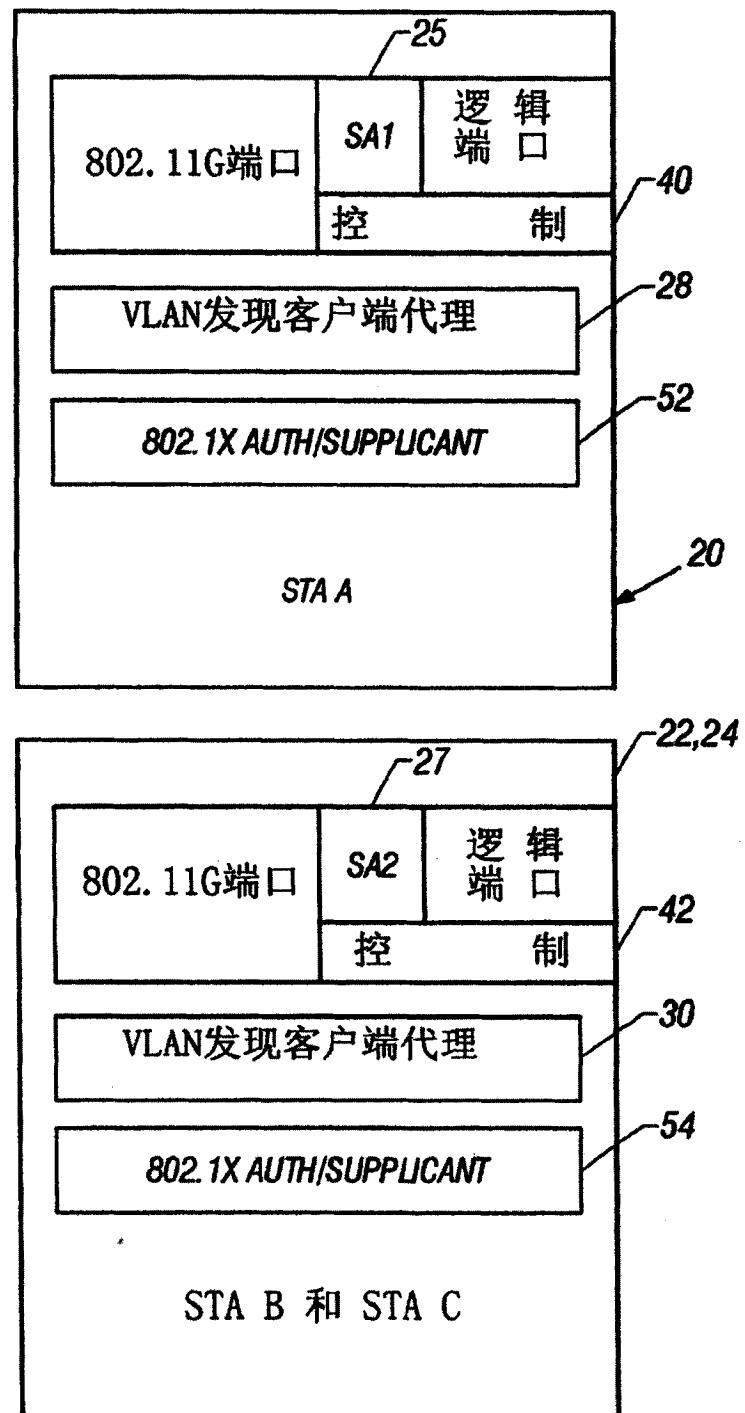


图 2

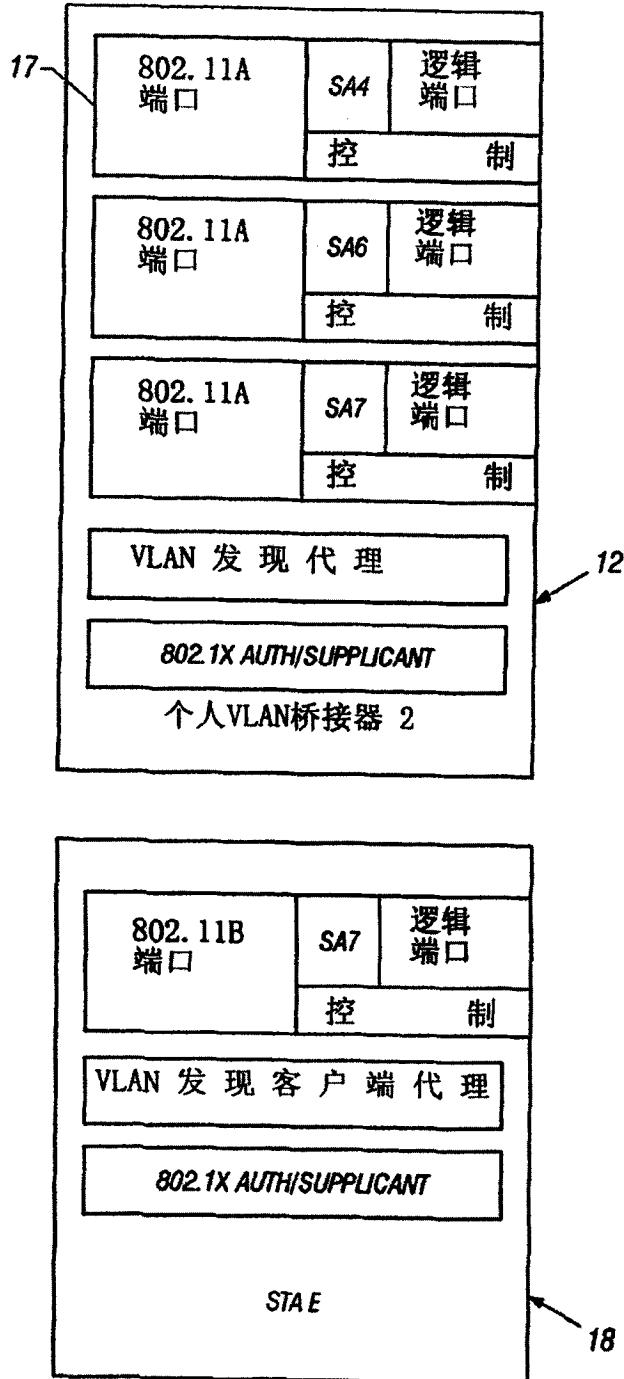


