



(12) 发明专利

(10) 授权公告号 CN 101360045 B

(45) 授权公告日 2015. 01. 07

(21) 申请号 200810131178. 4

(22) 申请日 2008. 07. 30

(30) 优先权数据

07/56817 2007. 07. 30 FR

(73) 专利权人 佳能株式会社

地址 日本东京

(72) 发明人 S·巴龙 P·卢梭

(74) 专利代理机构 中国国际贸易促进委员会专
利商标事务所 11038

代理人 杨国权

(51) Int. Cl.

H04L 12/70(2013. 01)

H04L 1/00(2006. 01)

H04L 1/18(2006. 01)

H04L 29/06(2006. 01)

(56) 对比文件

WO 2007036764 A1, 2007. 04. 05, 说明书第 1

页第 15 行至第 2 页第 3 行, 第 19 页第 28 行至第 21 页第 8 行, 第 21 页第 12 行至第 22 页第 8 行, 第 50 页第 24 行至 51 页第 4 行, 第 54 页第 23 行至第 55 页第 10 行及附图 2.

US 6771594 B1, 2004. 08. 03, 说明书第 1 栏第 53 行至 58 行, 第 2 栏第 31 行至 44 行, 第 7 栏第 18 行至 63 行.

CN 1402494 A, 2003. 03. 12, 全文.

US 2001030944 A1, 2001. 10. 18, 全文.

CN 1914877 A, 2007. 02. 14, 全文.

CN 1284809 A, 2001. 02. 21, 全文.

CN 1784674 A, 2006. 06. 07, 全文.

WO 2007040428 A1, 2007. 04. 12, 全文.

审查员 刘欣科

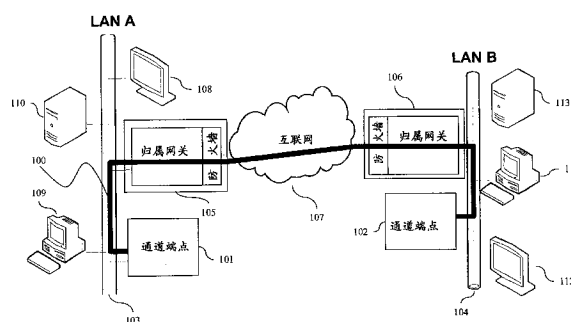
权利要求书3页 说明书17页 附图14页

(54) 发明名称

通道中传输数据包的方法、存储装置和通道端点

(57) 摘要

公开了通道中传输数据包的方法、相应计算机程序产品、存储装置和通道端点。提出了在将两个子网络互连以形成总通信网络的通道中传输数据包的方法, 通道在两个通道端点之间实现, 每个子网络包括通道端点中的独特通道端点, 通道实现至少两个传输信道, 该方法由通道端点中称为通道进入端点的端点实现。对每个数据包, 该方法包括: 接收来自与通道进入端点属于相同的子网络的源装置的数据包; 根据与包含在接收的包中的净荷数据相关的协议以及关于与传输信道中当前传输条件相关联的传输质量的信息, 从传输信道中选择有效信道; 根据与有效信道相关的传输协议, 封装接收的包, 用于获得将被发送的包; 和在选择的有效信道上, 传输将在通道中发送的包。



1. 一种用于在将两个子网络 (103, 104) 互连以便形成总的通信网络的通道中 (100) 进行数据包的传输的方法, 所述通道在两个通道端点 (101, 102) 之间实现, 所述子网络中的每一个包括所述通道端点之中的独特通道端点, 所述通道实现至少两个传输信道, 每个传输信道与不同的传输协议相关联, 所述方法由所述通道端点中称为通道进入端点的端点来实现, 其特征在于, 所述方法包括用于每个数据包的以下步骤:

- a) 接收 (1) 来自源装置的所述数据包, 该源装置与通道进入端点属于相同的子网络;
- b) 根据与包含在所述接收的包中的净荷数据相关的乘客协议以及关于与所述传输信道上当前传输条件相关联的传输质量的信息, 从传输信道中选择 (3) 有效信道, 所述信息取决于与包含在所述接收的包中的净荷数据相关的所述乘客协议;
- c) 根据与有效信道相关的所述传输协议, 封装 (5) 所述接收的包, 用于获得将被发送的包; 以及
- d) 在所选择的有效信道上, 传输 (6) 将在通道中发送的包。

2. 如权利要求 1 所述的方法, 其特征在于, 所述关于与当前传输条件有关的传输质量的信息属于包括以下项的组:

- 关于所述传输信道的拥塞 ECN 的信息;
- 关于所述传输信道的误包率 PER 的信息; 以及
- 关于所述传输信道的重传率, 即 TCP 信道重传率, 的信息。

3. 如权利要求 1 或 2 所述的方法, 其特征在于, 所述选择 (3) 有效信道的步骤 b) 包括以下步骤:

i) 确定 (32) 与所述接收的包相关的包类型, 每种包类型由与包含在拥有所述包类型的包中的净荷数据相关的不同乘客协议来定义;

ii) 根据关于如下传输质量的信息, 确定 (36) 称为在先优选信道的优选信道, 该在先优选信道对于由通道进入端点发送并具有与所述接收的包相同类型的先前发送的包实现最佳传输, 其中, 所述传输质量与对于所述先前发送的包获得的所述传输信道上的传输条件有关;

iii) 获得 (34) 所述关于与所述传输信道上的当前传输条件相关联的传输质量的信息;

iv) 根据与所接收的包相关的包类型以及所述至少一条关于与当前传输条件相关联的传输质量的信息, 选择 (35) 实现所述接收的包的最佳传输的、称为新的优选信道的信道; 以及

v) 根据在先优选信道、新的优选信道以及与所述接收的包相关的包类型, 选择 (38) 所述有效信道。

4. 如权利要求 3 所述的方法, 其特征在于, 如果对于与所述接收的包相关的数据类型, 在先优选信道不同于新的优选信道, 则通过对于与所述接收的包相关的包类型从所述在先优选信道平滑切换 (363, 364) 到所述新的优选信道的机制而得到对有效信道的选择。

5. 如权利要求 1 到 2 中的任何一个所述的方法, 其特征在于, 通过下面的两个信道来实现所述选择有效信道的步骤:

- 称为 TCP 信道的第一信道, 其相关的传输协议是 TCP 协议; 以及
- 称为 UDP 信道的第二信道, 其相关的传输协议是 UDP 协议。

6. 如权利要求 3 所述的方法,其特征在于,假设所接收的包是 UDP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的拥塞,则用于所述接收的包的新的优选信道是 UDP 信道 (359),以及如果关于与当前传输条件相关联的传输质量的所述信息没有指示所述传输信道的任何拥塞,则用于所述接收的包的新的优选信道是 TCP 信道 (358)。

7. 如权利要求 3 所述的方法,其特征在于,假设所接收的包是 UDP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的拥塞,则所述接收的包的新的优选信道是 UDP 信道 (359),以及如果关于与当前传输条件相关联的传输质量的所述信息指示误包率在确定的阈值以下,则用于所述接收的包的新的优选信道是 TCP 信道 (358),以及如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的误包率大于或等于所述确定的阈值,则用于所述接收的包的新的优选信道是 UDP 信道 (359)。

8. 如权利要求 3 所述的方法,其特征在于,假设所接收的包是 TCP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的重传率在确定的阈值之上,则用于所述所接收的包的新的优选信道是 UDP 信道 (359),以及如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的传输速率低于或等于所述确定的阈值,则用于所述接收的包的新的优选信道是 TCP 信道 (358)。

9. 一种通道进入端点,其能够在将两个子网络互连以便形成总的通信网络的通道中实现数据包的传输,所述通道在所述通道进入端点与通道离开端点之间被实现,所述子网络中的每一个包括所述通道端点中的一个独特通道端点,所述通道实现至少两个传输信道,每个传输信道与不同的传输协议相关联,

其特征在于,所述通道进入端点包括:

- 用于接收来自源装置的数据包的装置,该源装置与通道进入端点属于相同的子网络;

- 用于根据与包含在所述接收的包中的净荷数据相关的乘客协议以及关于与所述传输信道上当前传输条件相关联的传输质量的信息从传输信道中选择有效信道的装置,所述信息取决于与包含在所述接收的包中的净荷数据相关的所述乘客协议;

- 用于根据与有效信道相关的所述传输协议来封装所述接收的包以用于获得将被发送的包的装置;以及

- 用于在所选择的有效信道上传输将在通道中发送的包的装置。

10. 如权利要求 9 所述的通道进入端点,其特征在于,所述关于与当前传输条件有关的传输质量的信息属于包括以下项的组:

- 关于所述传输信道的拥塞的信息;

- 关于所述传输信道的误包率的信息;以及

- 关于所述传输信道的重传率的信息。

11. 如权利要求 9 和 10 中的任何一个所述的通道进入端点,其特征在于,所述选择有效信道的装置包括:

- 用于确定与所述接收的包相关的包类型的装置,每种包类型由与包含在拥有所述包类型的包中的净荷数据相关的不同乘客协议来定义;

- 用于根据关于如下传输质量的信息确定称为在先优选信道的优选信道的装置,该在先优选信道对于由通道进入端点发送并具有与所述接收的包相同类型的先前发送的包实现最佳传输,其中,所述传输质量与对于所述先前发送的包获得的所述传输信道上的传输条件有关;

- 用于获得所述关于与所述传输信道上的当前传输条件相关联的传输质量的信息的装置;

- 用于根据与所接收的包相关的包类型以及所述至少一条关于与当前传输条件相关联的传输质量的信息来选择实现所述接收的包的最佳传输的、称为新的优选信道的信道的装置;以及

- 用于根据在先优选信道、新的优选信道以及与所述接收的包相关的包类型来选择所述有效信道的装置。

12. 如权利要求 9 到 10 中的任何一个所述的通道进入端点,其特征在于,通过与每个信道相关的传输协议以及所述传输协议的输入和输出端口来唯一地标识每个信道。

13. 如权利要求 9 到 10 中的任何一个所述的通道进入端点,其特征在于,从中选择有效信道的所述传输信道是下面的两个信道:

- 称为 TCP 信道的第一信道,其相关的传输协议是 TCP 协议;以及
- 称为 UDP 信道的第二信道,其相关的传输协议是 UDP 协议。

14. 如权利要求 11 所述的通道进入端点,其特征在于,所述选择有效信道的装置是这样的,即:假设所接收的包是 UDP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的拥塞,则用于所述接收的包的新的优选信道是 UDP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息没有指示所述传输信道的任何拥塞,则用于所接收的包的新的优选信道是 TCP 信道。

15. 如权利要求 11 所述的通道进入端点,其特征在于,所述选择有效信道的装置是这样的,即:假设所接收的包是 UDP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的拥塞,则所述接收的包的新的优选信道是 UDP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息指示误包率在确定的阈值以下,则用于所述接收的包的新的优选信道是 TCP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的误包率大于或等于所述确定的阈值,则用于所述接收的包的新的优选信道是 UDP 信道。

通道中传输数据包的方法、存储装置和通道端点

技术领域

[0001] 本发明的技术领域是通信网络的技术领域。

[0002] 更具体地说,本发明涉及一种用于在通过通信网络的通道中传输数据包(也称为数据报)的技术。

[0003] 一方面,高比特率互联网在民众中得到普及,另一方面,出现了具有网络连接性的广泛传播的消费者视听设备,这两方面将创建对于用户部分的新的行为方式。这些新的行为方式毫无疑问地涉及属于具有共同兴趣(休闲、家庭等)的人群(我们可将其称作“持久联系”的群体)的个人的出现。这些群体将与相同兴趣领域的其他个人建立几乎永久性的联系,他们建立音频和/或视频通信,并共享各种信息(音频、视频、图片、文本等)。

