



# [12] 发明专利说明书

[21] ZL 专利号 02103924.0

[45] 授权公告日 2004 年 12 月 22 日

[11] 授权公告号 CN 1181645C

[22] 申请日 2002.2.7 [21] 申请号 02103924.0

[71] 专利权人 华为技术有限公司

地址 517057 广东省深圳市科技园科发路华为用户服务中心大厦知识产权部

[72] 发明人 宋强 万斌 周和秘 刘伟

审查员 刘欣科

[74] 专利代理机构 北京集佳知识产权代理有限公司

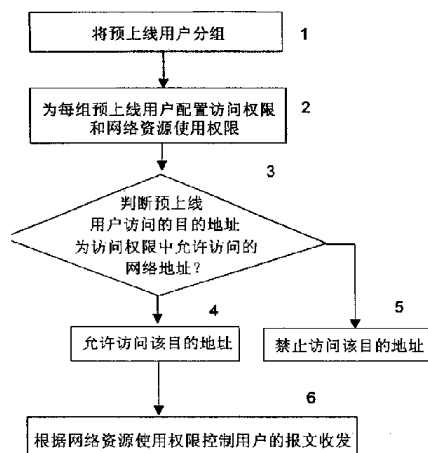
代理人 逯长明

权利要求书 2 页 说明书 5 页 附图 1 页

[54] 发明名称 预上线用户访问网络的控制方法

[57] 摘要

本发明涉及一种预上线用户访问网络的控制方法。该方法包括：首先将未通过网络认证的预上线用户根据其连接于网络中的网络标识进行分组；然后分别为每组预上线用户配置访问权限和网络资源使用权限；这样，预上线用户访问网络时，便可根据其所在的预上线用户组的访问权限和网络资源使用权限确定该预上线用户对网络资源的使用情况。本发明可对预上线的用户访问权限和网络资源使用权限进行分别配置，从而方便网络服务提供商根据市场的需要将不同的访问权限和网络资源使用权限配置给不同的预上线用户，使网络服务提供商可以更自如地根据需要对预上线用户的访问权限和网络资源使用权限进行有效地管理控制。



1、一种预上线用户访问网络的控制方法，包括：

(1) 将预上线用户根据其连接于网络中的网络标识进行分组，预上线用户为未通过网络认证的上网用户；

(2) 分别为每组预上线用户配置访问权限，访问权限用于描述网络地址的可访问性；

(3) 根据每组预上线用户的访问权限判断预上线用户访问的目的地址是否为可访问的网络地址，如果是可访问的网络地址，则允许该用户访问该目的地址，否则，禁止该用户访问该目的地址。

2、根据权利要求1所述的预上线用户访问网络的控制方法，其特征在于所述用户的网络标识是指用户访问网络时所处于的网络中的网络标识，该网络标识为虚拟网络标识VLAN ID。

3、根据权利要求1所述的预上线用户访问网络的控制方法，其特征在于所述的用户的网络标识是指用户连接于网络中所使用的端口信息。

4、根据权利要求1所述的预上线用户访问网络的控制方法，其特征在于所述的访问权限采用访问控制列表进行描述，访问控制列表中包含多个访问组，每个访问组中包括多个网段的访问控制的配置，为每个预上线用户组分配一个访问组。

5、根据权利要求1所述的预上线用户访问网络的控制方法，其特征在于所述的访问权限中定义有预上线用户组间及预上线用户组内部用户之间的互访权限。

6、根据权利要求1所述的预上线用户访问网络的控制方法，其特征在于所述的步骤（2）还包括：为每组预上线用户配置网络资源使用权限，网络资源使用权限包括网络报文收发的流速大小、优先级高低。

