

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 29/06 (2006.01)

H04L 12/56 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200510105507.4

[43] 公开日 2007 年 3 月 28 日

[11] 公开号 CN 1937619A

[22] 申请日 2005.9.23

[21] 申请号 200510105507.4

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

[72] 发明人 苗福友

[74] 专利代理机构 北京凯特来知识产权代理有限公司

代理人 郑立明

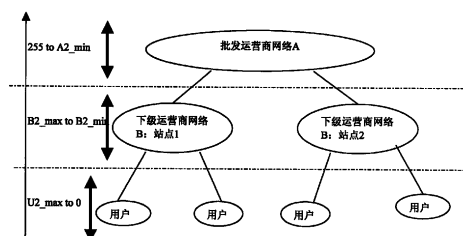
权利要求书 3 页 说明书 11 页 附图 3 页

[54] 发明名称

运营商的运营商情况下生存时间分区安全机制的实现方法

[57] 摘要

本发明提供了一种运营商的运营商情况下生存时间分区安全机制的实现方法，该方法主要包括：在批发运营商网络、下级运营商网络 and 用户网络中分别设置不同的 TPSM (生存时间分区安全机制) 参数；利用所述设置的 TPSM 参数，在批发运营商网络、下级运营商网络中同时实现 TPSM。利用本发明所述方法，可以在 CsC (运营商的运营商) 组网的情况下，在批发运营商网络和下级运营商网络中同时实施 TPSM。



1、一种运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，包括：

A、在批发运营商网络、下级运营商网络 and 用户网络中分别设置不同的生存时间分区安全机制TPSM参数；

B、利用所述设置的TPSM参数，在批发运营商网络、下级运营商网络中同时实现TPSM。

2、根据权利要求1所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的步骤A具体包括：

当下级运营商网络接受来自批发运营商网络中设备发出的报文时，设置批发运营商网络使用的生存时间TTL的取值范围为： $A1_min \leq TTL \leq 255$ ，其中A1_min为批发运营商网络的TTL允许的最小值；

设置下级运营商网络使用的TTL的取值范围为： $B1_min \leq TTL \leq 255$ ，其中B1_min为下级运营商网络的TTL允许的最小值，B1_min小于A1_min；

设置用户网络使用的TTL的取值范围为： $0 < TTL \leq U1_max$ ，其中U1_max为用户网络允许的TTL最大值，U1_max小于B1_min。

3、根据权利要求1所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的步骤A具体包括：

当下级运营商网络不接受来自批发运营商网络中设备发出的报文时，设置批发运营商网络使用的TTL的取值范围为： $A2_min \leq TTL \leq 255$ ，其中A2_min为批发运营商网络的TTL允许的最小值；

设置下级运营商网络使用的TTL的取值范围为： $B2_min \leq TTL \leq B2_max$ ，其中B2_max为下级运营商网络的TTL允许的最大值，B2_min为下级运营商网络的TTL允许的最小值，B2_max小于

A2_min;

设置用户网络使用的TTL的取值范围为： $0 < TTL \leq U2_max$ ，其中U2_max为用户网络允许的TTL最大值，U2_max小于B2_min。

4、根据权利要求2所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的步骤B具体包括：

批发运营商网络的边缘路由器PE检查每个进入批发运营商网络的报文，当该PE接收到目的地址不是自己的TTL大于A1_min的报文，则将该报文的TTL减少为B1_max，然后，将报文进行转发。

5、根据权利要求4所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的步骤B还包括：

设置批发运营商网络中的设备发出的报文的TTL初始值为255，当批发运营商网络中的设备收到目的地址是自己的报文，如果该报文的TTL不大于A1_min，则将该报文丢弃；否则，将报文转交上层协议进行处理。

6、根据权利要求5所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的步骤B还包括：

下级运营商网络的PE检查每个进入下级运营商网络的报文，当连接用户网络的PE接收到目的地址不是自己的TTL大于B1_min的报文，则将该报文的TTL减少为U1_max，然后，将报文进行转发，当连接批发运营商网络的PE接收到目的地址不是自己的报文，则将报文进行转发。