[0004] 虚拟专用网络(VPN)的技术正在提供针对上述预期的有价值的解决方案。VPN能够在使用可靠性低但并不昂贵的互联网体系结构时,以安全的方式在共享相同兴趣领域的个人之间实现实时的透明通信。

[0005] 为了进行透明的通信并克服对不可路由地址的需要,VPN使用称为隧穿(tunneling)的特定类型的封装,其创建所谓的通道(tunnel)。该操作在于借助封装协议C来以B级别协议(传输协议)封装A级别协议(乘客协议,passenger protocol),其中,在诸如ISO模型(其描述了由各个层中的每一层提供的服务以及它们的互相作用)的分层模型中,B协议的层(级别)高于或等于A协议的层(级别)。

[0006] 因此,传输协议处理乘客协议,就好像其是净荷数据一样。图2b(以下将详细描述)呈现了级别2的VPN的示例,即,级别-2通道中的封装的例子(级别-2通道表示乘客协议是ISO模型的层2的协议)。

[0007] 隧穿可用于在不支持网络协议的网络上传输该网络协议。隧穿还可用于提供不同类型的VPN功能,诸如作为示例的个人寻址。

[0008] 现在,承担远程接入的消费者功能以及本地局域网(LAN)正逐渐使用隧穿技术。

[0009] 在以下的描述中,作为示例,我们考虑的仅是传输层的级别高于或等于4的级别2或级别3(即,至少为传输层在ISO模型中的级别)。

[0010] VPN频繁地用于将两个LAN互连,以便创建由两个原始LAN的联合体形成的虚拟局域网。安全的VPN包括加密技术和认证算法,以确保传输的数据的私密性。在图1a(以下将详细描述)中示出基于隧穿技术的典型VPN配置。在该示例中,通道端点没有集成到网关中。在两个通道端点之间建立通道,由本地通道端点对发送到与远程LAN连接的设备的每个包(也成为帧)进行封装,然后,所述每个包被发送到将对其进行解封装并在远程LAN上进行发送的远程通道端点。关于所述设备,它们虚拟地链接到相同的LAN。两个设备之间通过通道进行的通信也称为点对点通信。

背景技术

[0011] 在决定在两个通道端点之间建立通道的情况下出现的首要问题之一是要知道所述通道的传输协议应该是哪个。

[0012] 在现有技术中,主要使用层 3IP(互联网协议)或层 4TCP/UDP(传输控制协议/用户数据报协议)。由于基于 IP 的隧穿技术不能考虑网络地址翻译(NAT)机制,并且它们没有全部与图 1 的典型隧穿配置兼容,所以在说明书的剩余部分中,我们考虑(仅作为示例)基于层 4(传输层)(即,基于 TCP 或 UDP)的解决方案。

[0013] TCP 协议是面向连接的可靠协议,其向发送方确保他或她的数据将被有效地接收(确认的管理),并且所有的帧按照给定顺序被接收。TCP 应用有效的拥塞控制机制。

[0014] UDP 协议是一种更简单并且更快速的协议,它不考虑帧的顺序,也不管理确认。

[0015] 在这种特定情况下(其作为示例被单独指出),上述问题变为知晓应该将 TCP 还是 UDP 用作通道的传输协议的问题。

[0016] 问题在于:与乘客协议中使用的数据相应的协议可干扰通道中以传输协议实现的机制。例如,如果我们将 TCP 作为传输协议,并将 TCP 作为与乘客协议的净荷数据相应的协议(称为 TCP 上的 TCP(TCP over TCP)的组合),我们要面临两种 TCP 拥塞控制机制之间破坏性的相互作用。对于进一步的细节,可具体参考“Understanding TCP over TCP:effects of TCP tunnelling on end-to-end throughput and latency(O Honda,H Ohsaki,M. Imase,M. Ishizuka, J. Murayama). (Proceedings of the SPIE, volume 6011, pp 138-146(Oct 2005))”。

[0017] 第一反应可能认为 TCP 上的 TCP 组合不是一个好的解决方案。然而,即使在特定条件下公知的是:上述类型的隧穿使得点对点的性能下降,但是在其它条件下,同样的组合改进了点对点的性能(例如,参见上述示例以及以下文献:“Avoiding congestion collapse on the Internet using TCP tunnels(B. P. Lee, R. K. Balan, L. Jacob, W. K. G. Seah, A. L. Ananda) (Computer Networks 39(2002)pages 207-219,Dec2002)”。同样的问题伴随“UDP 上的 UDP(UDP over UDP)”组合(即,当我们将 UDP 协议作为传输协议,并将 UDP 作为乘客协议时)而出现。

[0018] 因此,没有针对上述问题(即,将在通道中使用的传输协议是哪一个)的绝对性应对,因为这必须取决于三个因素:

[0019] -将通过通道发送的数据的类型(与乘客协议的净荷数据相应的协议)、应用的类型(文件的传送、音频和/或视频流传输等);

[0020] -两个通道端点之间的网络质量(在帧丢失或损坏、拥塞等方面);以及

[0021] -用户和/或管理员的偏好(在带宽、可靠性、抖动等方面)。

[0022] 目前,当决定在两个通道端点之间建立通道时,必须强制性地对传输协议进行预定的选择(即,假设每个信道使用不同的传输协议,则对通道中的信道进行预定的选择),尽管该选择并不是所有解决方案中的最佳选择。

[0023] 在第 6614800 号美国专利文献中描述的已知技术使用两个虚拟专用网络(VPN),即,两个通道:用于控制数据的第一通道(在两个 IP 地址之间)、用于净荷数据的第二通道(在另两个 IP 地址之间)。这一技术使得能够选择用于控制数据的第一传输协议以及用于净荷数据的第二传输协议,所述两种类型的数据通过两个不同的通道。因此,可在两个信道中的每一个上优化对传输协议的选择。

[0024] 然而,所述技术具有两个主要缺点:其要求有两个通道(两对 IP 地址),以及每种类型的数据(控制数据和净荷数据)总是使用相同的传输协议。因此,对于所考虑的数据

类型,所述选择不是在每种解决方案中都是最佳的(下面,我们将会讨论)。

发明内容

[0025] 本发明在至少一个实施例中的目的特别是克服现有技术不同缺点。

[0026] 更具体地说,在本发明的至少一个实施例中,本发明的目标在于提供一种在通道中进行数据包传输的技术,通过该技术可优化传输信道的选择。

[0027] 本发明在至少一个实施例中的另一目标在于避免将在通道的信道上发送的数据质量的突发改变,所述突发改变会导致所述信道上进行的传输的劣化。

[0028] 本发明的至少一个实施例还旨在提供一种实现简单并且成本低的技术。

[0029] 本发明至少一个实施例的另一目的在于提供一种能够在通道端点中实现并由此对于源设备和目的地设备透明的技术。

[0030] 在本发明的特定实施例中,提出一种用于在将两个子网络互连以便形成总的通信网络的通道中进行数据包的传输的方法,所述通道在两个通道端点之间实现,所述子网络中的每一个包括所述通道端点之中的独特通道端点,所述通道实现至少两个传输信道,所述方法由所述通道端点之一(称为通道进入端点)来实现。对于每个数据包,所述方法包括以下步骤:

[0031] a) 接收来自源装置的所述数据包,该源装置与通道进入端点属于相同的子网络;

[0032] b) 根据与包含在所述接收的包中的净荷数据相关的协议以及关于与所述传输信道中当前传输条件相关联的传输质量的信息,从传输信道中选择有效信道;

[0033] c) 根据与有效信道相关的传输协议,封装所述接收的包,用于获得将被发送的包;以及

[0034] d) 在所选择的有效信道上,传输将在通道中发送的包。

[0035] 因此,本发明总的原理在于:执行动态的多信道隧穿,即,使用多信道通道(例如由其传输协议并在可能的情况下由一对输入/输出端口来定义每个信道),以及对于将在通道上发送的每个数据包选择通道的信道中的一个。

[0036] 通过这种方式,所使用的有效信道(以及相应的传输协议)总是最佳的。

[0037] 必须注意到:选择有效传输信道的步骤是基于来自源装置的数据包类型(即,包含在所述包中的净荷数据的协议)以及关于网络上传输质量的返回信息两者的。

[0038] 有利地,所述关于与当前传输条件有关的传输质量的信息属于包括以下项的组:

[0039] - 关于所述传输信道的拥塞的信息(ECN);

[0040] - 关于所述传输信道的误包率(PER)的信息;以及

[0041] - 关于所述传输信道的重传率(TCP 信道重传率)的信息。

[0042] 选择信道的准则可基于所述列表的一个元素或多个组合的元素。上述列表并不是穷尽的。

[0043] 对于关于网络拥塞的信息,作为示例,我们使用如“RFC 3168-The Addition of Explicit Congestion Notification(ECN) to IP”中特别描述的 ECN(明确拥塞通知)。

[0044] 误包率也称为 PER。

[0045] 有利地,所述选择有效信道的步骤 b) 包括以下步骤:

[0046] i) 确定与所述接收的包相关的包类型,每种包类型由与包含在拥有所述包类型的

包中的净荷数据相关的不同协议来定义；

[0047] ii) 根据关于如下传输质量的信息,确定称为在先优选信道的优选信道,其对于由通道进入端点发送并具有与所述接收的包相同类型的先前发送的包实现最佳传输,其中,所述传输质量与对于所述先前发送的包获得的所述传输信道上的传输条件有关；

[0048] iii) 获得所述关于与所述传输信道上的当前传输条件相关联的传输质量的信息；

[0049] iv) 根据与所接收的包相关的包类型以及所述至少一条关于与当前传输条件相关联的传输质量的信息,选择实现所述接收的包的最佳传输的信道(称为新的优选信道)；以及

[0050] v) 根据在先优选信道、新的优选信道以及与所述接收的包相关的包类型,选择所述有效信道。

[0051] 重要的是:有效传输信道能够暂时与新的优选信道不同(例如,在对网络上的传输条件进行修改之后优选信道发生改变的情况下)。

[0052] 例如,如果所接收的包是 IP 数据报,则术语“与包含在包中的净荷数据相关的协议”被理解为是指与所述 IP 数据报的净荷数据相关的 ISO 模型的传输层(级别)协议(诸如 TCP 或 UDP)。不应把所述与净荷数据相关的 ISO 模型传输层(或级别)协议错认为是与通道的每个传输信道相关的传输协议。

[0053] 根据有利特征,如果对于与所述接收的包相关的数据类型,在先优选信道不同于新的优选信道,则通过对于与所述接收的包相关的包类型从所述在先优选信道平滑切换到所述新的优选信道的机制而产生对有效信道的选择。

[0054] 平滑切换的机制防止将在信道上发送的数据的量产生突然变化,该变化会导致传输的劣化。

[0055] 例如,在从 UDP 信道切换到 TCP 信道(即,从传输协议为 TCP 协议的信道切换到传输协议是 UDP 协议的信道)期间,如果 TCP 信道上的所有包被立即切换过去,而不考虑要与 TCP 信道的 TCP(拥塞)窗口的兼容,则不能立即发送的包将被延迟(或缓冲),从而产生这些包的 RTT(往返时间)的虚假增长,其结果可能甚至需要重传特定包,其中,假设乘客协议是 TCP 协议,则所述特定的重传包将具有灾难性的效果。很清楚,由于引入虚假干扰,所以所有预计的从 UDP 信道切换到 TCP 信道的好处将丢失,以及所进行的所有操作将是事情变得更为糟糕。

[0056] 类似地,不经过控制地从 TCP 信道切换到 UDP 信道将阻碍传输媒介,这是因为,不应忘记的是不同的传输信道共享对互联网的相同物理接入。在从 TCP 信道改变到 UDP 信道的情况下,由于 UDP 信道上的吞吐量迅速增长,会高度损害在 TCP 信道上缓冲并被设计为将在 TCP 信道上发送的包。因此,有必要建立渐进系统,用于将由 TCP 信道使用的带宽转移到 UDP 信道。利用这种系统,使得在 TCP 信道上缓冲的包有时间流动得足够多,以使得当在新的信道(UDP 信道)上发送全体包时,没有包会受到损害。

