[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/46
H04L 29/06
G06F 15/17

[12] 发明专利申请公开说明书

[21] 申请号 03820629.3

[43] 公开日 2005 年 10 月 5 日

[11] 公开号 CN 1679280A

[22] 申请日 2003.7.3 [21] 申请号 03820629.3
[30] 优先权
[32] 2002. 7. 5 [33] SE [31] 0202125 - 1
[86] 国际申请 PCT/SE2003/001161 2003.7.3
[87] 国际公布 WO2004/006513 英 2004.1.15
[85] 进入国家阶段日期 2005.2.28
[71] 申请人 帕克特弗兰特瑞典股份公司
地址 瑞典基斯塔
[72] 发明人 F·尼曼 A·厄曼
M·伦德斯特伦 A·贡纳松

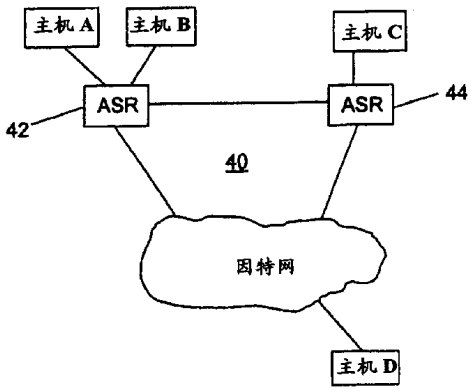
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 杨 凯 王 勇

权利要求书 3 页 说明书 17 页 附图 2 页

[54] 发明名称 业务分隔的过滤器

[57] 摘要

本发明涉及一种用于网络(40)的至少一个访问交换路由器(42)中的开放式系统互连第 2 层业务量分隔的过滤器，在路由器(42，44)中具有配置到相同虚拟局域网的端口。 过滤器过滤送往这些端口的数据包，进行模拟，如果源装置和目标装置在相同的第 2 层域中，则路由器第 2 层地址是源以及目标两种装置的实际目标地址。 还进行模拟，如果源装置和目标装置不在相同的第 2 层域中，但在相同的第 3 层子网中，则路由器第 2 层地址是源对目的地的实际目标第 2 层地址。 通过这种过滤来提供对一个 IP 子网的应用，将它遍布若干房屋和多个访问交换路由器及多个第 2 层域中的相同子网，从而覆盖更多客户。



ISSN1008-4274

1. 一种用于网络(40)的至少一个访问交换路由器(42,44)中的开放式系统互连第2层业务分隔的过滤器，在所述路由器(42,44)中具有配置到相同虚拟局域网的端口，所述过滤器过滤到所述端口的数据包业务，其特征在于它包括:

用于截取来自属于所述虚拟局域网的媒体访问控制地址的网络连接源装置(主机A,主机B)的第2层业务，确定是否准许业务被转发到其它端口的部件;

用于不管目标装置第2层域是否与源装置第2层域相同、响应对所述源装置(主机A,主机B)的所述广播而截取这种业务中的地址解析协议广播的部件，因而所述源装置(主机A,主机B)确定所述广播已经确认所寻找的目标装置(主机C,主机D)的第2层地址，从而所述源装置(主机A,主机B)将数据包传送给所述目标装置(主机C,主机D)，所述路由器接收所述传送的数据包;

用于确定到所述目标装置的出口端的部件;

用于确定所述目标装置(主机C,主机D)的第2层地址的部件;

用于从所述接收数据包调整所述第2层首标的部件，所述部件用于设置所述源第2层地址，设置所述数据包的所述路由器源地址，所述部件用于确定所述目标装置(主机C,主机D)的第2层地址，将所述目标第2层地址设置到所述目标装置(主机C,主机D)的地址，将所述数据包传送给所述目标装置(主机C,主机D); 以及

因此进行模拟，如果所述源装置(主机A,主机B)和目标装置(主机C,主机D)处于相同的第2层域，则所述路由器第2层地址为所述源和目标装置的实际目标地址，或者进行模拟，如果所述源装置和目标装置不在相同的第2层域但在相同的第3层子网，则所述路由器第2层地址为所述源对所述目的地的实际目标第2层地址。

2. 如权利要求 1 所述的过滤器，其特征在于，在对所述目标装

置(主机 C)寻址时为驻留在子路由器(42,44)中的端口提供所述路由器(42,44)第 2 层地址。

3. 如权利要求 1 或 2 所述的过滤器，其特征在于，所述路由器(42,44)正调查所述源和/或目标地址，以确定所述数据包的最佳出口端，确定所述数据包是否处于速率限制的简档中，或者根据所述开放式系统互连第 3 层及更高协议层中的信息进行其它过滤。

4. 如权利要求 1-3 所述的过滤器，其特征在于，路由器(42,44)是第 2 层交换机与第 3 层路由器的组合，将具有高级包控制的第 2 层交换和在第 3 层路由器中转发判定的能力进行结合。

5. 如权利要求 1-4 所述的过滤器，其特征在于，提供对一个 IP 子网的应用，将它遍布若干房屋和多个访问交换路由器及多个第 2 层域中的相同子网，从而覆盖更多客户。

6. 如权利要求 5 所述的过滤器，其特征在于，让具有多台计算机的用户接收更多地址。

7. 一种用于网络(40)的至少一个访问交换路由器(42,44)中的开放式系统互连第 2 层业务分隔的过滤器的方法，在所述路由器(42,44)中具有配置到相同虚拟局域网的端口，所述过滤器过滤到所述端口的数据包业务，其特征在于它包括:

截取来自属于所述虚拟局域网的媒体访问控制地址的网络连接源装置(主机 A,主机 B)的第 2 层业务，确定是否准许业务被转发到其它端口;

不管目标装置第 2 层域是否与源装置第 2 层域相同，响应对所述源装置(主机 A,主机 B)的所述广播而截取这种业务中的地址解析协议广播，因而所述源装置(主机 A,主机 B)确定所述广播已经确认所寻找的目标装置(主机 C,主机 D)的第 2 层地址，从而所述源装置(主机 A,主机 B)将数据包传送给所述目标装置(主机 C,主机 D)，所述路由器接收所述传送的数据包;

确定到所述目标装置的所述出口端;

确定所述目标装置(主机 C,主机 D)的第 2 层地址;

从所述接收数据包调整所述第 2 层首标,所述部件用于设置所述源第 2 层地址,设置所述数据包的所述路由器源地址,所述部件用于确定所述目标装置(主机 C,主机 D)的第 2 层地址,将所述目标第 2 层地址设置到所述目标装置(主机 C,主机 D)的地址,将所述数据包传送给所述目标装置(主机 C,主机 D); 以及

因此进行模拟,如果所述源装置(主机 A,主机 B)和目标装置(主机 C,主机 D)处于相同的第 2 层域,则所述路由器第 2 层地址为所述源以及目标装置的实际目标地址,或者进行模拟,如果所述源装置和目标装置不在相同的第 2 层域但在相同的第 3 层子网,则所述路由器第 2 层地址为所述源对所述目的地的实际目标第 2 层地址。

8. 如权利要求 7 所述的用于过滤器的方法,其特征在于,在对所述目标装置(主机 C)寻址时为驻留在子路由器(42,44)中的端口提供所述路由器(42,44)第 2 层地址。

9. 如权利要求 7 或 8 所述的用于过滤器的方法,其特征在于,路由器(42,44)正调查所述源和/或目标地址,以确定所述数据包的最佳出口端,确定所述数据包是否处于速率限制的简档中,或者根据所述开放式系统互连第 3 层及更高协议层中的信息进行其它过滤。

10. 如权利要求 7-9 所述的用于过滤器的方法,其特征在于,路由器(42,44)是第 2 层交换机与第 3 层路由器的组合,将具有高级包控制的第 2 层交换和在第 3 层路由器中转发判定的能力进行结合。

11. 如权利要求 7-10 所述的用于过滤器的方法,其特征在于,提供对一个 IP 子网的应用,将它遍布若干房屋和多个访问交换路由器及多个第 2 层域中的相同子网,从而覆盖更多客户。

12. 如权利要求 11 所述的用于过滤器的方法,其特征在于,让具有多台计算机的用户接收更多地址。

业务分隔的过滤器

技术领域

本发明涉及用于在网络的至少一个路由器中的开放式系统接口第2层业务分隔的过滤器以及用于此目的的方法。

背景技术

在为基于 Ethernet®的网络或类似网络安装网络装置（如路由器和交换机）时，运用 MAC 寻址(媒体访问控制寻址)的现行 OSI 第 2 层(开放式系统互连)技术使 VLAN(虚拟局域网)能够用于分隔例如第2层上的路由器和交换机的装置中的物理端口，以及将多个装置上属于相同 VLAN 的端口绑定在一起，称作“中继”。

在通过路由器运用 IP 寻址的 OSI 第 3 层，每个 VLAN 要求不同的 IP 子网用于寻址。在过去的几年，在使用这种技术来安装宽带网络方面已经进行了若干尝试。

Ethernet®是按照 CSMA/CD(带有检测冲突的载波侦听多路存取)的共享媒体，它表示连接到同一个 Ethernet®的所有主机获得全部业务，但它们依靠其 MAC 地址进行选取。

典型的宽带网络由安装在住宅区的多个交换机或路由器组成，以便把各个家庭连接到公共基础设施，即通常据说的服务提供商基础设施。

通过采用以太网技术来实现这个目的，立即引起一个如以太网所提供的把不同房屋、如家庭等连接到单个共享基础设施的安全问题。

服务提供商必需考虑:

- 将每个客户连接到单独的 VLAN-从而要求大量小 IP 子网，各 VLAN 一个，以保存第 2 层分隔。

- 将客户连接到单个 VLAN-从而要求单个更大的 IP 子网，但带

来了允许不同客户之间的第 2 层访问、如 Microsoft®文件共享的风险。

为了解决这种过滤问题，有些实现采用端口保护功能，其中，归入同一个 VLAN 的同一个装置中的两个端口之间的业务被阻止。这意味着连接在那些端口上的主机无法交换任何业务。对这种解决方案的其它增强包括将受保护端口之间的数据包转发给上游过滤装置，它判定是否应该准许数据包业务，假如是这样的话，则将该业务重新转发给其目的地。这无疑将增加交换机与过滤装置之间的主干链路的负荷。

随着目前到 Ethernet®网络的连接计算机数量的增加，加大了有关数据业务冲突的问题。为了解决这个问题，发明了网桥，它把 Ethernet®分为若干段，并记住/了解不同的 MAC 地址驻留在哪些段中。此后，数据包的转发只对送往广播地址或者驻留在非发送它的另一个段中的 MAC 地址的数据包来完成。但是，不同段仍然是同一个广播域的一部分。