7、根据权利要求6所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的步骤B还包括：

设置下级运营商网络中的设备发出的报文的TTL初始值为255，当下级运营商网络中的设备收到目的地址是自己的报文，如果该报文的TTL不大于B1_min，则将该报文丢弃；否则，将报文转交上层协议进行处理。

8、根据权利要求3所述运营商的运营商情况下生存时间分区安全机制的

实现方法，其特征在于，所述的步骤B具体包括：

批发运营商网络的PE检查每个进入批发运营商网络的报文，如果该PE接收到目的地址不是自己的TTL大于A2_min的报文，则将该报文的TTL减少为B2_max，然后，将报文进行转发。

9、根据权利要求8所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的步骤B还包括：

设置批发运营商网络中的设备发出的报文的TTL初始值为255，当批发运营商网络中的设备收到目的地址是自己的报文，如果该报文的TTL不大于A2_min，则将该报文丢弃；否则，将报文转交上层协议进行处理。

10、根据权利要求9所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的步骤B还包括：

下级运营商网络的PE检查每个进入下级运营商网络的报文，当连接用户网络的PE接收到目的地址不是自己的TTL大于B2_min的报文，则将该报文的TTL减少为U2_max，然后，将报文进行转发，当连接批发运营商网络的PE接收到目的地址不是自己的TTL大于B2_max的报文，则将该报文丢弃。

11、根据权利要求10所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的步骤B还包括：

设置下级运营商网络中的设备发出的报文的TTL初始值为B2_max，当下级运营商网络中的设备收到目的地址是自己的报文，如果该报文的TTL不大于B2_min，则将该报文丢弃；否则，将报文转交上层协议进行处理。

12、根据权利要求1所述运营商的运营商情况下生存时间分区安全机制的实现方法，其特征在于，所述的方法适用于IPv4网络或IPv6网络。

运营商的运营商情况下生存时间分区安全机制的实现方法

技术领域

本发明涉及网络通讯领域，尤其涉及一种运营商的运营商情况下生存时间分区安全机制的实现方法。

背景技术

为了防止IP网络中因为转发环路的存在，而造成报文在环路中不断转发，从而耗费大量资源的情况。在IPv4（因特网协议版本4）报文头中设置了一个TTL（生存时间）字段，在IPv6报文头中设置了一个Hop Limit（跳限制）字段，该两个字段的长度、作用和处理完全相同，下面我们介绍一下TTL字段的处理过程。

当一台主机在创建一个IPv4报文的时候，便给该报文的TTL字段分配一个初始值，该初始值为0到255之间的一个数值，一般在Linux（一种免费的操作系统）上该初始值缺省为64，而在Windows（一种微软公司的操作系统）上该初始值缺省为128。当一个路由器收到一个上述IPv4报文时，在转发该报文之前先检查该报文的TTL字段的值，如果该TTL字段的值=0，则丢弃该报文，否则将该报文的TTL字段的值减少1，然后转发该报文。这样，如果网络中如果存在转发环路，则报文在环路中最终会因为TTL减少到0而被丢弃，而不会不停止地在环路中转发。

在现有技术中有一些安全机制利用上述TTL的特点来保护网络或网络节点。比如，RFC3286介绍的GTSM（通用的TTL安全机制）。下面我们以后IGP（域内路由协议）协议为例来说明GTSM。

网络邻居之间称为对等体，IGP协议交互只发生在网络邻居之间，因此，IGP协议只接受来自于网络邻居的IGP路由协议报文，而来自于其他节点的IGP路由报文则认定是仿冒的，可以不进行处理。为了实现这个功能，就需要路由器能够判断一个报文是来自于网络邻居，还是来自于其他节点。于是，GTSM中规定网络邻居之间的IGP路由协议报文的TTL初始值必须是255，因此，网络邻居之间的IGP路由协议报文抵达目的路由器（即邻居）的时候，TTL的值必然为255，如果不是的话，则断定该报文并不是来自于一个网络邻居，可以直接丢弃该报文。