图 3

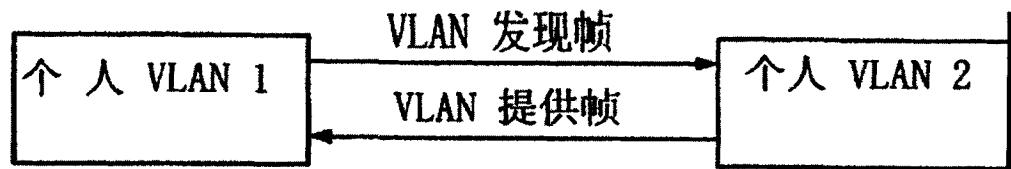


图 4

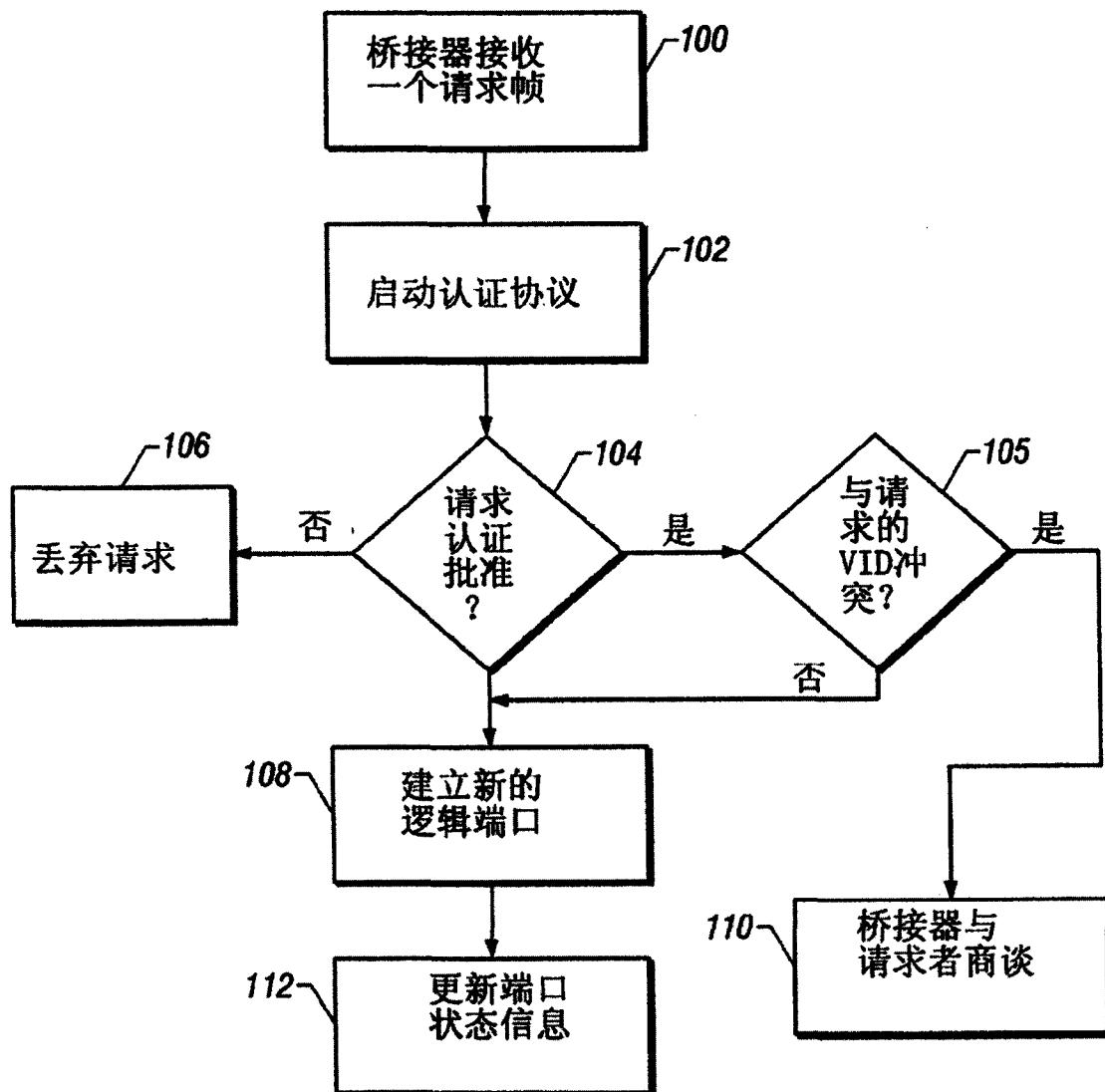


图 5