## 预上线用户访问网络的控制方法

### 技术领域

本发明涉及一种网络访问权限控制技术，尤其涉及一种预上线用户访问网络的控制方法。

### 背景技术

在网络服务中，上网用户未通过网络服务认证前为处于预上线阶段的用户，即为预上线用户，网络服务提供商对预上线用户的访问权限需要有所控制，以适应自己的经营管理需要。现有技术的解决方案是：一种为禁止预上线用户做任何访问，仅允许访问一个主机地址或其所在的一个网段；另一种为允许预上线用户做任何访问。上述两种解决方案对预上线用户的访问权限配置比较死板；如采用第一种方案，则对预上线用户限制过多，不利于网络服务提供商开展业务；如采用第二种方案，则预上线用户的访问权限过宽，影响了网络服务提供商的利益。因此，现有技术决定网络服务提供商无法根据市场需求针对不同的预上线用户分别配置不同的访问权限。另外，对于预上线用户的网络资源使用权限，如流速大小和优先级等，的配置也是全局一致的，不能对不同的预上线用户区别对待。

### 发明内容

本发明的目的是提供一种预上线用户访问网络的控制方法，使网络服务提供商可针对不同的预上线用户配置不同的访问权限。

本发明的目的是这样实现的：预上线用户访问网络的控制方法，包括：

(1) 将预上线用户根据其连接于网络中的网络标识进行分组，预上线用户为未通过网络认证的上网用户；

(2) 分别为每组预上线用户配置访问权限，访问权限用于描述网络地址的可访问性；

(3) 根据每组预上线用户的访问权限判断预上线用户访问的目的地址是否为可访问的网络地址，如果是可访问的网络地址，则允许用户访问该目的地址，否则，禁止访问该目的地址。

所述用户的网络标识是指用户访问网络时所处于的网络中的网络标识，该网络标识为虚拟网络标识（VLAN ID）。

所述的用户的网络标识是指用户连接于网络中所使用的端口信息。

所述的访问权限采用访问控制列表进行描述，访问控制列表中包含多个访问组，每个访问组中包括多个网段的访问控制的配置，为每个预上线用户组分配一个访问组。

所述的访问权限中定义有预上线用户组间及预上线用户组内部用户之间的互访权限。

所述的步骤（2）还包括：为每组预上线用户配置网络资源使用权限，网络资源使用权限包括网络报文收发的流速大小、优先级高低。

本发明将处于预上线阶段的用户进行分组并分别赋予不同的访问权限和网络资源使用权限，实现了对预上线用户的访问和资源使用权限进行分

别控制,使网络服务提供商可根据市场的需要将不同的访问权限和网络资源使用权限配置给不同的预上线用户,便于网络服务提供商业务工作的开展。同时本发明还可对预上线用户之间的互访权限加以控制,使网络服务提供商可以更自如地根据需要对预上线用户的访问权限进行有效地管理控制。

### 附图说明

图1为预上线用户访问网络的控制方法的流程图;

图2为定义访问权限的访问控制列表。

### 具体实施方式

本发明的具体实施方式叙述如下,参见图1,当用户通过虚拟局域网(VLAN)访问网络时,对预上线用户访问权限的控制方法如下:

步骤1:将处于预上线阶段的用户根据用户连接于网络中所具有的虚拟网络标识(VLAN ID)进行分组,每个VLANID为一组;或者可以扩展应用:将其所处的物理位置和设备位置等构成逻辑端口号,由逻辑端口号和VLAN ID一起作为分组的依据,以下以VLAN ID分组为例;

步骤2:分别为每组预上线用户配置访问权限和网络资源使用权限,同一组预上线用户具有相同的访问权限,访问权限用于描述网络地址的可访问性,网络地址的可访问性是由网络服务提供商根据需要设定的;

网络资源使用权限包括其网络报文收发的流速大小控制,优先级高低等等,为每个预上线用户组分配这些参数即可以控制网络报文收发过程中流速的大小、优先级的高低级别等情况。

访问权限可以用一个访问控制列表进行描述，访问控制列表中包含多个访问组，每个访问组中包括多个网段的访问控制的配置，为每个VLANID分配一个访问组；例如，配置访问控制列表中访问组1可以访问网段(10.11.112.0,255.255.255.0)和(10.11.200.0,255.255.255.0)，不能访问其余的网段；而访问组2只可以访问网段(10.11.112.0,255.255.255.0)，并将VLAN ID=1的用户在预上线阶段配置为访问组1，VLAN ID=2的用户在预上线阶段配置为访问组2，以实现具有不同VLAN ID的预上线用户可以对多个不同的网段具有不同或者相同的访问权限；