对GTSM的一种扩展是：定义一个TrustRadius（信任半径），该信任半径是能够信任的设备距离自己的最大跳数，通过TTL来判断一个报文是否来自于信任半径之内。

上述GTSM方案的缺点为：其使用范围受到很大限制。如果将TrustRadius限定为1，即只接受来自邻居的报文，则该安全机制只能用于象IGP这样的协议，而不能应用到更广泛的场景中去，比如BGP协议（边界网关协议）。如果将TrustRadius限定为一个比较大的值，则增大了安全风险，同时任何确定TrustRadius的值也很困难，给网络配置带来很大的挑战。另外，由于处于网络边界的设备或临近边界的设备的TrustRadius的值必须设置为比较小，因此，限制了该安全机制的适用范围。

现有技术中另一种利用TTL分段实现骨干网络安全保护的方法为TPSM（TTL Partition Security Mechanism，TTL分区安全机制）方法。

在TPSM方法中规定骨干网络设备不需要同用户直接进行交互，它对来自于用户的报文只需要转发，而不需要由IP层以上的协议进行处理，如果报文来自用户，并且报文的地址是该骨干网络设备的地址，则该骨干网络设备可以直接丢弃该报文。

在TPSM方法中，将网络分为运营商网络和客户网络，其中运营商网络由P（运营商的核心路由器）和PE（运营商网络边缘路由器）两种设备组成，PE直接连接客户的网络（如企业网）或者通过二层网络同用户的网络或主机，如ADSL（不对称数字用户线）相连，P设备是运营商网络的骨干设备，负责将PE路由器连接起来。

TPSM将TTL分为高低两个段，其中高段部分（255到255-TrustRadius）分配给运营商骨干网使用，骨干网的PE和P设备之间的通信的TTL只能是在这个范围之内，并且要求骨干网内的通信报文的TTL初始值都设为255。如果一个P或PE路由器发现一个目的地址为自己的TTL小于255-TrustRadius的报文，则认为该报文来自客户网络，则可以直接丢弃该报文；如果报文的TTL大于255-TrustRadius，则进行相应的处理。

来自一个客户网络的报文的TTL可能也大于255-TrustRadius，这样骨干网的P路由器就可能错误地接受这个报文。为了避免这种情况，需要在骨干网的边缘，也就是PE设备上将骨干网的TTL减少到一个比255-trustRadius还要小的一个值（TTL_USER_MAX），这个值一般是大于128（考虑到Windows的TTL缺省值为128，而Linux为64，所以将报文的TTL减少到TTL_USER_MAX的情况的发生概率是非常低的，因此对网络的影响也能够降到一个比较低的水平）。

上述TPSM方法的缺点为：该方法将网络分为客户网络和运营商网络，并且把运营商网络作为一个整体，实际上为一个客户提供服务的网络可能涉及到很多运营商网络，这些运营商网络之间有各种不同的关系，尤其是一个运营商网络可能为另一个运营商网络提供骨干网络连接，这样，第二个运营商网络对于它的客户来说是运营商，而对于为它提供骨干网络连接的运营商网络来说是客户。这种情况一般称为CsC（Carrier's Carrier，运营商的运营

商)，CsC中将提供VPN（虚拟专用网）业务的运营商称为批发运营商，而将使用批发业务的运营商称为下级运营商。CsC的组网示意图如图1所示。

在图1所示的组网中，在批发运营商网络A中可以单独实施上述TPSM方法。并且不会对本身网络产生不利的影响。

如果在图1所示的组网中，在下级运营商中单独实施TPSM，比如，在下级运营商网络B中单独实施TPSM，则网络B必须决定将批发运营商网络A作为客户网络还是仅仅作为是P设备。如果将A只当作客户网络，则TPSM只能在网络B中的每个场所中单独实施，不同场所内的设备无法直接通信，这是无法接受的；如果将A仅仅作为P设备，就需要在网络A中的P设备实施同网络B中的P设备相同的报文TTL处理规则，而这在实现上基本是不可能的，因为一个批发运营商网络可能同时为多个下级运营商提供批发业务，而各个下级运营商可能有的实现了TPSM，也可能没有，即使实现了参数可能也不完全相同，因此，在下级运营商网络中单独实施TPSM，而在批发运营商网络上不实施TPSM，TPSM正常工作是非常困难的，甚至是不可能的。