当前的交换机是网桥的进一步发展。据说它们在每个端口都有网桥。交换机记住/了解哪些 MAC 地址分别驻留在每个端口，并且仅当业务要送往不同端口的 MAC 地址时才实现端口之间的转发。因此，每个端口成为一段，但每个端口(a1 段)仍然是同一个广播域的一部分，因为广播被传送给每个端口。采用交换机的一个优点在于以高速进行通信，它实现了多个端口可同时以最高速度相互通信。

交换技术例如通过引入 VLAN、中继和生成树得到发展。

VLAN 使得能够将交换机中的端口分组为不同的广播域。其中包括，包含在特定 VLAN 中的端口无法与不同的 VLAN 中的端口通信。至少不通过第 2 层，它要求路由器连接这类端口。

在 RFC1027(IETF 控制下的“请求注释”文档；因特网工程任务小组)中，描述了称作“代理 ARP”的技术，在其中，路由选择装置响应本地连接主机请求的、对本地子网之外的任何地址的 ARP 请

求，从而让主机向路由器发送全部业务，而不要求了解IP缺省路由。这在因特网初期在缺少对IP的全面了解时用来指导主机，采用IP协议进行通信。目前很少采用。

发明内容

本发明针对解决与OSI第2层广播以及对于多个VLAN将IP地址分为子网的有限能力有关的问题。

为了实现它的目标和目的，本发明提出一种用于在网络的至少一个访问交换路由器中的开放式系统互连第2层业务分隔的过滤器。路由器中的端口配置到同一个虚拟局域网。过滤器过滤送往这些端口的数据包业务。它还包括:

用于截取来自属于虚拟局域网的MAC地址的网络连接源装置的第2层业务并确定是否准许业务被转发到其它端口的部件;

用于不管目标装置第2层域是否与源装置第2层域相同、响应对源装置的广播而截取这种业务中的地址解析协议广播的部件，因而源装置确定广播已经确认所寻找的目标装置的第2层地址，从而源装置将数据包传送给目标装置，路由器接收所传送的数据包;

用于确定到目标装置的出口端的部件;

用于确定目标装置的第2层地址的部件;

用于从所接收数据包调整第2层首标的部件，该部件用于设置源第2层地址，设置数据包的路由器源地址，该部件用于确定目标装置的第2层地址，将目标第2层地址设置到目标装置的地址，将数据包传送给目标装置；以及

因此进行模拟，如果源装置和目标装置处于相同的第2层域，则路由器第2层地址为源以及目标两种装置的实际目标地址，或者进行模拟，如果源装置和目标装置不在相同的第2层域但在相同的第3层子网，则路由器第2层地址为源对目的地的实际目标第2层地址。

在本发明的一个实施例中，假定在对目标装置寻址时为驻留在子路由器中的端口提供了所述路由器第2层地址。

另一个实施例提出，路由器正调查源和/或目标地址，以便确定数据包的最佳出口端，确定该数据包是否处于速率限制的简档中，或者根据开放式系统互连第 3 层及更高协议层中的信息进行其它过滤。

另一个实施例提出，访问交换路由器是第 2 层交换机与第 3 层路由器的组合，将具有高级包控制的第 2 层交换和在第 3 层路由器中转发判定的能力进行结合。

又一个实施例提供对 IP 子网的应用，将它遍布若干房屋和多个访问交换路由器及多个第 2 层域中的相同子网，从而覆盖更多客户。又一个实施例让具有多台计算机的用户接收更多地址。

本发明还提出一种用于在网络的至少一个访问交换路由器中的开放式系统互连第 2 层业务分隔的过滤器的方法。路由器让路由器中的端口配置到同一个虚拟局域网。过滤器过滤送往这些端口的数据包业务。它还包括以下步骤：

截取来自属于虚拟局域网的媒体访问控制地址的网络连接源装置(主机 A,主机 B)的第 2 层业务，确定是否准许业务被转发到其它端口；

不管目标装置第 2 层域是否与源装置第 2 层域相同、响应对源装置的广播而截取这种业务中的地址解析协议广播，因而源装置确定广播已经确认所寻找的目标装置的第 2 层地址，从而源装置将数据包传送给目标装置，路由器接收所传送的数据包；

确定到目标装置的出口端；

确定目标装置的第 2 层地址；

用于从所接收数据包调整第 2 层首标，该部件用于设置源第 2 层地址，设置数据包的路由器源地址，该部件用于确定目标装置的第 2 层地址，将目标第 2 层地址设置到目标装置的地址，将数据包传送给目标装置；以及

因此进行模拟，如果源装置和目标装置处于相同的第 2 层域，则

路由器第 2 层地址为源以及目标装置的实际目标地址，或者进行模拟，如果源装置和目标装置不在相同的第 2 层域但在相同的第 3 层子网，则路由器第 2 层地址为源对目的地的实际目标第 2 层地址。

大家知道，该方法能够执行符合上述实施例的所附从属方法权利要求集的步骤。

附图说明

此后，为了更好地理解本发明的给定实例和实施例，必需参照附图，附图包括:

图 1 示意说明连接到根据先有技术的宽带网络的住宅区;