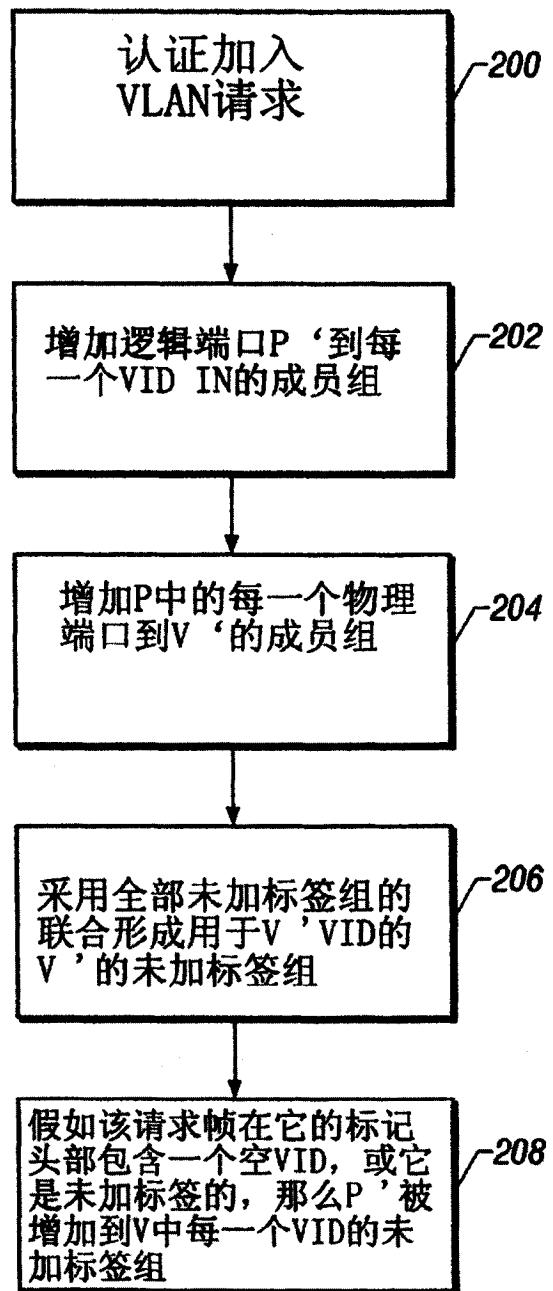
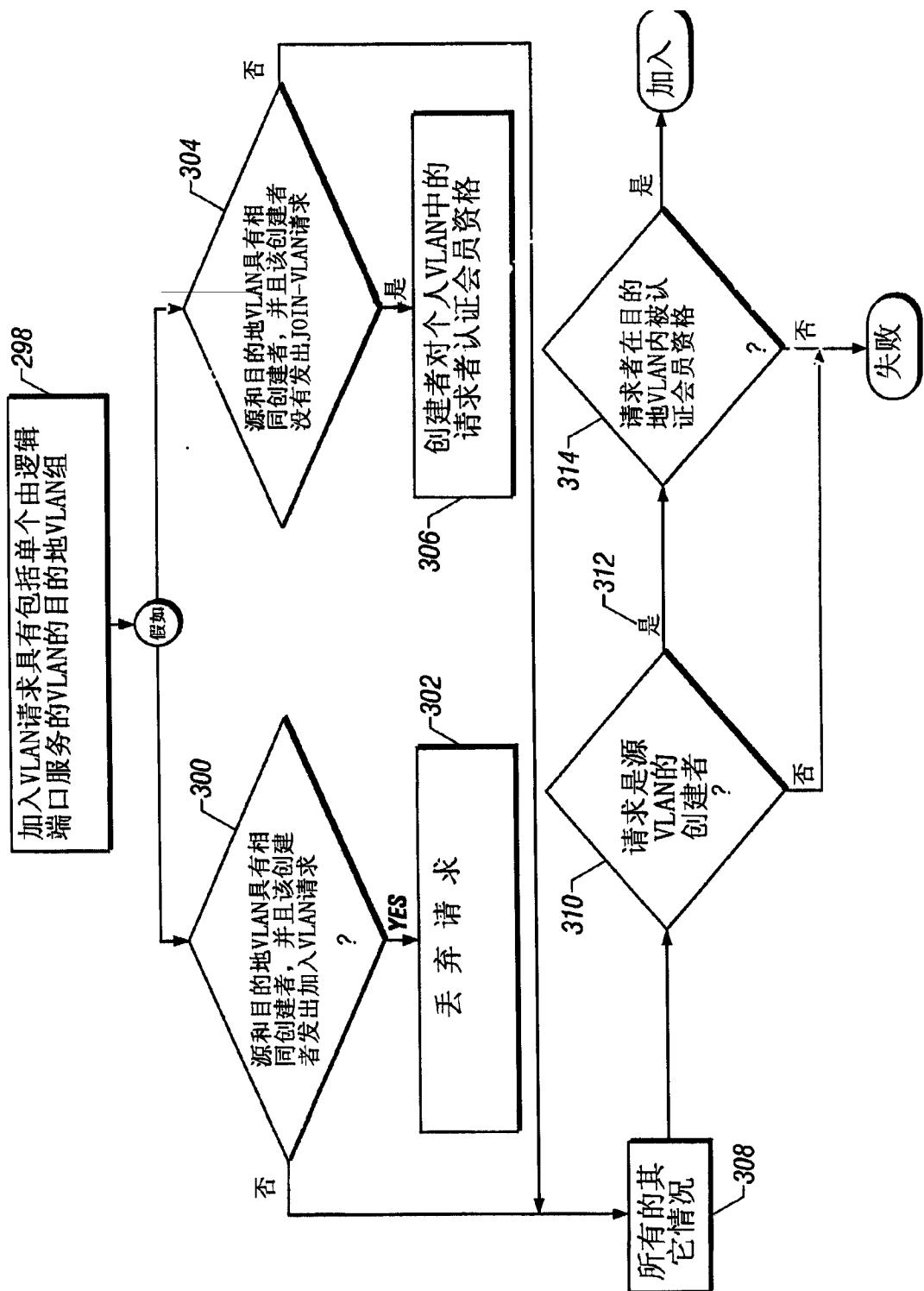