如果在图1所示的组网中，在批发运营商网络和下级运营商网络中同时实施TPSM，则必须正确地进行各种参数的设置，否则，将引起混乱，在现有技术当中，还没有在批发运营商网络和下级运营商网络中同时实施TPSM的具体方案。

发明内容

本发明的目的是提供一种运营商的运营商情况下生存时间分区安全机制的实现方法，从而可以在CsC组网的情况下，在批发运营商网络和下级运营商网络中同时实施TPSM。

本发明的目的是通过以下技术方案实现的：

一种运营商的运营商情况下生存时间分区安全机制的实现方法，包括：

A、在批发运营商网络、下级运营商网络 and 用户网络中分别设置不同的生存时间分区安全机制TPSM参数；

B、利用所述设置的TPSM参数，在批发运营商网络、下级运营商网络中同时实现TPSM。

所述的步骤A具体包括：

当下级运营商网络接受来自批发运营商网络中设备发出的报文时，设置批发运营商网络使用的生存时间TTL的取值范围为： $A1_min \leq TTL \leq 255$ ，其中A1_min为批发运营商网络的TTL允许的最小值；

设置下级运营商网络使用的TTL的取值范围为： $B1_min \leq TTL \leq 255$ ，其中B1_min为下级运营商网络的TTL允许的最小值，B1_min小于A1_min；

设置用户网络使用的TTL的取值范围为： $0 < TTL \leq U1_max$ ，其中U1_max为用户网络允许的TTL最大值，U1_max小于B1_min。

所述的步骤A具体包括：

当下级运营商网络不接受来自批发运营商网络中设备发出的报文时，设置批发运营商网络使用的TTL的取值范围为： $A2_min \leq TTL \leq 255$ ，其中A2_min为批发运营商网络的TTL允许的最小值；

设置下级运营商网络使用的TTL的取值范围为： $B2_min \leq TTL \leq B2_max$ ，其中B2_max为下级运营商网络的TTL允许的最大值，B2_min为下级运营商网络的TTL允许的最小值，B2_max小于A2_min；

设置用户网络使用的TTL的取值范围为： $0 < TTL \leq U2_max$ ，其中U2_max为用户网络允许的TTL最大值，U2_max小于B2_min。

所述的步骤B具体包括：

批发运营商网络的边缘路由器PE检查每个进入批发运营商网络的报文，

当该PE接收到目的地址不是自己的TTL大于A1_min的报文，则将该报文的TTL减少为B1_max，然后，将报文进行转发。

所述的步骤B还包括：

设置批发运营商网络中的设备发出的报文的TTL初始值为255，当批发运营商网络中的设备收到目的地址是自己的报文，如果该报文的TTL不大于A1_min，则将该报文丢弃；否则，将报文转交上层协议进行处理。

所述的步骤B还包括：

下级运营商网络的PE检查每个进入下级运营商网络的报文，当连接用户网络的PE接收到目的地址不是自己的TTL大于B1_min的报文，则将该报文的TTL减少为U1_max，然后，将报文进行转发，当连接批发运营商网络的PE接收到目的地址不是自己的报文，则将该报文进行转发。

所述的步骤B还包括：

设置下级运营商网络中的设备发出的报文的TTL初始值为255，当下级运营商网络中的设备收到目的地址是自己的报文，如果该报文的TTL不大于B1_min，则将该报文丢弃；否则，将报文转交上层协议进行处理。