[0057] 有利地,对于每种类型的包,所述平滑切换机制包括如下步骤:对于所述信道中的每一个管理最大传输窗口,其指示在给定的时间间隔期间,可在所述信道上发送的数据的最大数量。

[0058] 因此,通道的每个传输信道具有这样的传输窗口,其用于定义在给定的时间间隔

期间可通过通道端点在所述信道上发送的数据的最大数量。

[0059] 根据有利特征,在给定的时间间隔期满之后,新的优选信道的最大传输窗口增加,以及在先优选信道的最大传输窗口变小,这表示在新的给定时间间隔期间能够在所述信道上发送的数据的新的最大数量。

[0060] 因此,这确保了能够在传输信道上发送的数据的最大数量随着时间而改变,从而共同确保从一个信道(在先优选信道)到另一信道(新的优选信道)的平滑切换。

[0061] 根据优选特征,有效信道为:

[0062] - 在传输窗口的限制之内的新的优选信道,所述传输窗口与用于与所接收的包相关的包类型的所述新的优选信道相关,或者

[0063] - 在超出所述传输窗口的情况下为在先优选信道,所述传输窗口与用于与所接收的包相关的包类型的所述新的优选信道相关。

[0064] 有利地,通过与每个信道相关的传输协议来唯一地标识每个信道。

[0065] 例如,我们具有分别由 TCP 和 UDP 传输协议标识的 TCP 信道和 UDP 信道。

[0066] 在有利的变例中,通过与每个信道相关的传输协议以及所述传输协议的输入和输出端口来唯一地标识每个信道。

[0067] 因此,对于经过若干信道中的每一个的包,可使用相同的传输协议但是例如不同类型的服务来有区别地管理所述若干信道。

[0068] 在示例性实施例中,从下面的两个信道中进行选择有效信道的步骤:

[0069] - 第一信道,称为 TCP 信道,其相关的传输协议是 TCP 协议;以及

[0070] - 第二信道,称为 UDP 信道,其相关的传输协议是 UDP 协议。

[0071] 在第一特定实施例中,假设所接收的包是 UDP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的拥塞,则用于所述接收的包的新的优选信道是 UDP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息没有指示所述传输信道的任何拥塞,则用于所述接收的包的新的优选信道是 TCP 信道。

[0072] 在第二特定实施例中,假设所接收的包是 UDP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的拥塞,则所述接收的包的新的优选信道是 UDP 信道,如果关于与当前传输条件相关联的传输质量的所述信息指示误包率 (PER) 在确定的阈值 (Pth) 以下,则用于所述接收的包的新的优选信道是 TCP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的误包率 (PER) 大于或等于所述确定的阈值 (Pth),则用于所述接收的包的新的优选信道是 UDP 信道。

[0073] 在第三特定实施例中,假设所接收的包是 TCP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的重传率在确定的阈值 (Rth) 之上,则用于所述接收的包的新的优选信道是 UDP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的传输速率低于或等于所述确定的阈值 (Rth),则用于所述接收的包的新的优选信道是 TCP 信道。

[0074] 清楚的是,在不脱离本发明的范围的情况下,可设想选择新的优选信道的步骤的其它实施例。例如,可使用关于网络的其它传输质量准则和 / 或在上述第一、第二和第三实施例中使用的准则的其它组合。

[0075] 在另一实施例中,本发明涉及可从通信网络下载和 / 或记录在计算机可读载体

上和 / 或可由处理器执行的计算机程序产品,所述计算机程序产品包括程序代码指令,当所述程序在计算机上执行时,所述程序代码指令用于实现上述方法(在其至少一个实施例中)。

[0076] 在另一实施例中,本发明涉及一种可总体或局部分离的存储装置,其可由计算机读取,存储一组指令,当所述程序在计算机上执行时,可由所述计算机执行所述指令以实现上述方法(在其至少一个实施例中)。

[0077] 在另一实施例中,本发明涉及一种通道进入端点,其能够在将两个子网络互连以便形成总的通信网络的通道中实现数据包的传输,所述通道在所述通道进入端点与通道离开端点之间被实现,所述子网络中的每一个包括所述通道端点中的独特通道端点,所述通道实现至少两个传输信道。所述通道进入端点包括:

[0078] - 用于接收来自源装置的数据包的装置,该源装置与通道进入端点属于相同的子网络;

[0079] - 用于根据与包含在所述接收的包中的净荷数据相关的协议以及关于与所述传输信道中当前传输条件相关联的传输质量的信息从传输信道中选择有效信道的装置;

[0080] - 用于根据与有效信道相关的传输协议来封装所述接收的包以用于获得将被发送的包的装置;以及

[0081] - 用于在所选择的有效信道上传输将在通道中发送的包的装置。

[0082] 有利地,所述关于与当前传输条件有关的传输质量的信息属于包括以下项的组:

[0083] - 关于所述传输信道的拥塞的信息;

[0084] - 关于所述传输信道的误包率 (PER) 的信息;以及

[0085] - 关于所述传输信道的重传率的信息。

[0086] 有利地,所述选择有效信道的装置包括:

[0087] - 用于确定与所述接收的包相关的包类型的装置,每种包类型由与包含在拥有所述包类型的包中的净荷数据相关的不同协议来定义;

[0088] - 用于根据关于如下传输质量的信息确定称为在先优选信道的优选信道的装置,该在先优选信道对于由通道进入端点发送并具有与所述接收的包相同类型的先前发送的包实现最佳传输,其中,所述传输质量与对于所述先前发送的包获得的所述传输信道上的传输条件有关;

[0089] - 用于获得所述关于与所述传输信道上的当前传输条件相关联的传输质量的信息的装置;

[0090] - 用于根据与所接收的包相关的包类型以及所述至少一条关于与当前传输条件相关联的传输质量的信息来选择实现所述接收的包的最佳传输的信道(称为新的优选信道)的装置;以及

[0091] - 用于根据在先优选信道、新的优选信道以及与所述接收的包相关的包类型来选择所述有效信道的装置。

[0092] 根据有利特征,所述选择有效信道的装置包括:

[0093] - 用于对于与所述接收的包相关的包类型而实现从所述在先优选信道平滑切换到所述新的优选信道的机制的装置;以及

[0094] - 用于如果对于与所述接收的包相关的包类型,在先优选信道不同于新的优选信

道,则激活所述实现平滑切换机制的装置的装置。

[0095] 有利地,对于每种类型的包,所述实现平滑切换机制的装置包括:对于所述信道中的每一个管理最大传输窗口的步骤,最大传输窗口指示在给定的时间间隔期间,可在所述信道上发送的数据的最大数量。

[0096] 根据有利特征,所述窗口管理装置是这样的:在给定的时间间隔期满之后,新的优选信道的最大传输窗口增加,以及在先优选信道的最大传输窗口变小,这表示在新的给定时间间隔期间能够在所述信道上发送的数据的新的最大数量。

[0097] 根据优选特征,所述实现平滑切换机制的装置是这样的以使得有效信道为:

[0098] - 在传输窗口的限制之内的新的优选信道,所述传输窗口与用于与所接收的包相关的包类型的所述新的优选信道相关,或者

[0099] - 在超出所述传输窗口的情况下为在先优选信道,所述传输窗口与用于与所接收的包相关的包类型的所述新的优选信道相关。

[0100] 有利地,通过与每个信道相关的传输协议来唯一地标识每个信道。

[0101] 根据有利的变例,通过与每个信道相关的传输协议以及所述传输协议的输入和输出端口来唯一地标识每个信道。

[0102] 在一示例性实施例中,从中选择有效信道的所述传输信道是下面的两个信道:

[0103] - 第一信道,称为 TCP 信道,其相关的传输协议是 TCP 协议;以及

[0104] - 第二信道,称为 UDP 信道,其相关的传输协议是 UDP 协议。

[0105] 在第一特定实施例中,所述选择有效信道的装置是这样的,即:假设所接收的包是 UDP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的拥塞,则用于所述接收的包的新的优选信道是 UDP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息没有指示所述传输信道的任何拥塞,则用于所接收的包的新的优选信道是 TCP 信道。

[0106] 在第二特定实施例中,所述选择有效信道的装置是这样的,即:假设所接收的包是 UDP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的拥塞,则所述接收的包的新的优选信道是 UDP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息指示误包率在确定的阈值以下,则用于所述接收的包的新的优选信道是 TCP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的误包率大于或等于所述确定的阈值,则用于所述接收的包的新的优选信道是 UDP 信道。

[0107] 在第三特定实施例中,所述选择有效信道的装置是这样的,即:假设所接收的包是 TCP 类型的包,如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的重传率在确定的阈值之上,则用于所述接收的包的新的优选信道是 UDP 信道,以及如果关于与当前传输条件相关联的传输质量的所述信息指示所述传输信道的传输速率低于或等于所述确定的阈值,则用于所述接收的包的新的优选信道是 TCP 信道。

附图说明

[0108] 通过以下作为表示性和非穷尽的示例给出的描述(并不是本发明的所有实施例都被限于以下描述的实施例的特征和优点)以及附图,本发明实施例的其它特点和优点将

而变得清楚,其中:

[0109] 图 1a 示出使用通道的典型虚拟专用网络 (VPN) 配置;

[0110] 图 1b 示出可实现本发明方法的通道端点的经典分层模型的示例;

[0111] 图 2a 示出传送层 2 通道包的以太网帧的格式的示例;

[0112] 图 2b 是在根据本发明的方法的特定实施例中,由通过通道进行发送的通道端点执行的出站 (outbound) 算法的流程图;

[0113] 图 2c 是根据依照本发明的方法的特定实施例,由通过通道进行接收的通道端点执行的入站 (inbound) 算法的流程图;

[0114] 图 3 是根据依照本发明的方法的特定实施例,用于选择有效信道的算法的流程图 (图 2b 的步骤 3 的细节);

[0115] 图 4、图 5 和图 6 是根据依照本发明的方法的特定实施例,用于选择优选信道的三种不同算法的流程图 (图 3 的步骤 35 的细节);

[0116] 图 7a 是根据依照本发明的方法的特定实施例,用于管理当前传输模式以及用于包类型的传输窗口的算法的流程图 (图 3 的步骤 36 的细节);

[0117] 图 7b 是根据本发明的方法的特定实施例的包类型的表;

[0118] 图 8a 是根据本发明的特定实施例的用于管理过渡性 UDP 到 TCP 模式的算法的流程图;

[0119] 图 8b 是根据本发明的特定实施例的用于管理过渡性 TCP 到 UDP 模式的算法的流程图;

[0120] 图 8c 是根据依照本发明的方法的特定实施例,用于选择包类型的有效信道的算法的流程图 (图 3 的步骤 38 的细节);以及

[0121] 图 9 示出根据本发明特定实施例的通信设备 (通道端点) 的结构。

具体实施方式

[0122] 在本发明的所有附图中,相同的元素和步骤由相同的标号来指定。

[0123] 因此,本发明涉及这样一种技术,其在分别连接到第一和第二 LAN 的两个通道端点中实现,以便改善连接到第一 LAN 的各设备与连接到第 LAN 的各设备之间的通信。

[0124] 本发明总的原理包括:对于将经由通道发送的每个数据包,选择将被使用的最优信道 (通常由它的传输协议表征)。所述选择是基于将被发送的数据类型 (包含在所述包中的净荷数据的协议、应用的类型等) 以及 (在两个通道端点之间) 网络上的传输条件的。