图 2 示意说明连接在根据先有技术的两个宽带网络之间的网关; 以及

图 3 示意说明根据本发明的宽带网络。

具体实施方式

根据本发明，为了能够理解对于与第 2 层数据业务相关的问题的解决方案，了解 IP 寻址的基本特征也是重要的。将 Ethernet®用于 IP 通信的主要部分是使用 ARP(地址解析协议)协议。ARP 用于在 OSI 第 2 层与第 3 层地址之间进行解析。它使主机在已经知道第 3 层地址时能够确定另一个装置的第 2 层地址。这在 IP 子网中的主机要与同一个子网中的另一个主机通信时使用。因此，ARP 用于第 2 层地址(Ethernet®MAC 地址)与第 3 层地址(IP)之间的解释。

IP 的主要部分在于，不是网络中的每个装置都需要了解所提供的全局路由选择表。如果某个装置有数据包要转发给未知目的地，则该装置可配置缺省路由，即用于没有明确路由的任何业务的路径。缺省路由始终为主机直接连接到的子网中的 IP 地址。缺省路由的第 2 层地址由 ARP 协议记住/了解，除非没有在主机中静态配置。

根据本发明，路由器被定义为一种装置，这种装置分析 OSI 第 3 层或更高层协议信息以便进行业务转发判定。

这包括但不限于，调查源和/或目标地址，以便确定数据包的最

佳出口端，确定该数据包是否处于速率限制的简档中，或者根据 OSI 第 3 层及更高协议层中的信息进行其它过滤。

访问交换路由器(ASR)为第 2 层交换机与第 3 层路由器的组合。它把具有高级包控制的第 2 层交换和在第 3 层路由器中转发判定的能力进行结合。这个定义适合根据本发明的路由器的定义，并且还结合了本文所述的独立过滤特征。

本发明的优点使 ASR 中的所有 Ethernet®端口能够配置到同一个 VLAN，它使这些端口共享同一个 IP 子网。因此，不需要进行任何子网、如 32 位 IP 地址的分割。每次创建子网时，两个地址消失。它们是所谓的网址及作为子网广播地址的地址。当公司、因特网服务提供商等连接到因特网时，它们申请 IP 地址。地址的分配取决于连接到网络的计算机的数量、网络的设计方式及其将来的增长速度。

作为实例，为某个公司分配 192.168.1.0/24 作为地址，其中/24 表示子网范围。由于 IP 地址具有 32 个二进制位，因此更易于以二进制表示来提供实例:

192.168.1.0 = 11000000 10101000 00000001 00000000 /24 等于一个十进制子网掩码 255.255.255.0，二进制重组 11111111 11111111 11111111 00000000。

子网掩码为 0、以下表示主机部分的子网的部分允许用于设置单个计算机的 IP 地址。子网掩码为 1 的部分必须始终相同。这个部分的两个地址绝不可用于计算机，它们在主机部分仅包含二进制 0 时实质上是网络编号，以及在主机部分仅包含二进制 1 时是广播地址。因此:

11000000 10101000 00000001 00000000 192.168.1.0

11000000 10101000 00000001 11111111 192.168.1.255

250 台计算机连接到同一段是不太可能的。也许它由分为若干第 2 层广播域的数个段组成，因此每个第 2 层域需要它本身的一个 IP 子网。因此，需要将 256 个地址分为较小的子网。这通过进一步延长

子网掩码、即包含二进制 1 的部分来实现。

实例 1:

11000000 10101000 00000001 00000000 192.168.1.0

11111111 11111111 11111111 11000000 255.255.255.192

子网掩码这时正切入最后一个八位组中的两个位。这表示有 6 位保留用于主机地址，它以十进制方式重组为 64。因此，256 个地址已经变成各有 64 个地址的四个子网。

11000000 10101000 00000001 00000000 192.168.1.0

11111111 11111111 11111111 11000000 255.255.255.192

11000000101010000000000l 01000000 192.168.1.64

11111111 11111111 11111111 11000000 255.255.255.192

11000000 10101000 00000001 10000000 192.168.1.128

11111111 11111111 11111111 11000000 255. 255.255.192

11000000 10101000 00000001 11000000 192.168.1.192

11111111 11111111 11111111 11000000 255. 255.255. 192

这四个子网的每一个都具有不允许使用的两个地址。以十进制表示，它们是:

子网 192.168.1.0 禁止 192.168.1.0 和 192.168.1.63

子网 192.168.1.64 禁止 192.168.1.64 和 192.168.1.127

子网 192.168.1.128 禁止 192.168.1.128 和 192.168.1.191

子网 192.168.1.192 禁止 192.168.1.192 和 192.168.1.255

二进制重组:

11000000 10101000 00000001 00000000 192.168.1.0

11111111 11111111 11111111 11000000 255.255.255.192

11000000 10101000 00000001 00111111 192.168.1.63

11111111 11111111 11111111 11000000 255.255.255.192

11000000 10101000 00000001 01000000 192.168.1.64
11111111 11111111 11111111 11000000 255.255.255.192
11000000 10101000 00000001 01111111 192.168.1.127
11111111 11111111 11111111 11000000 255.255.255.192

11000000 10101000 00000001 10000000 192.168.1.128
11111111 11111111 11111111 11000000 255.255.255.192
11000000 10101000 00000001 10111111 192.168.1.191
11111111 11111111 11111111 11000000 255.255.255.192

11000000 10101000 00000001 11000000 192.168.1.192
11111111 11111111 11111111 11000000 255.255.255.192
11000000 10101000 00000001 11111111 192.168.1.255
11111111 11111111 11111111 11000000 255.255.255.192