图 6



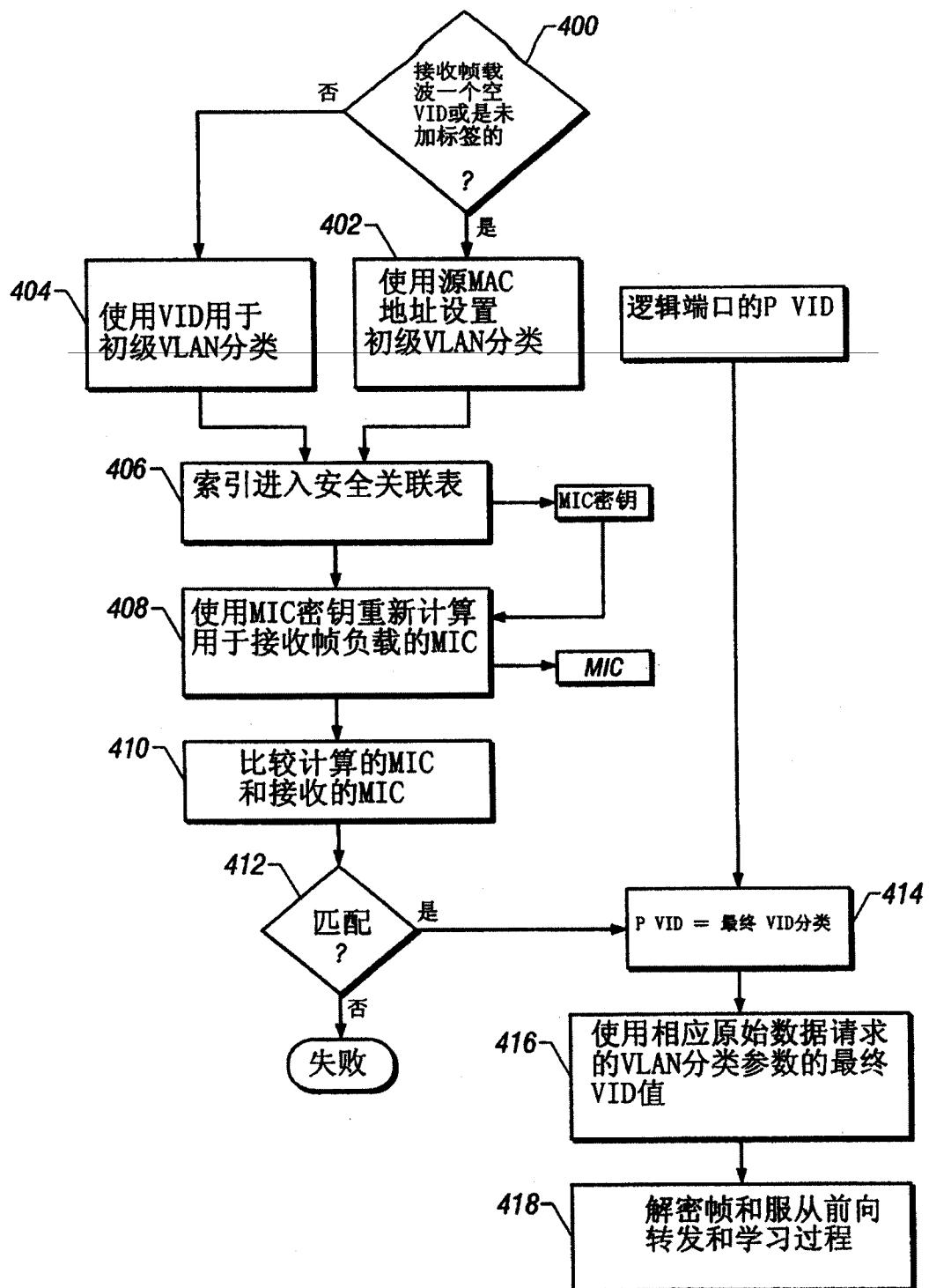


图 8