[0125] 图 1a 示出通过通信网络 107 (例如,互联网) 在本地通道端点 101 与远程通道端点 102 之间实现通道 100 的虚拟专用网络 (VPN) 的典型配置。所述通道 100 连接两个本地网络:LAN A 103 以及 LANB 104。LAN 103 和 104 中的每一个具有高比特率的互联网接入设备 (能够集成防火墙的归属网关 (home gateway)) 105 和 106、PC 类型设备 109 和 111、用于存储和分发数字媒体 (属于音频、视频和图片类型) 的服务器 110 和 113 以及数字媒体恢复 (restitution) 设备 108 和 112。通道端点可被集成到诸如数字电视机的视听设备中。通道端点也可以按照执行与 PC 类型设备相关的功能的程序的形式而设置在 PC 类型设备中。

[0126] 一旦通道 100 被建立,则连接到 LAN A 103 的设备 108、109 和 110 能够与连接到

LAN B 104 的设备 111、112 和 113 进行通信。例如,连接到 LAN A 103 的客户机 108 能够与连接到网络 LAN B 104 的服务器 113 进行通信。

[0127] 附图 1a 示出仅具有一个通道的简单通信网络,但是应理解,相同的通道端点可能会管理几个通道(通向等同数量的通道端点)以便将第一 LAN 与若干其它 LAN 互连。此外,为了简便起见,所述附图没有示出诸如互联网路由器的互联网中的基础设备。

[0128] 参照图 1b,我们将描述来自(连接到 LAN B 103 的)设备 108、109、110 之一并将进入通道 100 的以太网帧的路由。为此,将使用分层模型。该分层模型描述实现所述通道 100 所需的协议层。在该模型中,没有表示对于除了使用通道之外的其它功能所必需的协议元素。例如,没有显示当通道端点 101 被集成到 UPN p 设备时与 UPnP 结构相关的协议元素。

[0129] 通道端点 101 具有以太网物理接口 208,其将来自设备 108、109、110 的以太网帧给予链路层 207 以进行路由:对于去往包括通道端点的设备的以太网帧,向着网络层 206 来实现所述路由,而对于其它以太网帧,向着桥接层 209 来实现所述路由。桥接层 209 实现经典的以太网桥的操作,诸如过滤以太网帧,并将这些帧中继到适当的以太网输出端口。所述桥具有以太网接口 207 和至少一个虚拟接口 210,用于模拟附加到所述桥的以太网控制器。对于由应用 200 例示的每个信道创建虚拟接口 210,所述应用 200 向所述信道给出必须传送经过分别例示的通道的以太网帧。通常,由应用 200 表示的通道的封装的协议执行实现每个通道所必需的操作,其中,具体是帧的配置、过滤和封装(形成通道包)以及提取。

[0130] 从虚拟接口 210 接收的帧在通过应用 200 处理之后,通过应用接口或套接(socket)层 201 以包的形式被转移到可靠的 TCP 传输协议 203 或不可靠的 UDP 传输协议 205,它们分别由 SSL 协议 202 和 DTLS 协议 204 确保其安全。在由传输协议处理以形成通道包 250(图 2a)之后,其被传递到网络层 206。用通道包由此形成的 IP 数据报现在可以通过链路层 207 和物理层 208 在 LAN 上进行发送。

[0131] 帧的接收将在通道端点中采取与以上提供的路径相反的路径。

[0132] 图 2a 提供传送级别 2 通道包的以太网帧(标为 260)的格式的示例。

[0133] 所述格式相应于这样的帧,作为示例,所述帧在图 1a 的 LAN A103 上在通道端点 101 与归属网关 105 之间传送(要在互联网上发送或从互联网接收),并包括以太网头部 3261、传送级别 2 通道包(标号 250)的第一 IP 数据报本身以及 FCS(“帧校验序列”)字段。

[0134] 通道包 250 具有 4 个部分:

[0135] - 传输协议(即,该示例中的 TCP UDP)的头部字段 251,

[0136] - 封装协议(即,该示例中的 L2TP 或 TLS,具体描述在文献 IETF RFC3931,“Layer two tunneling protocol-version 3(L2TPv3)”,J.Lauand all, March 2005 和文献 IETF RFC2246,“The TLS Protocol Version1.0”中)的头部字段 252,

[0137] - 乘客协议(即,该示例中的以太网)的头部字段 253,以及最后

[0138] - 用户数据字段 254,其自身包括第二 IP 数据报,如果在其从源设备行进期间没有出现分片,则第二 IP 数据报是完整的。

[0139] 现参照图 2b,描述根据本发明的方法的特定实施例由通道端点(例如,图 1a 中的标号 101 所标识的端点)执行的 LAN 出站算法。该附图解释对通过通道 100 发送到其它通

道端点 102 的数据的一般处理。

[0140] 在步骤 1, 侦听网络接口并捕获要去往连接到 LAN B 104 的至少一个设备的 IP 或以太网数据包。这可以通过使用网桥并利用添加到网桥的若干虚拟网络装置 (诸如 TUN/TAP) 来完成。

[0141] 在步骤 2, 判定所述包是否被授权向 LAN B 发送。例如, 从 LANB 接收的包将不会向该相同的 LAN 发送。

[0142] 在步骤 3, 选择最适合的信道, 以用于将数据包发送到 LAN B104。以下, 参照其它附图在此详细描述该步骤 3。

[0143] 在步骤 4 (可选步骤), 可对数据执行加密, 以确保用户数据的私密性。例如, 可使用公知的加密算法 (诸如 AES (高级加密标准)) 来完成所述步骤。

[0144] 在步骤 5, 基于步骤 3 的结果, 利用与在步骤 3 选择的信道相关的封装协议 (也称为隧穿协议) 对所接收的包进行封装。所述封装协议添加特定信息 (头部 (header)), 并可选地能够添加附加数据, 以便提供特别针对通道的功能 (诸如 “保持活动” 机制, 其使得两个通道端点均能够知晓信道是否仍为活动, 即, 是否可进行传输) 的特征。这些附加功能可取决于信道。例如, 可能值得添加附加数据, 以便测量通常没有给出任何 RTT (往返时间) 测量机制的 UDP 信道的 RTT。这可以通过在封装数据中添加对立即响应 (包括标识符) 的请求来实现。当远程通道头部接收到这种请求时, 其立即做出响应。当接收到所述响应时, 本地通道头部可随后确定 RTT。这种机制自然不需要在已经实现 RTT 评估机制的信道中 (例如, 这是基于 TCP 的信道的情况) 实现 (Cf. “TCP/IP illustrated, Volumes 1, 2 and 3”, Stevens, Wright, Addison-Wesley, 1994, 1995 and 1996)。

[0145] 在步骤 6, 在步骤 3 中选择的信道上发送通过封装产生的包。这可以通过将数据写到被配置成在通道上发送数据的连接接口 (套接字) 来完成。在这一步骤之后, 所述包将最终具有图 2a 的标号 250 所标识的包的形状。该步骤还更新信道统计 (重传、发送的数据类型等)。

[0146] 参照图 2c, 描述根据本发明的方法的特定实施例由通道端点 (例如, 图 1a 中的标号 102 所标识的端点) 在 LAN 上执行的入站算法。该附图解释了来自其它通道端点 101 并通过通道 100 接收的数据的整个处理。

[0147] 在步骤 7, 侦听与每个信道相应的每个特定连接接口 (套接字), 以接收包。

[0148] 在步骤 8, 更新关于在其上进行接收的信道的网络质量 (重传、RTT、PER、拥塞等) 的信息。

[0149] 在步骤 9, 使用解密算法以及与步骤 4 所使用的密钥兼容的相关密钥来对净荷数据进行解密 (如果已经执行过图 2b 的步骤 4)。

[0150] 在步骤 10, 将数据包进行解封装, 以取回原始数据包 (由通道端点 101 在 LAN A 103 上最初所捕获的)。在这一步骤中, 如果还存在与可选附加机制相关的任何附加数据, 则还处理附加数据 (参照图 5 的描述)。

[0151] 在步骤 11, 判定通过解封装得到的包是否是被允许的。例如, 解密或解封装没有给出令人满意的结果的包将不会被授权在 LAN A 上传输, 从而不会扰乱连接到所述 LAN 的设备的工作。

[0152] 在步骤 12, 信道统计 (关于带宽、被发送数据的类型等) 被更新。

[0153] 在步骤 13, 在 LAN B 104 上发送通过解封装得到的包。这可以通过使用诸如 TUN/TAP 的虚拟网络装置来实现。

[0154] 以下在此参照图 3 来描述根据本发明的方法的特定实施例来选择有效信道的算法(图 2b 的步骤 3 的细节)。

[0155] 在步骤 31 分析从步骤 2(图 2b)接收的包, 以便确定其是否是 IP 包(因为在该实施例中, 只考虑 IP 包)。这通过分析包的内容来实现(LLC 头部等)。如果其不是 IP 包, 则处理进行到选择默认信道的步骤 37。该默认信道可由用户来确定, 例如, 其为 TCP 信道。如果其是 IP 包, 则操作进行到步骤 32。

[0156] 在该步骤 32 中, 对包进行分类(提取关于随后将用于选择最优信道的包的所有信息)。通常, 为了根据包净荷数据确定包类型(分类的结果), 确定净荷数据传输协议(IP 上的传输协议), 该信息在 IP 头部的 8 个保留比特中被编码。这里, 在以下的描述中, 将净荷数据传输协议用作包类型(TCP、UDP、SCTP、DCCP 等)的标识符。

[0157] 在步骤 33, 确定在步骤 32 确定的包类型是否由下面的步骤 35 来管理。如果不是, 则操作进行步骤 37。如果答案为“是”, 则操作进行步骤 34。

[0158] 例如, 在此讨论的特定实施例中, TCP 和 UDP 是通过下面的步骤 35 管理的乘客协议。对于其它乘客协议, 在步骤 37 选择默认信道。例如, 所述协议为: 传输协议, 如 DCCP(数据报拥塞控制协议, “Datagram Congestion Control Protocol”)或 SCTP(流控制传输协议 “Stream Control Transmission Protocol”); 或资源保留协议, 如 RSVP(资源保留协议, “Resource Reservation Protocol”); 以及非层 4(在 ISO 模型中)协议, 诸如 ICMP(因特网控制消息协议, “Internet Control Message Protocol”)或 IGMP(因特网群组多播协议, “Internet Group Multicast Protocol”)。因此, 利用单个信道在通道中发送所述类型的乘客协议的包。对于非 IP 包, 默认信道可由用户来设置或可包括预设的默认值; 可注意到: 将 TCP 信道定义为用于上述乘客协议(不由步骤 35 管理)的默认信道允许应用保留策略。

[0159] 在步骤 34, 确定 QoE(“试验质量”)。为此, 涉及网络质量(拥塞、PER、带宽、RTT、重传率等)的所有数据被取回。每当包通过通道被发送或接收时, 所有上述数据被评估(步骤 8、12、384 和 387)。

[0160] 在步骤 35, 确定优选信道(并因此确定优选传输协议), 优选信道被用于尽可能有效地将净荷数据发送到远程 LAN。信道可仅仅由它的传输协议来表征, 但是可使用其它特征, 例如, TOS(服务类型)参数。作为示例, 以下给出用于确定优选信道的三种可行策略(分别在图 4、图 5 和图 6 中的步骤 35a、35b 和 35c)。

[0161] 在步骤 36, 确定用于被处理的包(以下称为“被处理包”)的类型的传输模式。传输模式相应于管理给定类型的包的传输的方式。该模式可以是稳定的(例如, TCP 或 UDP)或过渡(例如, TCP 到 UDP 或 UDP 到 TCP)的。

[0162] 在图 7a、图 8a 和图 8b 中示出步骤 36 的可能实现方式。在该实现方式中, 我们考虑由其传输协议表征的信道的情况(与图 4、图 5 和图 6 兼容)。根据优选传输协议以及用于被处理包的类型的当前传输模式, 在步骤 36, 对于每种包类型(在步骤 32 确定的类型), 传输模式的进展被管理(在四种可行模式: 两种稳定模式 TCP 和 UDP, 两种过渡模式 TCP 到 UDP 以及 UDP 到 TCP)。例如, 如果在步骤 35 确定为 UDP 类型的包, 也称为 UDP 包(即, UDP 是乘客协议的净荷数据协议的包), 优选传输协议是 TCP(即, 优选信道是 TCP 信道), 但

