(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1662001 B
(45)授权公告日 2011.05.18

(21)申请号 200410003421.6

(22)申请日 2004.02.26

(73)专利权人 神州亿品科技有限公司
地址 100086 北京市海淀区玉泉山闵庄路 3 号清华科技园玉泉慧谷 25 号楼 2500、2502 室

(72)发明人 钱振宇 隋成

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 余刚

(51)Int.Cl.
H04L 29/02(2006.01)

(56)对比文件
CN 1357997 A,2002.07.10, 全文.
US 2003233461 A1,2003.12.18, 全文.
CN 1455905 A,2003.11.12, 全文.
CN 1437359 A,2003.08.20, 说明书第 2-5 页,图 4.
CN 1370300 A,2002.09.18, 全文.

审查员 冯美玉

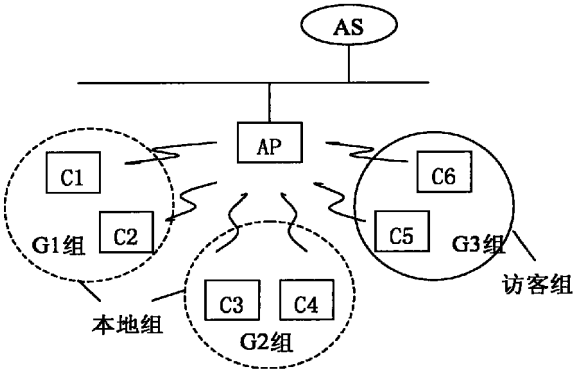
权利要求书 1 页 说明书 5 页 附图 1 页

(54)发明名称

一种无线局域网移动用户的分组实现方法

(57)摘要

一种对无线局域网中移动用户的分组,以及对这些用户之间的单播、多播和广播数据包的传输进行控制的方法。该方法实现了对不同组的本地用户之间的、访客用户之间的、以及访客用户和本地用户之间的数据传输控制,从而达到了在大多数应用程序下的一种基于用户组的用户访问控制。该方法的特点是它不需要移动用户装置特殊客户端软件,也不要求系统管理员管理加密密钥,所以系统和用户管理相对简单;但本方法本身不提供对无线数据传输的加密功能。



CN 1662001 B

1. 一种无线局域网移动用户的分组实现方法，其特征在于，本方法引入用户组的概念，每个组由若干用户组成，每个用户可属于多个用户组，根据对组内用户权限的控制方式，用户组分为两类：一类称为本地组，另一类称为访客组，其用户分别称为本地移动用户和访客移动用户；一个无线局域网可支持多个本地组，但只支持一个访客组；其中设置多个本地组，将企业本地移动用户按分组划分，使得同组内本地移动用户之间能够共享数据，并阻止属于不同组的本地移动用户共享数据；设置访客组，将所有访客移动用户归入该组，使得访客移动用户与本地移动用户之间，以及所有访客移动用户之间，都不能共享数据；也就是说，只要求有一个访客组。

2. 按照权利要求 1 中所述的方法，其中本地移动用户除了可以通过局域网访问外部互联网之外还有在用户组内互相访问的权限，而无跨用户组的访问权限；访客移动用户则只可访问外部互联网，而无相互访问的权限，更没有访问任何本地移动用户的权限。

3. 一种接入点转发用户到用户的数据包的方法，其特征在于，在执行核心步骤之前，作为准备步骤，所有移动用户必须先与接入点进行标准的 IEEE 802.11 关联，并执行一个相互鉴别过程；这鉴别过程无需产生任何用来加密数据的加密密钥，但接入点对所有通过鉴别的移动用户都建立了一个从用户 MAC 地址到所有所属用户组集合的映射；

在接入点 AP 收到用户 A 的数据包 P 后，先根据 P 中的发送 MAC 地址 SA 找到发送用户所对应的用户组集合 SG；

如果 P 中的目标 MAC 地址 DA 是本 AP 的 MAC 地址，而且 SG 含有至少一个本地组或访客组，AP 则将 P 送入自己的协议栈进行处理；这时，P 可能是本地用户或访客用户请求访问外部互联网的数据包；