步骤3：预上线用户组中的用户进行网络访问时，根据该预上线用户的访问组中的多个网段的访问控制的配置情况，判断该预上线用户所访问的目的地址是否为用户可访问的网络地址，如果为可访问的网络地址，执行步骤4，否则，执行步骤5；

步骤4：允许该用户访问该目的地址，执行步骤6；

步骤5：禁止该用户访问该目的地址，本次预访问过程结束，当用户下一次访问过程到来时，执行步骤3；

步骤6：根据该预上线用户的网络资源使用权限，控制该用户收发报文的流速大小、优先级高低等情况；对于主动访问预上线用户的报文，其流速大小、优先级高低等情况也需要服从为该预上线用户所配置的网络资源使用权限。

所述的将处于预上线阶段的用户分组也可依据用户连接于网络中所使用的端口信息，可将若干个端口上所连接的预上线用户分为一组。

所述的访问权限还可以定义各个预上线用户组之间及预上线用户组内部用户之间的互访权限，如图2所示，图中的g1、g2、g3、g4分别代表一个预上线用户组，P表示允许访问，D表示禁止访问，由图中可以看出：g1与g1的交点处标志为P，表示g1内部用户之间可以互相访问；g2与g2的交点处标志为D，表示g2内部用户之间不允许互相访问；g3与g4的交点处标志为P，表示g3的用户可以访问g4的用户，g4与g3的交点处标志为D，表示g4的用户不允许访问g3的用户，依次类推，这样预上线用户组内部用户之间及不同组之间的互访权限就可以确定在该列表中，依据此列表便可以实现对预上线用户组内部用户之间及不同组之间的互访权限进行控制。



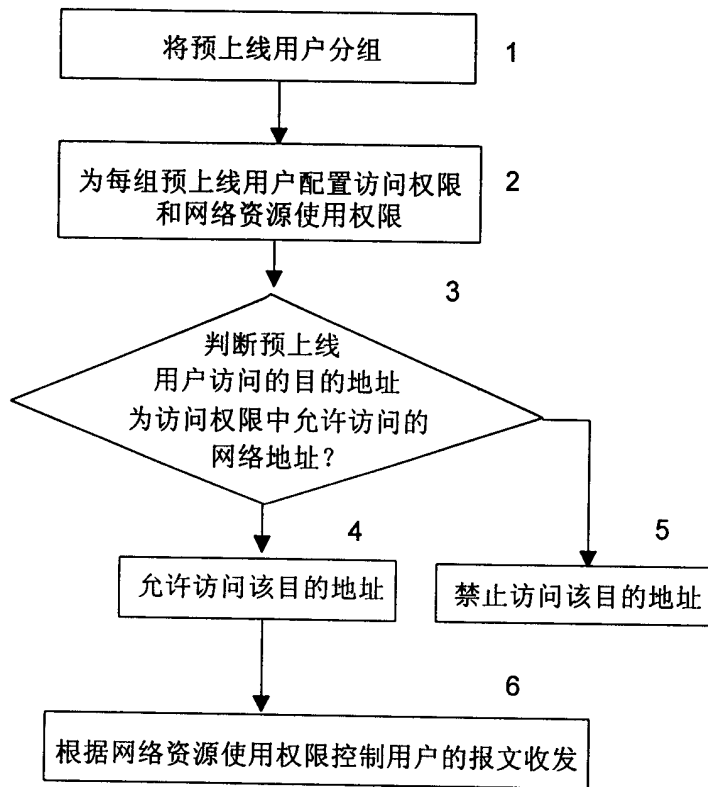


图1

组号	g1	g2	g3	g4
g1	P	P	P	D
g2	D	D	P	P
g3	P	P	D	P
g4	P	D	D	D

图2