是 UDP 包的当前传输模式是 UDP 模式,而在步骤 36,进入过渡 UDP 到 TCP 模式,用于被处理包的有效传输信道可以是优选的 TCP 信道或 UDP 信道(参见以下对图 7a、图 7b、图 8a、图 8b 和图 8c 的详细描述)。

[0163] 在步骤 38,根据当前传输模式的优选信道(参见步骤 35)以及被处理包的类型的传输窗口参数(见以下的描述)来选择有效信道。在图 8c 中示出所述步骤 38 的可能实现方式。对于给定类型的包,这是一种用于从一种传输模式平滑地传递到另一种模式的选择机制。这种机制对于避免通道的“虚假”拥塞很重要。

[0164] 例如,如果一种类型的包的优选传输协议从 UDP 切换到 TCP,则不可能直接在 TCP 信道上发送所有这种类型的包,这是因为:将在该 TCP 信道上发送的包的数量上的突然增加将逐渐导致 TTP 拥塞窗口被超出。结果,即使实际可用带宽足够大,所述包也会被 TCP 堆栈延迟或被缓冲。这些缓冲的包将增加测量的点对点通信的 RTT,并且会在 TCP 包的情况下引起不必要的重传(在 TCP 情况下,随着称为 RTT(“重传时间超时”)的重传超时期满)。

[0165] 在从 TCP 传输模式切换到 UDP 传输模式的情况下,有必要注意 UDP 信道大小的突然增加,这可能突然使得 TCP 传输降速,这也会产生问题。

[0166] 图 4 示出选择信道(即,选择优选传输协议)的优选算法的第一示例(图 3 的步骤 35 中的细分标号 35a)。在该第一示例中,只有 ECN 通知机制被使用。

[0167] 在该第一示例中选择的策略是这样一种策略:只有在不存在网络拥塞的情况下,在 UDP 信道上发送 TCP 包(以防止“TCP 上的 TCP”组合的问题)并在 TCP 信道上发送 UDP 包(以提供与 LAN 上相同的可靠性)。在存在网络拥塞的情况下,在 UDP 信道上发送 UDP 包(以便即使一些包被消除,也保持 UDP 速度)。

[0168] 在步骤 352,确定被处理包的类型,即,用于包含在被处理包中的净荷数据的传输协议。

[0169] 如果包是 TCP 包,则执行步骤 359。在该步骤中,UDP 信道被选择,作为用于被处理包的优选信道。

[0170] 如果包是 UDP 包,则执行步骤 353。在该步骤中,通过 ECN 通知机制确定是否检测到网络拥塞(在步骤 8)。

[0171] 如果没有检测到拥塞,则执行步骤 358。在该步骤中,选择 TCP 信道作为用于被处理包的优选信道。如果检测到拥塞,则执行步骤 359。在该步骤中,UDP 信道被选择作为用于被处理包的优选信道。

[0172] 图 5 示出用于选择优选信道(即,优选传输协议)的算法的第二示例(图 3 中的步骤 35 的细分标号 35b)。在该第二示例中,联合地使用 ECN 通知机制和误包率(PER)。

[0173] 在该第二示例中,在新的步骤 354 中,将网络的 PER 与确定的阈值 Pth(例如,由用户选择)进行比较。

[0174] 在这种情况下,当步骤 353 没有检测到拥塞时,操作进行到步骤 354(而不是如图 4 所示直接执行步骤 358)。

[0175] 在步骤 354 中,如果 PER 高(大于或等于阈值 Pth),但是如果步骤 353 指示不存在拥塞,则为了增加点对点的可靠性而选择 TCP 信道作为用于被处理包的优选信道是有用的。如果不是(如果 PER 低于阈值 Pth),则选择 UDP 信道,作为用于被处理包的优选信道。

[0176] 图 6 示出用于选择优选信道(即,优选传输协议)的算法的第三示例(图 3 的步

骤 35 的细分标号 35c)。在该第三示例中,联合地使用 ECN 通知机制、误包率 (PER) 以及 TCP 信道上的重传率。

[0177] 对于 TCP 包,已知 (参见上述文献“Understanding TCP over TCP(...)”) 通道中的多次重传能够在 TCP 通信中产生从端到端的重传,从而产生不必要的重传。为了防止这种情况,以上建议 (参见图 4 和图 5) 在 UDP 信道上发送 TCP 包。然而,为了确保通道的可靠性而允许通道重传包是有用的。为了实现这一目的,该第三示例考虑在 TCP 信道上进行重传。如果在 TCP 信道上的重传率低于阈值 R_{th} (例如,10%),则值得在 TCP 信道上发送 TCP 包。如果 TCP 信道上的重传率大于或等于阈值 R_{th} ,则在 UDP 信道上发送 TCP 包。

[0178] 因此,与图 5 相比,存在附加步骤 357 (在步骤 352 的输出),其中,进行检查以检测在 TCP 信道上的重传率是否低于阈值 R_{th} 。如果响应为“是”,则操作进行到步骤 358,其中, TCP 信道被选择,作为用于被处理包的优选信道。如果答案为“否”,则操作进行到步骤 359,其中, UDP 信道被选择,作为用于被处理包的优选信道。

[0179] 参照图 7a,我们现在提出根据本发明的方法的特定实施例的用于管理当前传输模式以及用于包类型的传输窗口的算法 (参见图 3 中的步骤 36 的细节)。

[0180] 因此,对于每种包类型,我们管理传输模式以及两个传输窗口 (通道的每个传输信道有一个传输窗口)。通过一组参数来定义与给定信道相关的传输窗口 (见图 7b),所述参数用于定义能够在确定的持续时间期间 (相应于 RTT) 在给定信道上发送的数据的最大数量。对于给定类型的包,根据传输的模式,所述两个窗口将增加或减小,以便平滑地从一个信道切换到另一个信道。

[0181] 可回想到的:在图 3 的分类步骤 32 期间确定正在被处理的包 (或被处理包) 的类型。

[0182] 该示例考虑两种类型的包:TCP 包或 UDP 包。对于所述两种类型的包中的每一种,一种传输模式以及两个传输窗口被管理。所述传输窗口以下称为“TCP 传输窗口”和“UDP 传输窗口”。

[0183] 重要的是要注意到:下面针对具有给定类型的包来描述图 7a,因此,每当提到传输模式或窗口参数 (W_{tcp} 、 S_{tcp} 、 W_{tcp_max} 、 W_{udp} 、 S_{udp} 、 W_{udp_max}) 时,必须理解:这是属于适合所述给定的包类型的一组变量的传输模式或窗口参数 (参见图 7b)。这同样适用于以下描述的图 8a、图 8b 和图 8c。

[0184] 对于具有给定类型的被处理包,在步骤 35 (图 3) 确定优选传输信道之后到达步骤 360 (例如,根据图 4、图 5 和图 6 的三种策略之一来实现)。

[0185] 在步骤 360,根据优选信道来实现切换:如果优选信道是 TCP 信道 (即,如果优选传输协议是 TCP),则操作进行到步骤 361,或者如果优选信道是 UDP 信道 (即,如果优选传输协议是 UDP),则操作进行到步骤 362。

[0186] 在步骤 362 (优选信道是 UDP 信道的情况),根据当前传输模式 (对于被处理包的类型),实现切换。

[0187] 如果在步骤 362,当前模式是稳定 TCP 模式 (与作为 TCP 信道的在先优选信道相关),则系统必须进入过渡 TCP 到 UDP 模式,其在步骤 263 建立。首先,方法进行到步骤 369,其中,对于被处理包的类型初始化窗口参数:

[0188] - 将对于被处理包的类型已经在 UDP 信道上发送的数据的数量 (S_{udp}) 设置为

0 (Sudp = 0)

[0189] - 将 UDP 窗口的大小 (Wudp) (能够在 UDP 信道上发送的数据的最大数量) 设置为 TCP 上的 TCP 信道连接的最大分段大小 (MSS) (Wudp = MSS) ;

[0190] - 将相应于 TCP 窗口的最大大小的停止条件 (Wudp_max) 设置为 TCP 拥塞窗口的当前值 (Cwnd) (Wudp_max = Cwnd)。所述停止条件将确定过渡 TCP 到 UDP 模式的输出。

[0191] 如果在步骤 362, 当前模式是过渡 UDP 到 TCP 模式 (与作为 TCP 信道的优选在先信道相关), 所述系统在这里也必须进入在步骤 263 建立的过渡 TCP 到 UDP 模式。可对于被处理包的类型, 保存已经重置的窗口参数 (参见图 8a)。

[0192] 在步骤 362, 如果当前模式是稳定 UDP 模式 (与作为 UDP 信道的在先优选信道相关) 或过渡 TCP 到 UDP 模式 (与作为 UDP 信道的优选在先信道相关), 则不需要动作。

[0193] 在步骤 363 之后, 操作进行到步骤 366, 其中, 发起执行用于管理过渡 TCP 到 UDP 模式的算法 (以下将参照图 8b 来描述)。在所述发起操作之后, 操作进行到图 3 的步骤 38。

[0194] 在步骤 361 (优选信道是 TCP 信道的情况), 根据当前传输模式 (对于被处理包的类型), 完成切换。

[0195] 在步骤 361, 如果当前模式是稳定 UDP 模式 (与作为 UDP 信道的在先优选信道相关), 系统必须进入在步骤 364 建立的过渡 UDP 到 TCP 模式。首先, 操作进入到步骤 268, 其中, 用于被处理包的类型的窗口参数被初始化:

[0196] - 将对于被处理包的类型已经在 TCP 信道上发送的数据的数量 (Stcp) 设置为 0 (Stcp = 0) ;

[0197] - 将 TCP 窗口的大小 (Wtcp) (能够在 TCP 信道上发送的数据的最大数量) 设置为当前 TCP 拥塞窗口的大小 (Cwnd) (Wtcp = Cwnd)。因此, 在最初, 两个窗口 (Wtcp 和 Cwnd) 具有同样的大小;

[0198] - 将与 TCP 窗口的最大大小相应的停止条件 (Wtcp_max) 设置为 UDP 窗口的当前值 (Wudp)。该停止条件将确定过渡 UDP 到 TCP 模式的输出。

[0199] 如果在步骤 361, 当前模式是过渡 TCP 到 UDP 模式 (与作为 UDP 信道的在先优选信道相关), 则系统在此也必须进入在步骤 364 建立的过渡 UDP 到 TCP 模式。对于被处理包的类型, 可保存已经初始化的窗口参数 (参见图 8b)。

[0200] 如果在步骤 361, 当前模式是稳定 TCP 模式 (与作为 TCP 信道的在先优选信道相关) 或过渡 UDP 到 TCP 模式 (与作为 TCP 信道的在先优选信道相关), 则不需要动作。

[0201] 在步骤 364 之后, 操作进行到步骤 365, 以发起执行用于管理过渡 UDP 到 TCP 模式的算法 (以下将参照图 8a 来描述)。在所述发起处理之后, 操作进行到图 3 的步骤 38。

[0202] 图 7b 提供根据本发明的方法的特定实施例的包类型的表。该表 4000 指示将对于每种类型的包而考虑的变量集合。

[0203] 更具体地说, 表 4000 对于每种包类型 (例如, TCP 包或 UDP 包) 包含一行。列 4002 指示用于这种包类型的当前传输模式。列 4003 到 4005 给出对于这种包类型定义 TCP 传输窗口的变量 (分别在以上讨论过的 Wtcp、Stcp 和 Wtcp_max) 的值。列 4006 到 4008 给出定义 UDP 传输窗口的变量 (分别在以上讨论过的 Wudp、Sudp 和 Wudp_max) 的值。