如果 P 中的目标 MAC 地址 DA 是广播或多播地址，则执行如下步骤：

(a) 如 SG 带有本地组，AP 则转发 P；所有与 AP 关联并带有匹配 DA 的 MAC 地址的移动用户将能接收到 P；

(b) 否则，SG 不带有本地组，AP 则丢弃 P；

如果 P 中的目标 MAC 地址 DA 不是广播或多播地址，AP 则根据 DA 找到目标用户对应的用户组集合 DG：

(c) 如果集合 SG 和 DG 不包含任何相同用户组，包含 SG 或 DG 是空集的情况，AP 则丢弃 P；

(d) 否则，如果 SG 和 DG 包含相同的用户组，AP 则继续判断这些用户组的类型：

i. 如果这些相同的用户组中有一个本地组，AP 则转发 P；

与 AP 关联并带有 MAC 地址 DA 的用户将接收到 P；

ii. 否则，如果这些相同的用户组都是访客组，AP 则丢弃 P。

一种无线局域网移动用户的分组实现方法

技术领域

[0001] 本发明描述了一种对无线局域网移动用户进行分组，以及对这些用户之间的单播、多播和广播数据包的传输进行控制的方法。该方法实现了对不同组的本地用户之间的、访客用户之间的、以及访客用户和本地用户之间的数据传输控制，从而在大多数应用程序下实现了一种基于用户组的用户访问控制。

背景技术

[0002] 有线互联网中用户分组多基于虚拟局域网（VLAN 或 Virtual LAN）技术。这种技术的特点是通过网络设备对其物理端口的（接通和断开）控制来完成与这些物理端口相连接的用户的分组和相应数据传输控制。由于网络设备多处于系统管理员的控制下，这种分组方法具有较高的安全性。

[0003] 具体说来，虚拟局域网可以分为端口 VLAN、动态 VLAN、Super VLAN、MAC VLAN 等几种划分模式。

[0004] 端口 VLAN 是一种比较常用的 VLAN 划分方法，其原理是从逻辑上将局域网中交换机的端口分配到相应的 VLAN 中。每个 VLAN 有自己的 IP 地址空间。用户根据接入端口决定其所处 VLAN。端口 VLAN 分为单交换机和多交换机两种模式；前者只支持在一台交换机上指定若干的端口组成 VLAN，而后者允许一个 VLAN 跨越多个交换机，并且同一个交换机上的端口可以属于不同的 VLAN。

[0005] 动态 VLAN 的原理是在交换机的内存中制定一张用户信息表，用来记录相连用户的 IP 地址、VLAN 标识以及端口信息等。当用户交换数据时，交换机根据信息表进行检查，并根据检查结果进一步进行寻址和路由选择。动态 VLAN 的保密性比端口 VLAN 的安全性更高，因为交换机不仅要检查用户的 IP 地址还要复核其 VLAN 标识。

[0006] SuperVLAN 是目前比较先进的一种 VLAN 划分方法。SuperVLAN 的本质是采用了优化的 IP 地址的管理技术。它的每个子网（sub-VLAN）都是独立的多播通道，多播信息不能在不同的子网中进行交换。当数据需要送到多个目的节点时，就动态建立 VLAN 代理，通过代理设备对 VLAN 中的用户进行管理。这样每个子网不需要设定 IP 地址，而是一个 SuperVLAN 中的所有子网共享一个 IP 地址，这个 IP 地址就是 SuperVLAN 的 IP 地址。

[0007] MAC VLAN 通过设备的 MAC 地址（硬件地址），由人工进行初始配置来完成 VLAN 分类。当用户交换数据时，交换机根据人工配置进行寻址和路由选择。

[0008] 在无线局域网中，无线可在空中四面八方传播并被任何人接收，所以没有物理连线来保证虚拟局域网内（无线）移动用户的数据定向传输。这时，一般控制移动用户数据接收的方法是采用数据加解密技术。这种方法要求接入点和移动用户都带有加解密能力。任何以无线方式传输的信息都须先经加密后再发出；虽然任何接收点都能接收到发出的信息，但只有相应的接受点才能真正解密该信息，从而实现了数据的定向传输。

[0009] 基于数据加密的虚拟局域网具有较高的安全保密性，但缺点是移动用户需配有相应的客户端软件并带有相应证书或 / 和密钥来实现认证和加解密功能。这对密钥管理、用

户设置和用户管理，以至于整个系统的维护都提出了较高的要求。

发明内容

[0010] 本发明涉及无线局域网中用户的分组技术，以及基于用户组的用户数据传输控制技术。

[0011] 进一步说，本发明之技术区分无线局域网中的本地和访客用户，并将本地用户按用户组组织；它通过控制属于不同用户组的本地用户之间的、不同访客用户之间的、以及访客用户和本地用户之间的数据传输，实现所有用户之间的访问控制。