这时能够将这64个地址子网其中之一分为两个部分，接收32个地址的两个子网，但其中的每个包含两个禁止的地址:

11000000 10101000 00000001 11000000 192.168.1.192
11111111 11111111 11111111 11100000 255.255.255.224
11000000 10101000 00000001 11011111 192.168.1.223
11111111 11111111 11111111 11100000 255.255.255.224

11000000 10101000 00000001 11100000 192.168.1.224
11111111 11111111 11111111 11100000 255.255.255.224
11000000 10101000 00000001 11111111 192.168.1.255
11111111 11111111 11111111 11100000 255. 255.255. 224

在宽带网络中，32 个地址对于单个家庭是过量的。连接到子网的每台计算机被认为具有一个地址，它也包含缺省网关路由器，需要至少两个地址用于每个家庭，一个用于计算机以及一个用于路由器。如果此家庭由一台以上计算机控制，则需要更大的子网。

因此，每个家庭两个地址要求最小的子网必需具有四个地址的范

围。二进制:

11000000 10101000 00000001 10000000 192.168.1.0

11111111 11111111 11111111 11111100 255.255.255.252

由于两个地址被禁止:

11000000 10101000 00000001 00000000 192.168.1.0

11111111 11111111 11111111 11111100 255.255.255.252

11000000 10101000 00000001 00000011 192.168.1.3

11111111 11111111 11111111 11111100 255.255.255.252

保留使用的地址为 192.168.1.1 和 192.168.1.2。在下一个子网中，地址 192.168.1.4 和 192.168.1.7 被禁用。可使用的地址为 192.168.1.5 和 192.168.1.6 等等。

在自开始的 256 个地址中，有 256/4 = 64 个子网或 64 个客户。这些种类的小子网中的地址的一半被保留作为广播地址及网址，以及地址空间的损失为 50%。

如果在更大范围内设计子网，则地址空间的损失因广播地址和网址而减少(每个子网 8 个地址提供 256/8 = 32 个子网，25% 的地址空间损失)。但每个子网有 6 个有用地址，如果为路由器提供一个，则每个家庭有 5 个地址。如果那 5 个地址没有完全被使用，则由于每个家庭中没有两台以上计算机，因此仍然存在地址损失，因为 3 个地址未被使用。

通过根据本发明的一个实施例的解决方案，使得能够使用子网中提供的 256 个地址其中的 254 个，并将它遍布若干房屋和多个 ASR，从而覆盖更多客户。如果一个客户的计算机比另一个客户要多，则没有引起额外的地址空间损失，因为有更多数量的计算机的客户接收更多地址。因此，如果网络构建成优化地址空间，则采用本发明的地址空间的损失保持在几个百分点。

根据本发明，应用一种过滤器，除了其中的协议选项表明第 2 层数据包中携带的数据为 IP、Ipv6 或通信目的可接受的任何业务之外，

它阻止属于 VLAN 的端口之间的其它第 2 层业务。这意味着，即使这些端口属于相同的第 2 层广播域，但根据它们的源和目标第 2 层地址来防止它们之间的业务被交换。

当连接到端口的客户机开始传送时，第一数据包将经过 Ethernet®段，其中包括 ASR。

每当客户机主机设法与另一个主机进行通信时，它将在目的地不是客户机主机的 IP 子网的一部分时发出缺省路由的 ARP 请求，或者在其目标地址处于客户机主机相同子网中时发出目的地自身。这个 ARP 请求为第 2 层广播，它通常经过整个 VLAN。根据本发明，ARP 消息由 ASR 截取，并被阻止转发给属于那个 VLAN 的任何其它端口。如果 ARP 请求针对 ASR 的任何其它端口中存在的目的地，或者如果已知目的地处于 ASR 第 3 层路由选择表中，则 ASR 采用其自身的 MAC 地址作为下一跳来响应 ARP 请求。这个过程使客户机主机认为（模拟）ASR 第 2 层地址是要用来到达实际第 3 层目的地的目标第 2 层地址。因此，客户机主机将数据包传送给 ASR 第 2 层地址。

如果根据目标第 3 层地址和 ASR 路由选择表和/或地址解析表的内容确定该数据包将被转发到 ASR 端口的另一个，则该数据包的源 MAC 地址被改变为出口端上的 ASR 第 2 层地址。源 IP 地址将继续是原始客户机主机地址中的地址。因此，ASR 中的接收机记住/了解，源客户机主机地址映射到 ASR 第 2 层地址，以及任何对源客户机主机的返回业务被导向 ASR 而不是直接送往源客户机 MAC 地址。这样，源以及目标客户机主机被模拟成认为 ASR MAC 地址是另外主机的地址，以及通信流被保持。

为了能够采用 TCP/IP 进行通信，主机必需配置：

- IP 地址
- 子网掩码
- 缺省网关
- 名称服务器

名称服务器用于在名称与因特网中的IP地址之间进行连接。

图1示意说明连接到根据先有技术的宽带网络10的住宅区。在交换12，示出具有连接到其中的所有端口14的VLAN，意味着邻居们在他们之间有第2层访问。这使一个邻居能够例如游览另一个邻居的硬盘驱动器。交换机16包括属于不同的VLAN的每个端口14，它要求每个VLAN较小的IP子网。这是地址空间的浪费，因为每个子网对网络和广播功能引起不可用的地址。具有两个可用地址的子网还要求两个不可用的地址，浪费50%的地址空间。图1中的装置18为路由器。