所述的步骤B具体包括：

批发运营商网络的PE检查每个进入批发运营商网络的报文，如果该PE接收到目的地址不是自己的TTL大于A2_min的报文，则将该报文的TTL减少为B2_max，然后，将报文进行转发。

所述的步骤B还包括：

设置批发运营商网络中的设备发出的报文的TTL初始值为255，当批发运营商网络中的设备收到目的地址是自己的报文，如果该报文的TTL不大于A2_min，则将该报文丢弃；否则，将报文转交上层协议进行处理。

所述的步骤B还包括：

下级运营商网络的PE检查每个进入下级运营商网络的报文，当连接用户

网络的PE接收到目的地址不是自己的TTL大于B2_min的报文，则将该报文的TTL减少为U2_max，然后，将报文进行转发，当连接批发运营商网络的PE接收到目的地址不是自己的TTL大于B2_max的报文，则将该报文丢弃。

所述的步骤B还包括：

设置下级运营商网络中的设备发出的报文的TTL初始值为B2_max，当下级运营商网络中的设备收到目的地址是自己的报文，如果该报文的TTL不大于B2_min，则将该报文丢弃；否则，将报文转交上层协议进行处理。

所述的方法适用于IPv4网络或IPv6网络。

由上述本发明提供的技术方案可以看出，本发明通过对现有的TPSM方案进行改进，从而可以在CsC组网的情况下，根据实际组成网络的不同要求，设置不同的TPSM参数，在批发运营商网络和下级运营商网络中同时实施TPSM，为批发运营商网络和下级运营商网络同时提供安全保护机制。

附图说明

图1为CsC的组网示意图；

图2为本发明所述方法的具体处理流程图；

图3为下级运营商接受来自批发运营商的网络中设备发出的报文的情况下，在批发运营商网络、下级运营商网络 and 用户网络中设置TPSM参数的示意图；

图4为下级运营商不接受来自批发运营商的网络中设备发出的报文的情况下，在批发运营商网络、下级运营商网络 and 用户网络中设置TPSM参数的示意图。

具体实施方式

本发明提供了一种运营商的运营商情况下生存时间分区安全机制的实现方法，本发明的核心为：在CsC组网的情况下，根据实际组成网络的不同要求，设置不同的TPSM参数，在批发运营商网络和下级运营商网络中同时实施TPSM。

下面结合附图来详细描述本发明，本发明所述方法的具体处理流程图如图2所示，包括如下步骤：

步骤2-1：在批发运营商网络、下级运营商网络 and 用户网络中设置不同的TPSM参数。

本发明根据CsC实际组网的不同要求设置不同的TPSM参数。本发明将CsC实际组网分为两种情况：

第一种情况：下级运营商接受来自批发运营商的网络中设备发出的报文，比如路由更新报文的情况。

在该情况下，在批发运营商网络、下级运营商网络 and 用户网络中设置TPSM参数的示意图如图3所示。

如图3所示，本发明将TTL分成多个段，其中批发运营商使用的TTL段是比较高的段，取值范围为255到A1_min，A1_min为运营商A的TTL允许的最小值；而下级运营商使用更大的TTL段，取值范围为255到B1_min，B1_min为运营商B的TTL允许的最小值，并且B1_min比A1_min小，因此，该TTL段包含了批发运营商使用的TTL段；用户网络使用的TTL段为U1_max到0，U1_max为用户网络允许的TTL最大值，并且U1_max小于B1_min。

第二种情况：下级运营商不接受来自批发运营商的网络中设备发出的报文，比如，认为这类报文本身也存在安全攻击的可能的情况。

在该情况下，在批发运营商网络、下级运营商网络 and 用户网络中设置TPSM参数的示意图如图4所示。

在该情况下本发明也将TTL分成多个段，其中批发运营商使用比较高的

TTL段，取值范围为255到A2_min，A2_min为运营商A的TTL允许的最小值；而下级运营商使用比较低的TTL段，取值范围为B2_max到A2_min，B2_max为运营商B的TTL允许的最大值，B2_min为运营商B的TTL允许的最小值，并且B2_max比A2_min小；用户网络使用最低的TTL段，取值范围为U2_max到0，U2_max为用户网络允许的TTL最大值，并且U2_max小于B2_min。