[0012] 本发明采用的技术是用接入点直接控制用户之间的单播数据传输，并以此来控制用户之间的多播和广播的应答，从而在大多数应用上提供用户访问控制。

[0013] 本发明引入用户组的概念，每个组由若干用户组成，每个用户可属于多个用户组。根据对组内用户权限的控制方式，用户组分为两类：一类称为本地（local）（用户）组，另一类称为访客（guest）（用户）组，其用户分别称为本地用户和访客用户。一个无线局域网可支持多个本地组，但只支持一个访客组。

[0014] 直观说来，本地用户除了可以通过局域网访问外部互联网之外还有在用户组内互相访问的权限，而无跨用户组的访问权限；访客用户则只可访问外部互联网，而无相互访问的权限，更没有访问任何本地用户的权限。

[0015] 设置多个本地组的动机是将企业本地移动用户按分组划分，使得同组内移动用户之间能够共享数据，并阻止属于不同组的移动用户共享数据。

[0016] 设置访客组的动机是将所有访客移动用户归入该组，使得访客移动用户与本地移动用户之间，以及所有访客移动用户之间，都不能共享数据。这些要求蕴含着只要有一个访客组就够用了！

[0017] 本发明的核心技术体现在一种接入点转发用户到用户的数据包的方法。在执行相应的核心步骤之前，作为准备步骤，所有移动用户必须先与接入点进行标准的 IEEE 802.11 关联，并执行一个相互鉴别过程；这鉴别过程无需产生任何用来加密数据的加密密钥，但接入点对所有通过鉴别的移动用户都建立了一个从用户 MAC 地址到所有所属用户组集合的映射。在执行了上述准备步骤后，核心步骤的可具体描述如下：

[0018] 1、在接入点 AP 收到用户 A 的数据包 P 后，先根据 P 中的发送 MAC 地址 SA 找到发送用户所对应的用户组集合 SG；

[0019] 2、如果 P 中的目标 MAC 地址 DA 是本 AP 的 MAC 地址，而且 SG 含有至少一个本地类分组或访客组（即 SG 非空），AP 则将 P 送入自己的协议栈进行处理；（这时，P 可能是本地用户或访客用户请求访问外部互联网的数据包。）

[0020] 3、如果 P 中的目标 MAC 地址 DA 是广播或多播地址，则执行如下步骤：

[0021] a) 如 SG 带有本地类分组，AP 则（无线）转发 P；（所有与 AP 关联并带有匹配 DA 的 MAC 地址的移动用户将能接收到 P。）

[0022] b) 否则，即 SG 不带有本地类分组（是空集或只带有访客组），AP 则丢弃 P。

[0023] 4、否则，即如果 DA 不是广播或多播地址，AP 则根据 DA 找到目标用户对应的用户组集合 DG，

[0024] a) 如果集合 SG 和 DG 不包含任何相同用户组（包含 SG 或 DG 是空集的情况），AP

则丢弃 P。

[0025] b) 否则，即如果 SG 和 DG 包含相同的用户组，AP 则继续判断这些用户组的类型：

[0026] i. 如果这些相同的用户组中有一个本地组，AP 则（无线）转发 P；

[0027] （与 AP 关联并带有 MAC 地址 DA 的用户将接收到 P。）

[0028] ii. 否则，即如果这些相同的用户组都是访客组，AP 则丢弃 P。

[0029] 上述步骤达到如下效果：

[0030] ●转发本地和访客用户请求访问外部互联网的所有数据包；

[0031] ●转发本地用户发出的任何多播和广播数据传输；

[0032] ●截断访客用户发出的任何多播和广播数据传输；

[0033] ●转发任何在同一本地组内的用户之间的单播数据传输；

[0034] ●截断不同用户组的用户之间的单播数据传输；

[0035] ●截断访客组用户与任何其它访客组或本地组用户之间的单播数据传输；

[0036] ●截断从无所属用户组的用户发出的任何单播、多博和广播数据传输；

[0037] ●截断向无所属用户组的用户发出的任何单播、多博和广播数据传输。

[0038] 虽然上述步骤转发本地用户的多播和广播，但由于多播和广播的应答多为单播，所以这些步骤还是可以截断多播和广播的应答，使需要应答的多播和广播通信过程无法完成，从而阻止那些基于多播和广播应答的协议、如 ARP、DHCP 和 NetBIOS 协议等的完成。