图2示意性示出连接在根据先有技术的两个宽带网络32、34之间的网关30，另外还示出主机A、主机B和主机C。

以下序列描述ARP路由选择协议的传统操作。

步骤1)-9)的第一序列提供一个实例，其中，主机A向主机B进行传送，参照图2:

1) 主机A具有要发送的IP数据包

2) 主机A将主机A地址+子网掩码与主机B地址进行比较

3) 主机B与主机A处于同一个网络

4) 主机A向网络1发送ARP广播，请求主机B第2层地址

5) 主机B识别对其第2层地址的请求

6) 主机B进行响应

7) 主机A这时具有主机B第2层地址

8) 主机A传送数据

9) 主机B接收数据

步骤1)-17)的第二序列提供一个实例，其中，主机A向主机C进行传送，参照图2:

1) 主机A具有要发送的IP数据包

2) 主机A将主机A地址+子网掩码与主机C地址进行比较

3) 主机C与主机A不在同一个网络

4) 主机 A 向网络 1 发送 ARP 广播，请求网关第 2 层地址

5) 网关识别对其第 2 层地址的请求

6) 网关进行响应

7) 主机 A 这时具有网关第 2 层地址

8) 主机 A 传送数据

9) 网关接收数据

10) 网关从数据包中去掉第 2 层信息

11) 网关在路由选择表中查找主机 C 地址，并确定出口接口

12) 网关向网络 2 发送 ARP 广播，请求主机 C 第 2 层地址

13) 主机 C 识别对其第 2 层地址的请求

14) 主机 C 进行响应

15) 网关这时具有主机 C 第 2 层地址

16) 网关构建数据包的新的第 2 层首标并传送数据

17) 主机 C 接收数据

如果网关 30 没有直接连接到网络 2，则步骤 12 将是“把数据包转发到网络 2”，在沿路径的每个网关中重复步骤 9、10、11 和新的步骤 12，直至直接连接到网络 2 的网关接收数据包为止，其中将开始根据上述流程的步骤 12-17。

图 3 示意说明根据本发明的宽带网络 40，其中具有两个 ASR 路由器 42、44。主机 A 和主机 B 连接到路由器 42，以及主机 C 连接到路由器 44。两个路由器 42 和 44 彼此之间具有直接连接，其中路由器 42 包括本发明的过滤器。图 3 还说明经由因特网连接到宽带网络的主机 D。

本发明的过滤器被提供用于在宽带网络 40 的至少一个 ASR 路由器 42 中的开放式系统互连第 2 层业务分隔。路由器 42、44 中的 A1 端口(未示出)配置到同一个 VLAN。ASR 44 是对路由器 42 的子路由器或者只是被连接，提供根据本发明的相同过滤优点。数据包业务由包括过滤器的路由器 42 截取，它过滤送往端口的数据包业务。过滤

器包括:

用于截取来自属于虚拟局域网的 MAC 地址的网络连接源装置(主机 A,主机 B)的第 2 层业务并确定是否准许业务被转发到其它端口的部件;

用于不管目标装置第 2 层域是否与源装置第 2 层域相同、响应对源装置的广播而截取这种业务中的地址解析协议广播的部件,因而源装置确定广播已经确认所寻找的目标装置的第 2 层地址,从而源装置将数据包传送给目标装置,路由器接收所传送的数据包;

用于确定到目标装置的出口端的部件;

用于确定目标装置的第 2 层地址的部件;

用于从所接收数据包调整第 2 层首标的部件,该部件用于设置源第 2 层地址,设置数据包的路由器源地址,该部件用于确定目标装置的第 2 层地址,将目标第 2 层地址设置到目标装置的地址,将数据包传送给目标装置。

因此,本发明的过滤器进行模拟,如果源装置和目标装置处于相同的第 2 层域,则路由器第 2 层地址为源以及目标两种装置的实际目标地址,或者进行模拟,如果源装置和目标装置不在相同的第 2 层域但在相同的第 3 层子网,则路由器第 2 层地址为源对目的地的实际目标第 2 层地址。

大家知道,本发明的部件最好是路由器中的软件构建块或者是硬件和软件的组合。

下面根据本发明并参照图 3 提供数据包流程的三种情况。

要注意,在 IP 路由选择中,IP 数据包中第 2 层首标的封装和拆封是一种传统过程。具有 IP 源和目标地址的 IP 首标保持不变,而用于以太网、令牌环、帧中继、ATM 或其它所使用的第 2 层技术的第 2 层首标发生变化。由于第 2 层协议不是可路由的,因此源地址始终设置为传送数据包的装置的地址。这是传统的。