[0204] 两个附加变量 Nudp_tcp 和 Ntcp_udp 总是提供关于分别在过渡 UDP 到 TCP 模式以及 TCP 到 UDP 模式中的包类型的数量的知识。这两个变量对于确定增加传输窗口的步长

(step) 很重要 (参见图 8a 和图 8b 中的步骤 3654 和 3664)。实际上,在过渡 UDP 到 TCP 模式下的传输窗口以及在过渡 TCP 到 UDP 模式下的传输窗口分别为了遵循拥塞窗口的大小 (Cwnd) 的自然进展而进行的进展必须考虑由被考虑的过渡模式所考虑的所有包类型。如果没有考虑,如果独立地考虑所述包类型中的每一种,则在过渡 UDP 到 TCP 模式下的传输窗口以及在 TCP 到 UDP 模式下的传输窗口分别进行的进展将不会遵循拥塞窗口的大小 (Cwnd) 的自然进展,将存在超出在过渡 UDP 到 TCP 模式下可由 TCP 传输协议接受的数据量以及在过渡 TCP 到 UDP 模式下可由 UDP 传输协议接受的数据量的阈值的风险。

[0205] 图 8a 提出根据依照本发明的方法的特定实施例的用于管理过渡 UDP 到 TCP 模式的算法。

[0206] 该附图描述:对于给定的包,TCP 和 UDP 传输窗口(对于所述给定包类型)的参数演变(develop),以实现从稳定 UDP 传输模式到稳定 TCP 传输模式的平滑切换的方式。

[0207] 为了避免由于与所述大小 (Cwnd) 相比在 TCP 信道上发送过多数量的包而引起的问题,本发明考虑在 TCP 信道中计划的机制,以防止拥塞,并且, TCP(虚拟)传输窗口的大小 (Wtcp) 被增加,以匹配拥塞窗口的大小 (Cwnd) 的自然进展。

[0208] 在步骤 3659,将 UDP 到 TCP 模式下包类型的数量 (Nudp_tcp) 增加一个单位。

[0209] 然后,为了管理 TCP 传输窗口的大小 (Wtcp),在步骤 3651 发起超时(相应于 TCP 信道的 RTT,每当接收到包时被更新,参见步骤 12),在步骤 3652,等待所述超时的期满。

[0210] 同时(在步骤 3651 与 3652 之间),与步骤 38 相兼容地发送包(对于每个包执行一次步骤 38)。

[0211] 在超时过期之后,在步骤 3653 执行测试,以查出传输模式是否已经改变(在步骤 35 对优选信道进行修改之后,可在步骤 36 判定将传输模式从过渡 UDP 到 TCP 模式改变到过渡 TCP 到 UDP 模式)。

[0212] 如果传输模式已经改变,则操作在结束之前进行到步骤 3657,其中,UDP 到 TCP 模式下的包类型的数量 (Nudp_tcp) 被减少。

[0213] 如果传输模式尚未改变,则算法运行,以继续管理 TCP(虚拟)传输窗口的进展。操作进行到步骤 3654,其中, TCP 传输窗口的大小 (Wtcp) 增加 $MSS/Nudp_tcp$ 。因此,在避免拥塞并考虑包的 Nudp_tcp 类型同时处于过渡 UDP 到 TCP 模式的情况时遵循 TCP 拥塞窗口的大小 (Cwnd) 的最大发展。此外,在步骤 3654,将在最后的 RTT 期间,对于被处理包的类型已经在 TCP 信道上发送的数据的量 (Step) 设置为 0 ($Step = 0$)。

[0214] 在步骤 3655,确定过渡 UDP 到 TCP 模式下的过渡阶段是否已经结束。为此,进行检查,以查看 TCP 传输窗口的大小 (Wtcp) 是否已经充分地增加 ($Wtcp > Wtcp_max$?),以及对于被处理包的类型,是否不再有在 UDP 信道上发送的任何数据 ($Sudp = 0$?)。

[0215] 如果过渡阶段已经结束,则操作进行到步骤 3656,其中,稳定 TCP 模式被建立。然后,在结束之前,操作进行到步骤 3657,其中,在 UDP 到 TCP 模式下的包类型的数量 (Nudp_tcp) 被减少。

[0216] 如果过渡阶段没有结束,则操作进行到步骤 3658,其中,将对于被处理包的类型已经在 UDP 信道上发送的数据的量 ($Sudp = 0$) 设置为 0。然后,操作返回步骤 3651,并且发起新的超时。

[0217] 图 8b 示出根据本发明特定实施例的用于管理过渡 TCP 到 UDP 模式的算法。

[0218] 该附图描述：对于给定包类型，TCP 和 UDP 传输窗口（对于所述给定包类型）的参数如何发展来实现从稳定 TCP 传输模式到稳定 UDP 传输模式的平滑切换。

[0219] 管理 UDP 传输窗口的所述机制类似于以上对于 TCP 传输窗口参照图 8a 描述的机制。UDP 传输窗口的大小 (Wudp) 指示在持续时间 RTTu 能够在 UDP 信道上发送的数据的最大量。所述持续时间 RTTu 是由系统计算的值，并相应于对于 TCP 描述的往返时间（该值可通过周期性地将特定控制请求从一个通道端点发送到另一通道端点来计算，所述另一通道端点立即遵照所述请求进行动作）。

[0220] 为了避免由于在 UDP 信道上发送过多数量的包（在 TCP 信道已经完成对它的缓冲器的清空之前）而引起的拥塞，不可突然从完全的 TCP 传输切换到完全的 UDP 传输。因此，使用图 8B 的机制（与图 8a 类似）。

[0221] 在步骤 3669，因此，将 TCP 到 UDP 模式下包类型的数量 (Ntcp_udp) 增加一个单位。

[0222] 然后，为了管理 UDP 传输窗口的大小 (Wudp)，在步骤 3661 发起超时（相应于上述 RTTu），在步骤 3662，等待所述超时期满。

[0223] 同时（在步骤 3661 与 3662 之间），与步骤 38 相兼容地发送包（对于每个包执行一次步骤 38）。

[0224] 在超时过期之后，在步骤 3663 执行测试，以查出传输模式是否已经改变（在步骤 35 对优选信道进行修改之后，可在步骤 36 确定将传输模式从过渡 TCP 到 UDP 模式改变到过渡 UDP 到 TCP 模式）。

[0225] 如果传输模式已经改变，则操作在结束之前进行到步骤 3667，其中，TCP 到 UDP 模式下的包类型的数量 (Ntcp_udp) 被减少。

[0226] 如果传输模式尚未改变，则算法运行，以继续管理 UDP（虚拟）传输窗口的进展。操作进行到步骤 3664，其中，UDP 传输窗口的大小 (Wudp) 增加 $MSS/Ntcp_udp$ 。此外，在步骤 3654，将在最后的 RTT 期间对于被处理包的类型已经在 UDP 信道上发送的数据的量 (Sudp) 设置为 0 ($Sudp = 0$)。

[0227] 在步骤 3665，判定过渡 TCP 到 UDP 模式下的过渡阶段是否已经结束。为此，进行检查，以查看 UDP 传输窗口的大小 (Wudp) 是否已经充分地增加 ($Wudp > Wudp_max$?)，以及对于被处理包的类型，是否不再有在 TCP 信道上发送的数据 ($Stcp = 0$?)

[0228] 如果过渡阶段已经结束，则操作进行到步骤 3666，其中，稳定 UDP 模式被建立。然后，在结束之前，操作进行到步骤 3667，其中，在 TCP 到 UDP 模式下的包类型的数量 (Ntcp_udp) 被减少。

[0229] 如果过渡阶段没有结束，则操作进行到步骤 3668，其中，将对于被处理包的类型已经在 TCP 信道上发送的数据的量 ($Stcp = 0$) 设置为 0。然后，操作返回步骤 3661，并且发起新的超时。

[0230] 现在参照图 8c，我们提出根据本发明的方法的特定实施例的用于对于包类型选择有效信道的算法（图 3 的步骤 38 的细节）。

[0231] 在步骤 380，根据当前传输模式来执行切换（对于被处理包的类型）。

[0232] 如果在步骤 380，当前模式是稳定 TCP 模式，则操作进行到步骤 383，其中，TCP 信道被选择作为有效传输信道，然后进入操作 384，其中，TCP 信道的参数（例如，平均吞吐量、拥塞窗口等）被评估。

[0233] 在步骤 380, 如果当前模式是稳定 UDP 模式, 则操作进行到步骤 386, 其中, UDP 信道被选择作为有效传输信道, 然后进行到步骤 387, 其中, UDP 信道的参数 (例如, 平均吞吐量、拥塞窗口等) 被评估。

[0234] 在步骤 380, 如果当前模式是过渡模式之一 (TCP 到 UDP 或 UDP 到 TCP), 则操作进行到步骤 381, 其中, 确定会向其发送包的信道。为此, 进行检查, 以查看是否已经到达将在优选信道上发送的最大数据数量 (在过渡 UDP 到 TCP 模式的情况下, 确认“ $Stcp > Wtcp_max$ ”; 在 TCP 到 UDP 过渡模式的情况下, 确认“ $Sudp > Wudp_max$ ”)。如果尚未达到最大数量, 则优选信道用于发送被处理包。否则, 在在优先信道发送被处理包。

[0235] 因此, 对于 UDP 到 TCP 模式:

[0236] - 如果对于被处理包的类型, 从步骤 3668 的最后执行 (将 $Stcp$ 复位为 0) 起已经在 TCP 信道上发送的数据数量 ($Stcp$) 大于最大授权值 ($Wtcp_max$) (对步骤 381 的测试的响应为“是”), 则即使优选信道为 TCP 信道, 也将在 UDP 信道上发送被处理包 (在步骤 385 之后, 操作进行到步骤 386 和 387)。在步骤 385, 对于被处理包的类型, 从步骤 3658 的最后执行 ($Sudp$ 的复位) 起已经在 UDP 信道上发送的数据数量 ($Sudp$) 被增加了被处理包的大小 ($Sudp = Sudp + \text{包的大小}$);

[0237] - 如果对于被处理包的类型, 从步骤 3668 的最后执行 ($Stcp$ 的复位) 起已经在 TCP 信道上发送的数据数量 ($Stcp$) 小于或等于最大授权值 ($Wtcp_max$) (对步骤 381 的测试的否定响应), 则将在 TCP 信道上发送被处理包 (在步骤 382 已经执行之后, 操作进行到步骤 383 和 384)。在步骤 382, 对于被处理包已经在 TCP 信道上发送的数据数量 ($Stcp$) 被增加了被处理包的大小 ($Stcp = Stcp + \text{包的大小}$)。

[0238] 对于 TCP 到 UDP 模式:

[0239] - 如果对于被处理包的类型, 从步骤 3658 的最后执行 (将 $Sudp$ 复位) 起已经在 UDP 信道上发送的数据数量 ($Sudp$) 小于或等于最大授权值 ($Wudp_max$) (对步骤 381 的测试的响应为“是”), 则即使优选信道为 TCP 信道, 也将在 UDP 信道上发送被处理包 (在步骤 385 之后, 操作进行到步骤 386 和 387);

[0240] - 如果对于被处理包的类型, 从步骤 3658 的最后执行 ($Sudp$ 的复位) 起已经在 UDP 信道上发送的数据数量 ($Sudp$) 大于最大授权值 ($Wudp_max$) (对步骤 381 的测试的否定响应), 则将在 TCP 信道上发送被处理包 (在步骤 382 已经执行之后, 操作进行到步骤 383 和 384)。