根据上述TPSM参数设置情况，批发运营商使用的TTL段、下级运营商使用的TTL段和用户网络使用的TTL段之间都没有重叠。

步骤2-2：根据设置的TPSM参数，在批发运营商网络、下级运营商网络中执行相应的TPSM处理流程。

在设置完TPSM参数后，本发明便根据设置的TPSM参数，在批发运营商网络、下级运营商网络中执行相应的TPSM处理流程。

针对上述第一种情况，在批发运营商网络A中的TPSM处理流程描述如下：

对于批发运营商网络A，可以按照现有的TPSM中规定的处理流程来实现TPSM。

网络A的PE（边缘路由器）检查每个进入网络A的报文，如果PE检查到一个报文的地址不是自己，并且报文的TTL大于A1_min，即TPSM中规定的255-TrustRadius，则将该报文的TTL减少为B1_max，对于网络A而言，B1_max即是TPSM基本方案中的TTL_USER_MAX。然后，将报文进行正常的转发。

设置网络A中每个设备发出的报文的TTL初始值为255。网络A中每个设备（包括网络A中的PE）如果收到目的地址是自己的报文，同时TTL不大于A1_min，则将该报文直接丢弃；如果TTL大于或等于A1_min，则根据事先确定的安全策略、报文的TTL和网络A的TPSM参数，将报文转上层协议进行处理。

针对上述第一种情况，在下级运营商网络B中的TPSM处理流程描述如下：

网络B的PE检查每个进入网络B的报文，当连接用户网络的PE检查到一个来自用户网络的目的地址不是自己的报文，并且报文的TTL大于B1_min，则将该报文的TTL减少为U1_max，然后，将报文进行正常的转发。当连接网络A的PE检查到一个来自网络A的目的地址不是自己的报文，则直接将报文进行正常的转发。

设置网络B中每个设备发出的报文的TTL初始值也为255。因此，此时网络B中某个设备收到一个TTL大于A1_min的报文，也无法确定该报文是来自网络A还是网络B。

网络B中每个设备（包括网络B的PE）如果收到目的地址是自己的报文，同时TTL不大于B1_min，则认为该报文来自用户网络，将该报文直接丢弃；如果TTL大于或等于B1_min，则根据事先确定的安全策略、报文的TTL和网络B的TPSM参数，将报文转上层协议进行处理。

上述第一种情况下的本发明所述方法的处理流程的特点是实施简单，能够适应大多数的情况，同基本的TPSM差别不大，其中B1_min对于网络B来说就是TPSM中的255-TrustRadius。

针对上述第二种情况，在批发运营商网络A中的TPSM处理流程如下：

网络A的PE检查每个进入网络A的报文，如果PE检查到一个报文的目的地址不是自己，并且报文的TTL大于A2_min，即TPSM中规定的255-TrustRadius，则将该报文的TTL减少为B2_max，对于网络A而言，B2_max即是TPSM基本方案中的TTL_USER_MAX。然后，将报文进行正常的转发。

设置网络A中每个设备发出的报文的TTL初始值为255。网络A中每个设备（包括网络A中的PE）如果收到目的地址是自己的报文，同时TTL不大于A2_min，则将该报文直接丢弃；如果TTL大于或等于A2_min，则根据事先确

定的安全策略、报文的TTL和网络A的TPSM参数，将报文转上层协议进行处理。

针对上述第二种情况，在下级运营商网络B中的TPSM处理流程描述如下：

网络B的边缘路由器PE检查每个进入网络B的报文，当连接用户网络的PE检查到一个来自用户网络的目的地址不是自己的报文，并且报文的TTL大于B2_min，则将该报文的TTL减少为U2_max，然后，将报文进行正常的转发。当连接网络A的PE检查到一个来自网络A的目的地址不是自己的报文，并且报文的TTL大于B2_max，则直接将该报文丢弃。