具有序列步骤 1)至 3)的第一种情况描述从主机 A 到主机 B 的数

据包传送。两个主机均连接到同一个 ASR 中的端口。这些端口配置成属于相同的广播域(VLAN)，但根据本发明，在 ASR 上启用了具有附加功能的端口保护。

第一种情况

1) 主机 A 具有要发送的 IP 数据包

2) 主机 A 将它的地址 + 子网掩码与主机 B 进行比较，并确定它们在同一个子网中

3) 主机 A 发送 ARP 广播以便获得主机 B 地址

4) 由于 ASR 42 端口之间的过滤器的原因，广播无法到达主机 B

5) ASR 截取 ARP 广播，并确定它知道主机 B 所处的位置

6) ASR 响应对于主机 B 的 ARP 请求，将它自身的第 2 层地址设置为主机 B 的地址

7) 主机 A 接收 ARP 响应，并认为它这时知道主机 B 的第 2 层地址

8) 主机 A 传送数据

9) ASR 42 接收数据

10) ASR 42 删除第 2 层信息，并确定对于主机 B 的出口端

11) ASR 42 将它自身的第 2 层地址设置为数据包的源，并封装用于主机 B 的数据包

12) ASR 42 传送数据

13) 主机 B 接收来自主机 A 的数据

由于 ASR 42 第 2 层地址设置为源，因此主机 B 认为 ASR 42 的第 2 层地址是主机 A 的地址。同样，由于 ARP 响应，因此主机 A 将认为 ARS 42 的第 2 层地址是主机 B 的地址。

具有序列步骤 1)至 18)的第二种情况描述从主机 A 到主机 C 的数据包传送。这些主机均连接到不同的 ASR 中的端口。但是，ASR 和中央管理系统的地址共享特征同意主机根据 DHCP 从相同的 IP 子网

接收 IP 地址。ASR 已经交换了相互通知关于已连接主机的路由选择信息。

第二种情况

1) 主机 A 具有要发送的 IP 数据包

2) 主机 A 将它的地址 + 子网掩码与主机 C 进行比较，并确定它们在同一个子网中

3) 主机 A 发送 ARP 广播以便获得主机 C 地址

4) 由于 ASR 42 端口之间的过滤器的原因，广播没有到达 ASR 中的任何其它端口

5) ASR 42 截取 ARP 广播，并确定它知道主机 C 所处的位置

6) ASR 42 响应对于主机 C 的 ARP 请求，将它自身的第 2 层地址设置为主机 C 的地址

7) 主机 A 接收 ARP 响应，并认为它这时知道主机 C 的第 2 层地址

8) 主机 A 传送数据包

9) ASR 42 接收数据包

10) ASR 42 删除第 2 层信息，并确定对于主机 C 的出口端

11) ASR 42 采用适当的第 2 层首标封装数据包，用于到 ASR 44 的链路

12) ASR 42 将数据包转发给 ASR 44

13) ASR 44 接收数据包

14) ASR 44 删除来自 ASR 42、在链路上使用的第 2 层封装

15) ASR 44 确定送往主机 C 的数据包的出口端

16) ASR 44 采用第 2 层首标封装数据包，将它自身的第 2 层地址设置为源

17) ASR 44 传送数据

18) 主机 C 接收来自主机 A 的数据

由于 ARP 42 对 ARP 请求的响应，因此主机 A 将认为 ARS 42 的第 2 层地址是主机 C 的地址，由于 ASR 44 在上述最后的步骤中将它自身的第 2 层地址设置为送往主机 C 的数据包的源，因此主机 C 认为 ASR 44 的第 2 层地址是主机 A 的地址。