附图说明

[0039] 图 1 是本发明的分组方法及移动用户与接入点进行关联的示意图。AP 依靠其鉴别服务功能在此完成移动用户的鉴别、分组及无线接入控制。

[0040] 图 2 是分组方法逻辑描述示意图。

具体实施方式

[0041] 本发明的一个具体实施可参照图 1 如下解释。

[0042] 在执行本发明核心步骤之前，所有移动用户 C1、C2、C3、C4、C5 和 C6 都必须先与接入点 AP 进行关联，并依靠系统的鉴别服务 AS(AuthenticationService) 与 AP 相互鉴别；AS 可运行于系统内的一台单独的服务器、AP、或其它的网络设备的硬件之上。鉴别的机制可以是多样的，如基于 IEEE802.1X 的用户名 / 口令 (EAP-MD5 即 Extensible Authentication Protocol-Message Digestalgorithm 5) 模式、IEEE802.1X 的数字证书 (EAP-TLS 即 ExtensibleAuthentication Protocol-Transport Layer Security) 模式、或基于 WEB 的用户名 / 口令模式等。不同鉴别的机制决定了移动用户与 AP 关联完成和鉴别的顺序。但无论是怎样的顺序，在关联和鉴别成功完成后，AP 都已找出所有用户的所属分组。这里我们需要特别指出，本发明所描述的步骤只控制用户之间的数据传输，而不影响用户和系统的数据传输；这里用户和系统的数据传输包括在执行 IEEE802.1X 的鉴别过程中，用户与 AS 和 AP 的信息交换，还包括在执行基于 WEB 的用户名 / 口令鉴别过程时，移动用户必须在通过 WEB 输入用户名 / 口令之前，已与 AP 成功关联并与 DHCP 服务通过信息交换取得局域网地址。

[0043] 在图 1 中，移动用户 C1、C2、C3、C4、C5 和 C6 均通过关联和鉴别，AP 也已找出它们

所属的本地组 G1 和 G2，以及访客组 G3，并建立了从 MAC 地址到这些用户组的映射。

[0044] 在已经建立了用户组映射以后，本发明的核心步骤将进行如下执行：

[0045] ●当 C1 经 AP 向 C2 发送单播数据时，由于 C1 和 C2 属于同一本地组，AP 转发此数据，使 C2 能够接收到此数据；进一步，当 C2 经 AP 向 C1 发送（单播）应答时，由于同样的原因，C2 也能够接收到该应答。

[0046] ●当 C1 经 AP 向 C3（或 C5）发送单播数据时，由于 C1 和 C3（或 C5）属于不同用户组，因此 AP 丢弃此数据，使 C3（或 C5）不能收到此数据，从而使 C1 与 C3（或 C5）的通信不能完成。

[0047] ●当 C1 经 AP 向用户组 G1 发广播（或多播）数据时，由于是广播（或多播），也由于 C1 属于的用户组 G1 是本地组，所以 AP 将广播（或多播）数据发出。用户组 G1 内的所有除 C1 外的用户 - 当前例子中只有 C2- 都可以收到此广播（或多播）信息。进一步，当 C2 经 AP 向 C1 发送对应此广播（或多播）的（单播）应答时，由于 C1 和 C2 属于同一本地组，C1 也能够接收到应答。

[0048] ●当 C1 经 AP 向用户组 G2（或 G3）发广播（或多播）数据时，由于是广播（或多播），也由于 C1 属于的用户组 G1 是本地组，所以不管用户组 G2（或 G3）是什么类型的用户组，也不管 C1 是否属于用户组 G2（或 G3），AP 一律将广播数据发出。用户组 G2（或 G3）内的所有用户，都可以收到此广播（或多播）信息。但是，当 G2（或 G3）内的用户，例如 C3（或 C5），经 AP 向 C1 发送对应此广播（或多播）的（单播）应答时，由于 C3 和 C5 不属于 G1，因此 AP 丢弃此应答，从而使 C1 不能够接收到应答。

[0049] ●当 C5 经 AP 向 C1 发送单播数据时，由于 C5 和 C1 属于不同用户组，因此 AP 丢弃此数据，从而使 C1 不能收到此数据 .