设置网络B中每个设备发出的报文的TTL初始值为B_max。网络B中每个设备（包括网络B的PE）如果收到目的地址是自己的报文，同时TTL不大于B2_min，则认为该报文来自用户网络，将该报文直接丢弃；如果TTL大于或等于B2_min，则根据事先确定的安全策略、报文的TTL和网络B的TPSM参数，将报文转上层协议进行处理。

在上述第一种情况和第二种情况中，选择B_max和B_min的时候需要考虑网络A的复杂性，因为从网络B的一个场所经网络A到达网络B的另外一个场所的过程中，TTL也是要减少的。因此，理论上规定： $B_max - B_min > \text{网络A的信任半径} + \text{网络B中信任半径最大的两个场所的信任半径之和}$ 。

本发明所述的方法适用于IPv4网络或IPv6网络。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

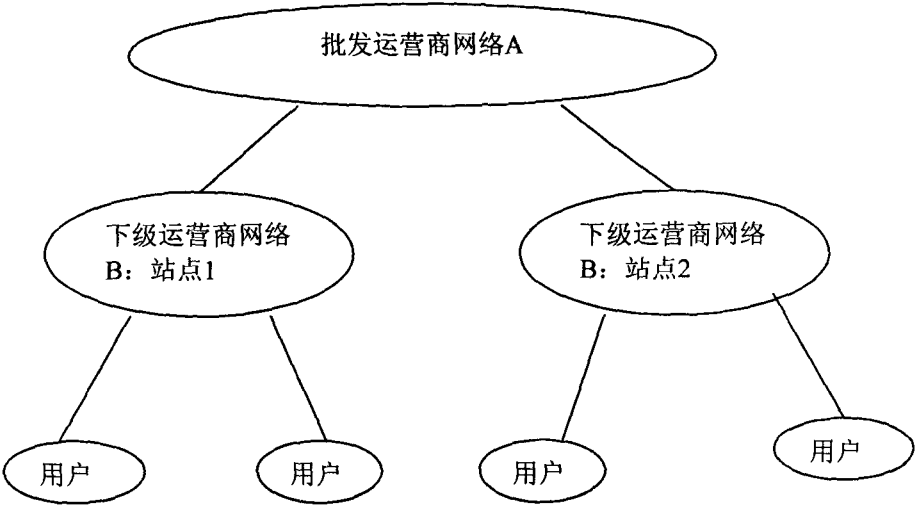


图1

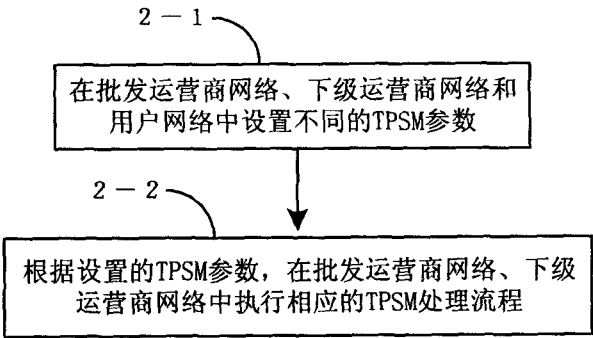


图2

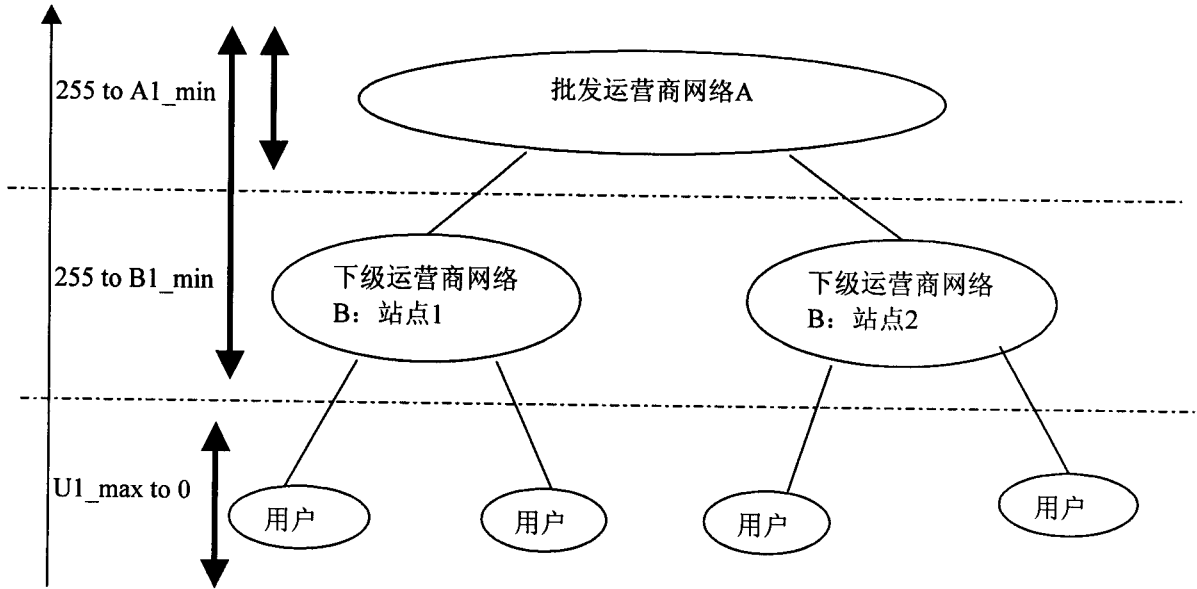


图3

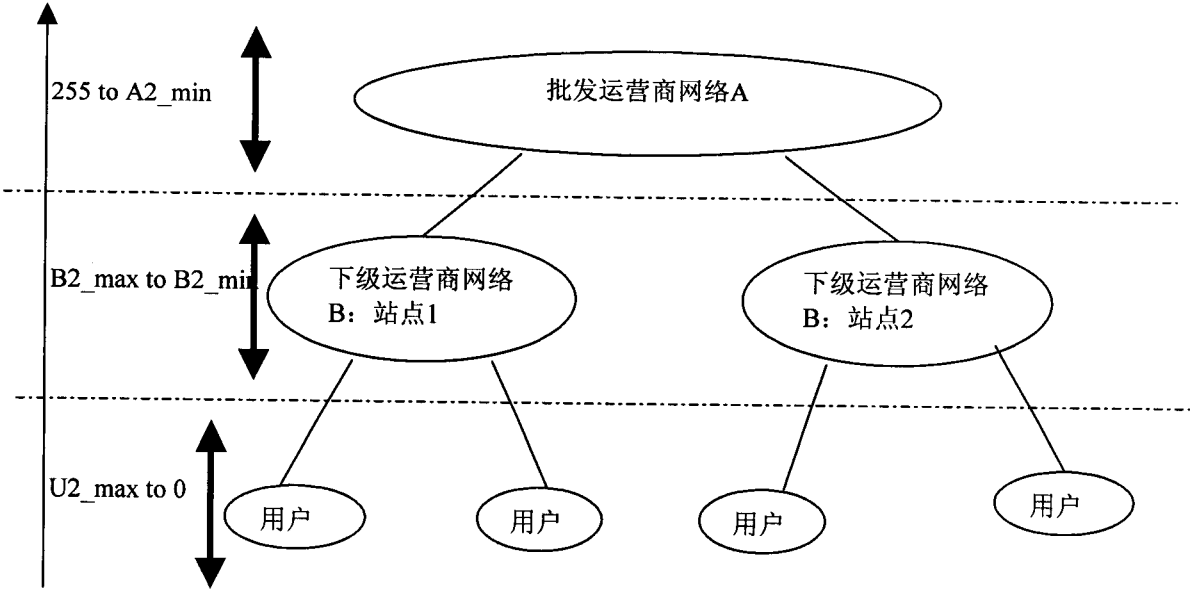


图 4