具有序列步骤 1)至 15)的第三种情况描述从主机 A 到主机 D 的数据包传送。主机 A 连接到 ASR 42 中的端口。主机 D 连接到因特网的某个位置。

第三种情况

1) 主机 A 具有要发送的 IP 数据包

2) 主机 A 将它的地址 + 子网掩码与主机 D 进行比较，并确定它们不在相同子网中

3) 主机 A 发送 ARP 广播以便获得缺省网关地址

4) 由于 ASR 42 端口之间的过滤器的原因，广播无法到达 ASR 中的任何其它端口

5) ASR 截取 ARP 广播，并确定它是缺省网关

6) ASR 用它自身的第 2 层地址来响应对于缺省网关的 ARP 请求

7) 主机 A 接收 ARP 响应，并认为它这时知道缺省网关的第 2 层地址

8) 主机 A 传送数据

9) ASR 42 接收数据

10) ASR 42 删除第 2 层信息，并确定对于主机 D 的出口端

11) ASR 42 采用适当的第 2 层首标封装数据包，用于到主机 D 的链路

12) 沿 ASR 42 与主机 D 之间的路径的网关重复步骤 9-11。

13) 连接主机 D 的网关接收数据包

14) 网关执行 ARP 查找，并根据因特网标准将数据包转发到主机 D

15) 主机 D 接收数据

已经通过不是用于限制本发明的范围的实例及实施例描述了本发明，从而本领域的技术人员能够根据所附权利要求集来得出其它实施例。

5

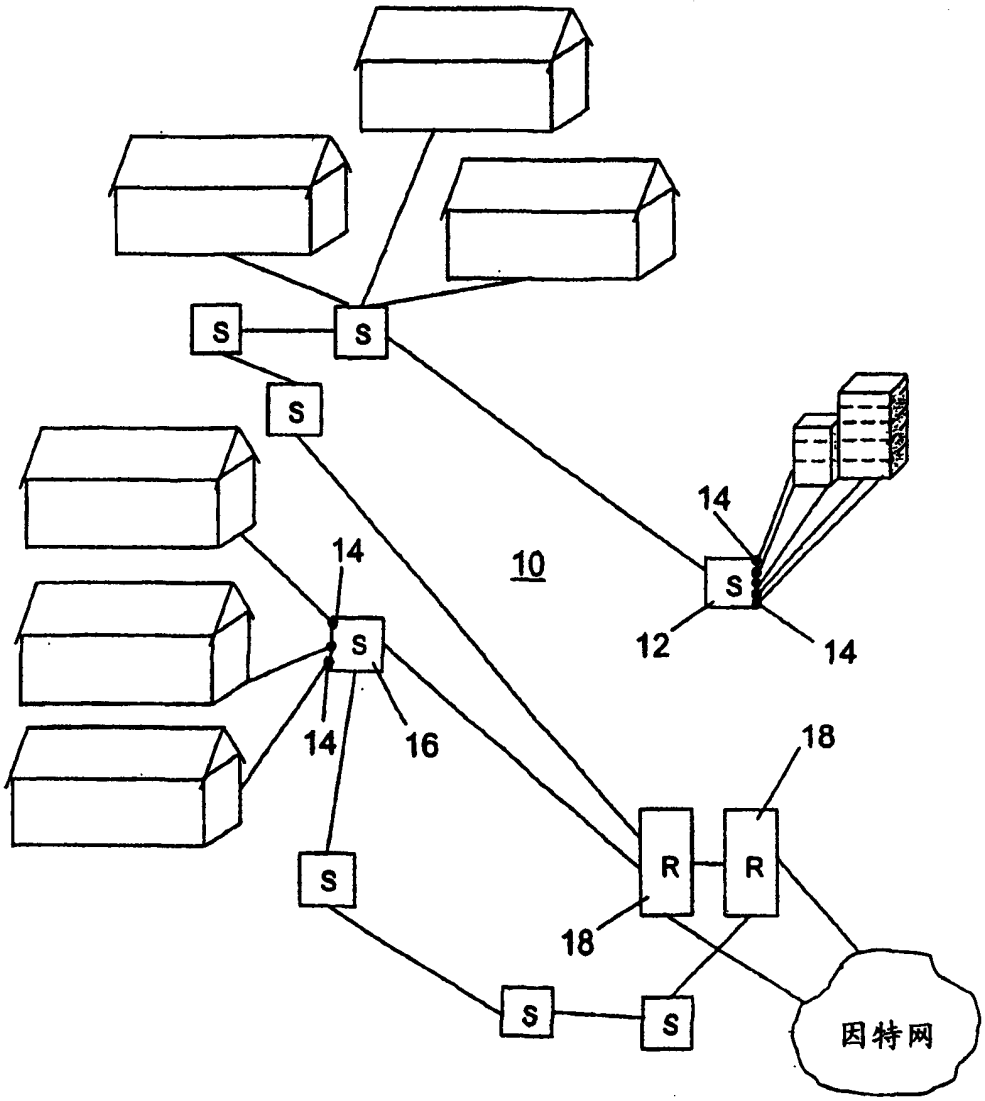
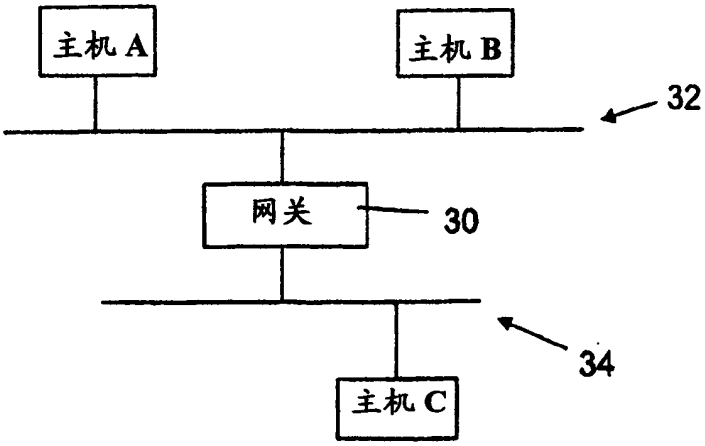


图 1

图 2



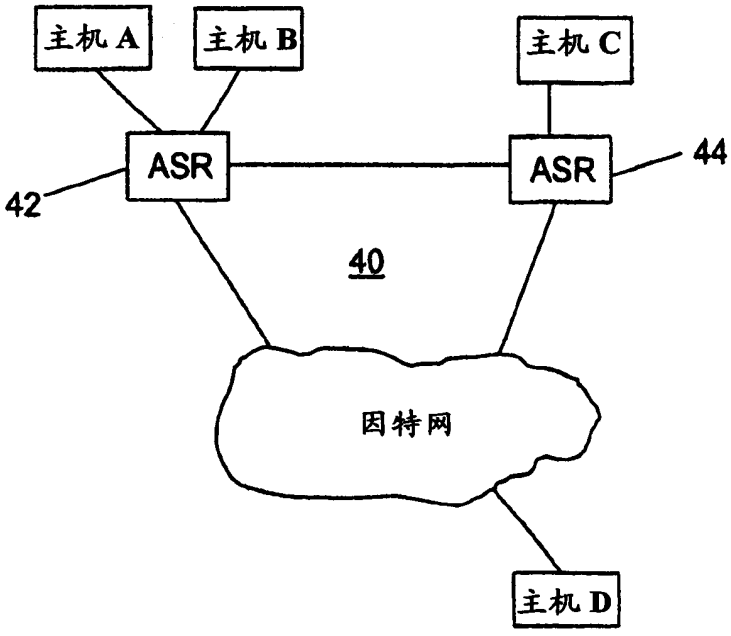


图 3