[0050] ●当 C5 经 AP 向 C6 发送单播数据时，由于 C5 属于访客组，故 AP 丢弃此数据，从而使 C6 不能收到此数据。

[0051] ●当 C5 经 AP 向用户组 G1(G2 或 G3) 发广播（或多播）数据时，由于 C5 属于访客组，故 AP 丢弃此广播（或多播）数据，从而使 G1(G2 或 G3) 内用户不能收到此广播（或多播）数据。

[0052] ●在一个用户正处于鉴别过程中，AP 还不存有从此用户 MAC 地址到其所属用户组的映射，即此用户的所属用户组集为空，所以 AP 将不转发此用户转来的单播，多播或广播的数据，也不转发以此用户为目标地址的数据。

[0053] ●上述仅是举例，事实上，C1 与 C2，C3 与 C4，C5 与 C6 等起组内的其他用户其顺序调换是等效的。

[0054] 在移动用户都使用 Windows 操作系统的前提下，本发明保证了无线局域网内的以下特征：

[0055] ● AP 不允许一个未鉴别的移动用户与其他任何（未鉴别或已鉴别的）用户利用网上邻居 (Network Neighborhood) 进行相互访问；这里的原因是对未鉴别的移动用户，AP 不存有从其 MAC 地址到用户组的映射。

[0056] ● AP 允许所有俩俩经过成功鉴别、且属于统一本地类用户组的移动用户通过网上邻居相互访问；

[0057] ● AP 不允许访客用户通过网上邻居访问任何其他网上用户，也不允许访客用户

通过网上邻居被任何其他网上用户访问。

[0058] 本发明的特点之一是无线局域网中的移动用户使用 Web 浏览器、用户名和密码进行鉴别和接入，而不需要特别客户端软件和数字证书，从而省去许多系统管理员的麻烦。但本发明不提供对无线传输的数据加密功能。

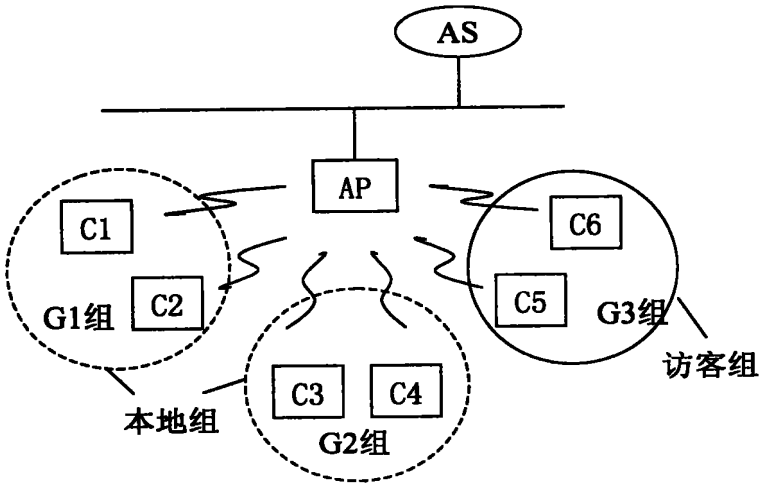

AS
AP
C1
C2
G1组
本地组
C3
C4
G2组
C6
C5
G3组
访客组

图 1

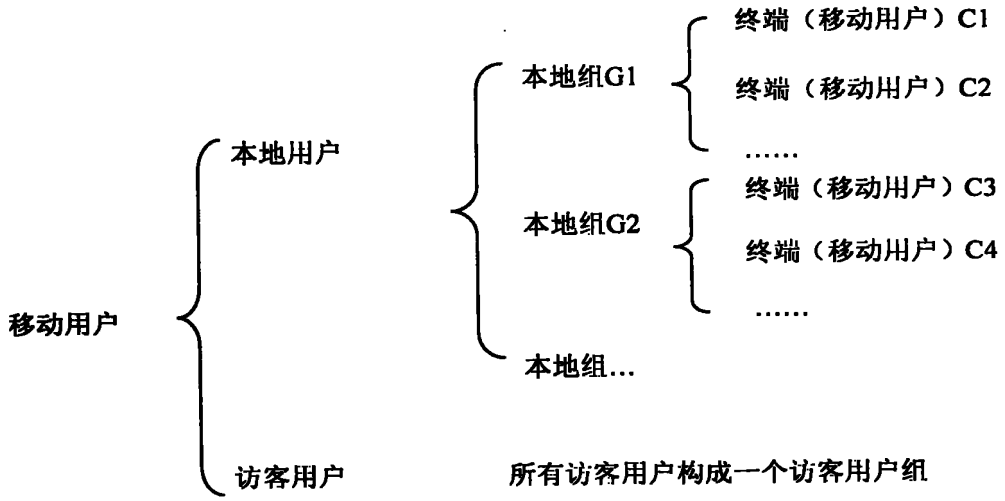

移动用户
本地用户
访客用户
本地组G1
本地组G2
本地组...
终端（移动用户）C1
终端（移动用户）C2
.....
终端（移动用户）C3
终端（移动用户）C4
.....
所有访客用户构成一个访客用户组

图 2