[0241] 图 9 示出被用于实现本发明的技术的通信设备 1000 (图 1a 的通道端点 101 或 102) 的示意性配置。它包括: RAM 1002, 其作为中央处理单元 (CPU) 1001 的主要存储器、工作区等。它的存储容量可通过连接到扩展端口的可选 RAM (未示出) 来扩展。中央处理单元 1001 能够在通信设备被开启时执行程序 1003 的来自 ROM 的指令。在开启之后, 中央处理单元 1001 能够在指令例如已经从程序 ROM 1003 或硬盘驱动器 (HDD) 1006 载之后执行与软件应用程序有关的来自主存储器 1002 的指令。虽然所述软件应用程序由中央处理单元 1001 来执行, 但是其会促使执行图 2b、图 2c、图 3、图 4、图 5、图 6、图 7a、图 8a、图 8b 和图 8c 所示的流程图的全部或部分步骤。

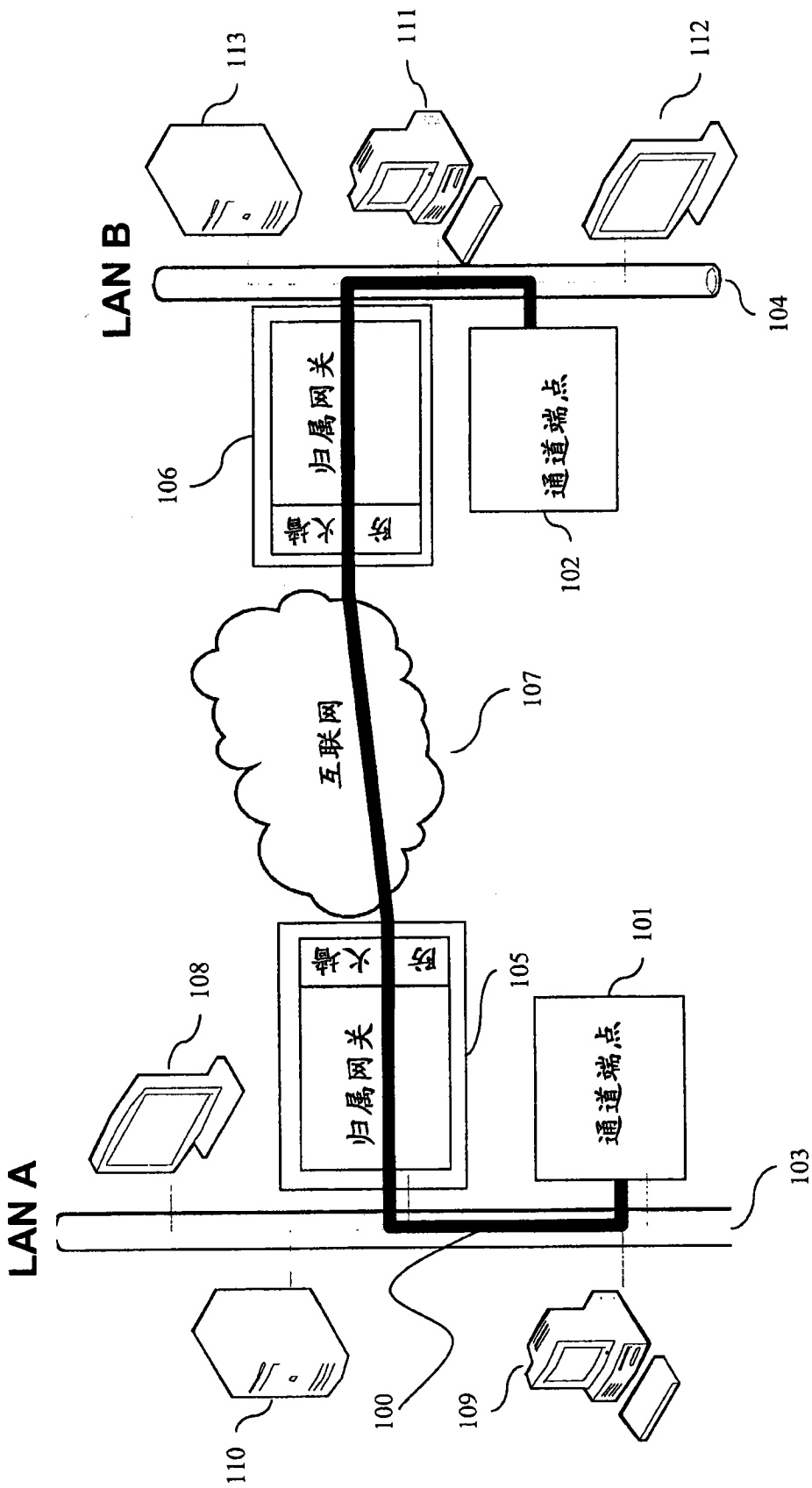


图1a

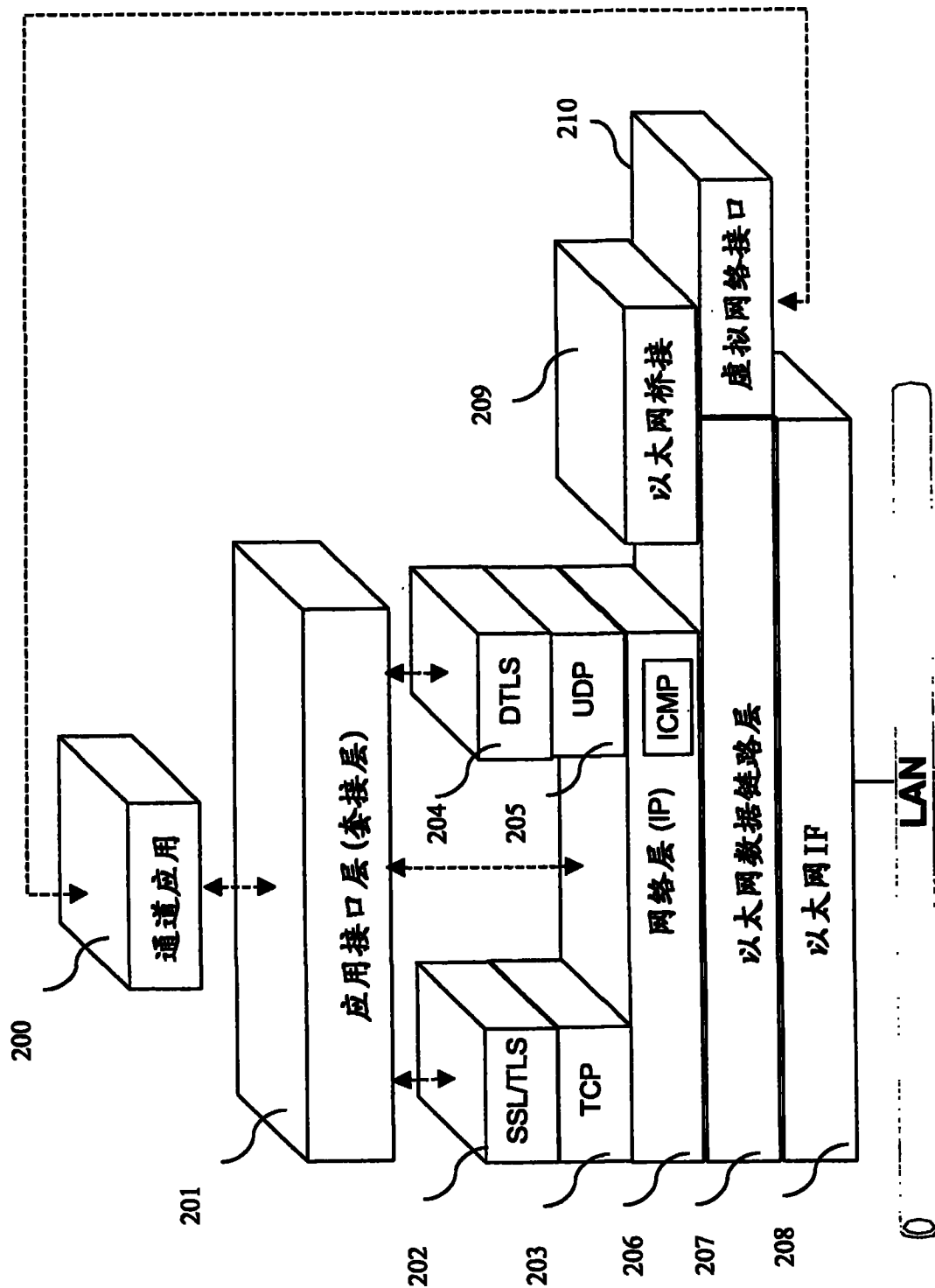


图1b

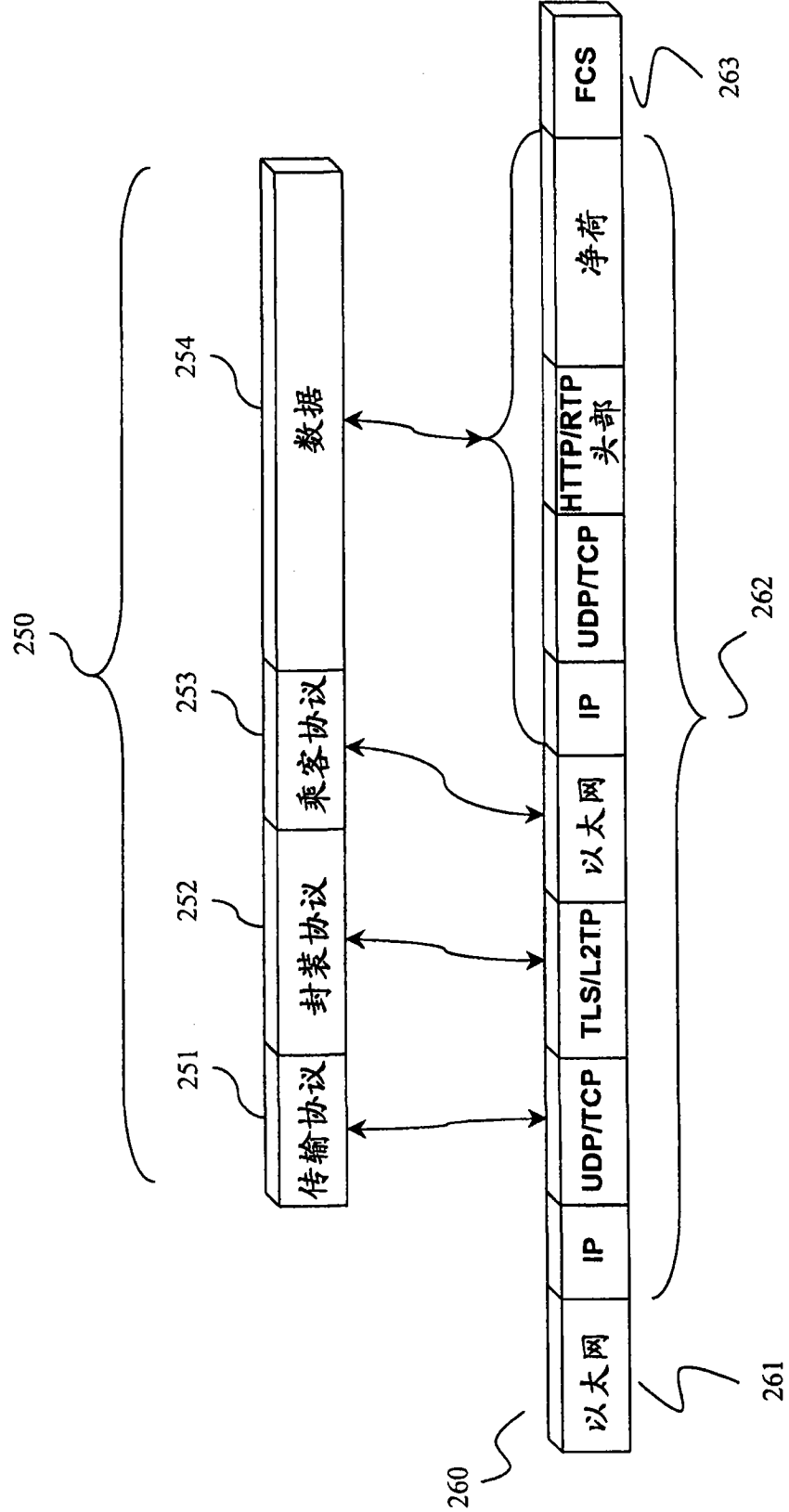


图2a

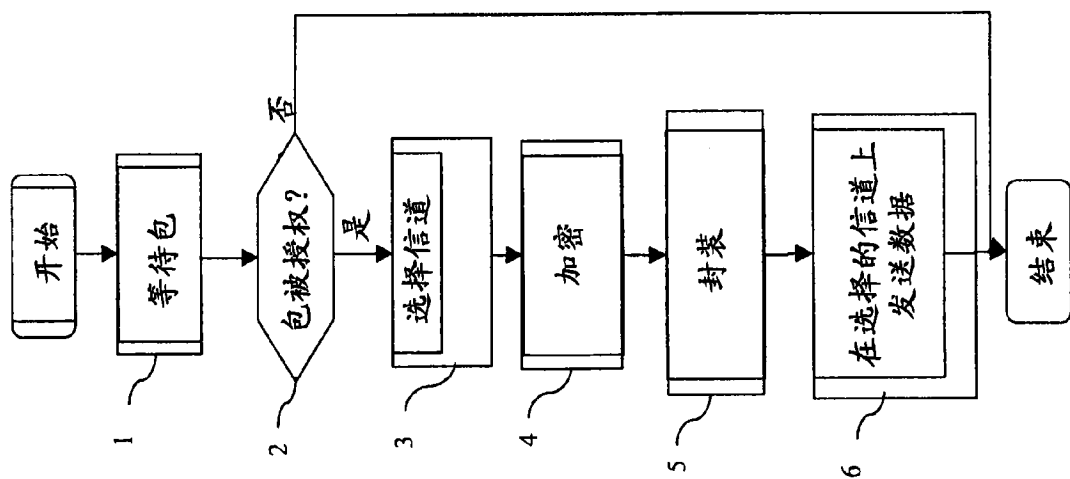


图2b

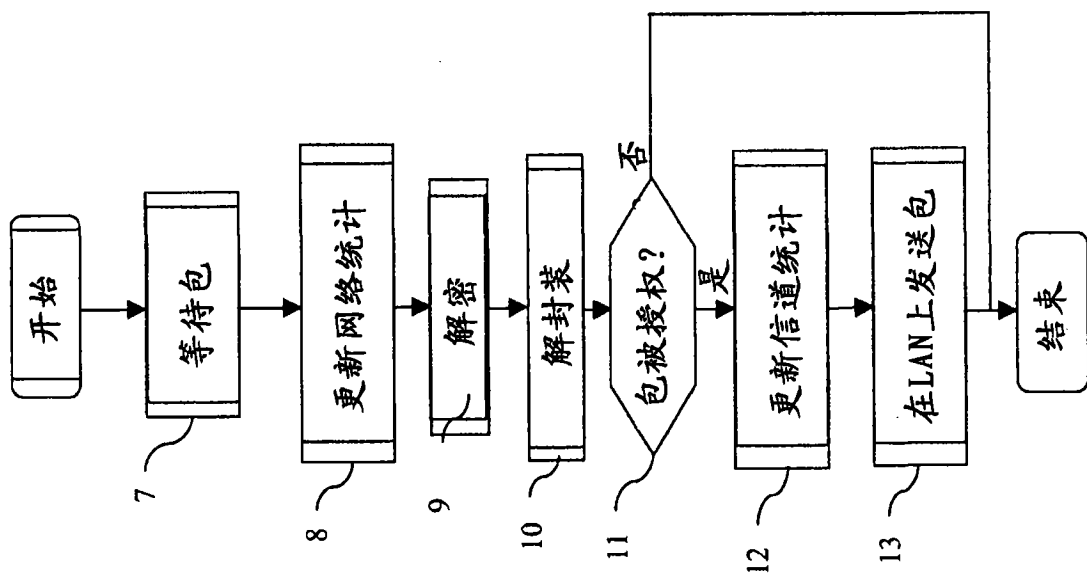


图2c

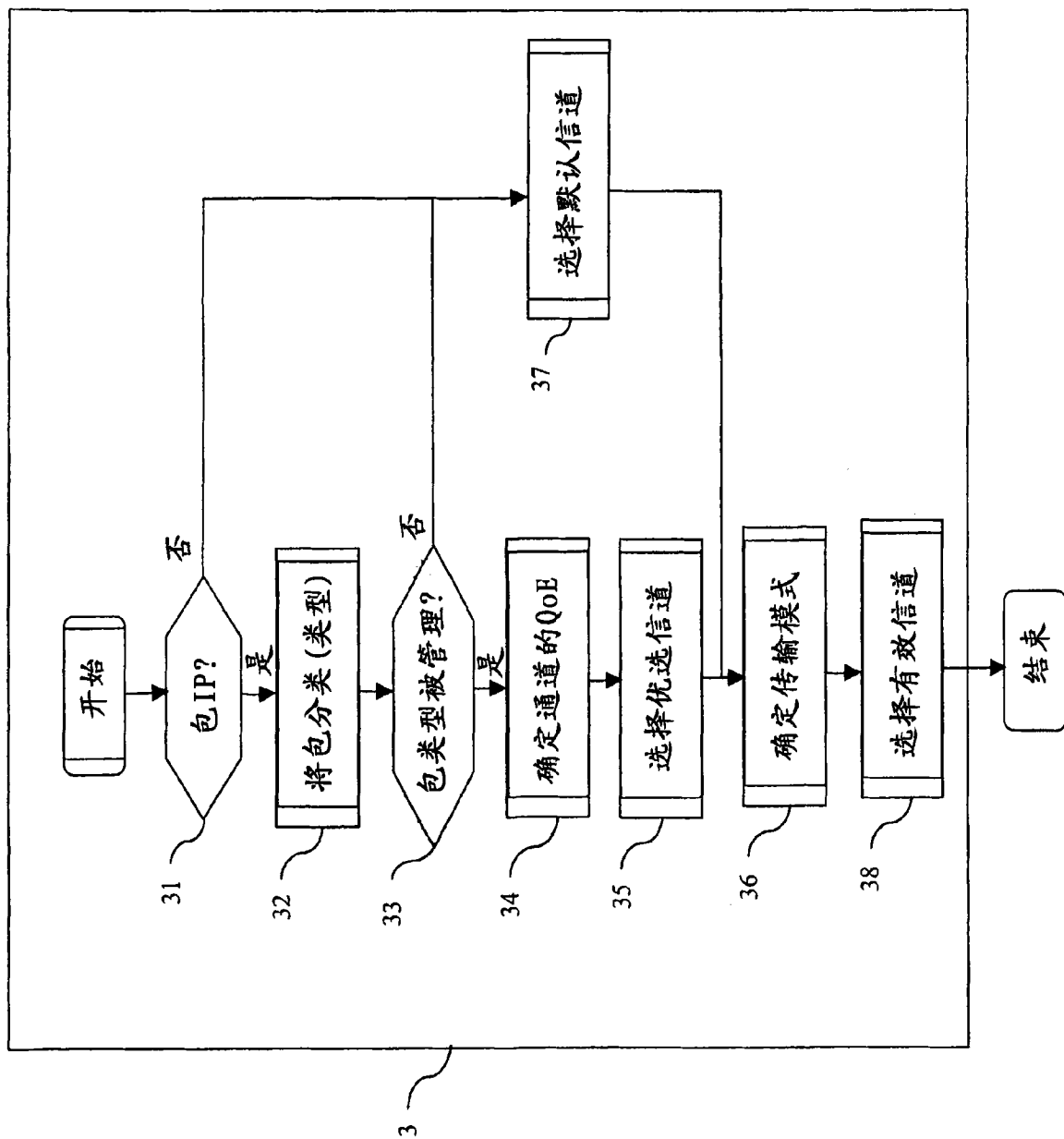


图3

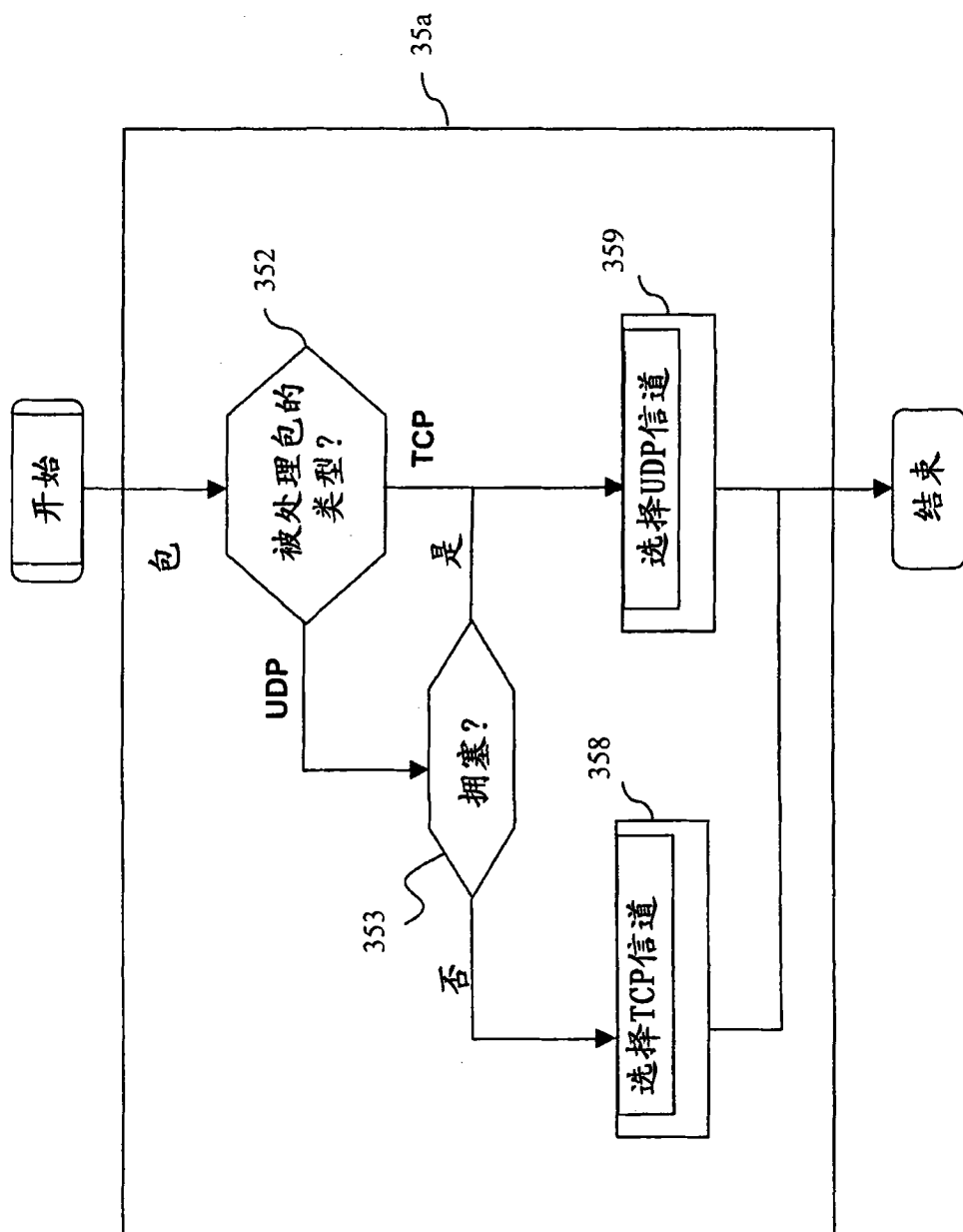


图4

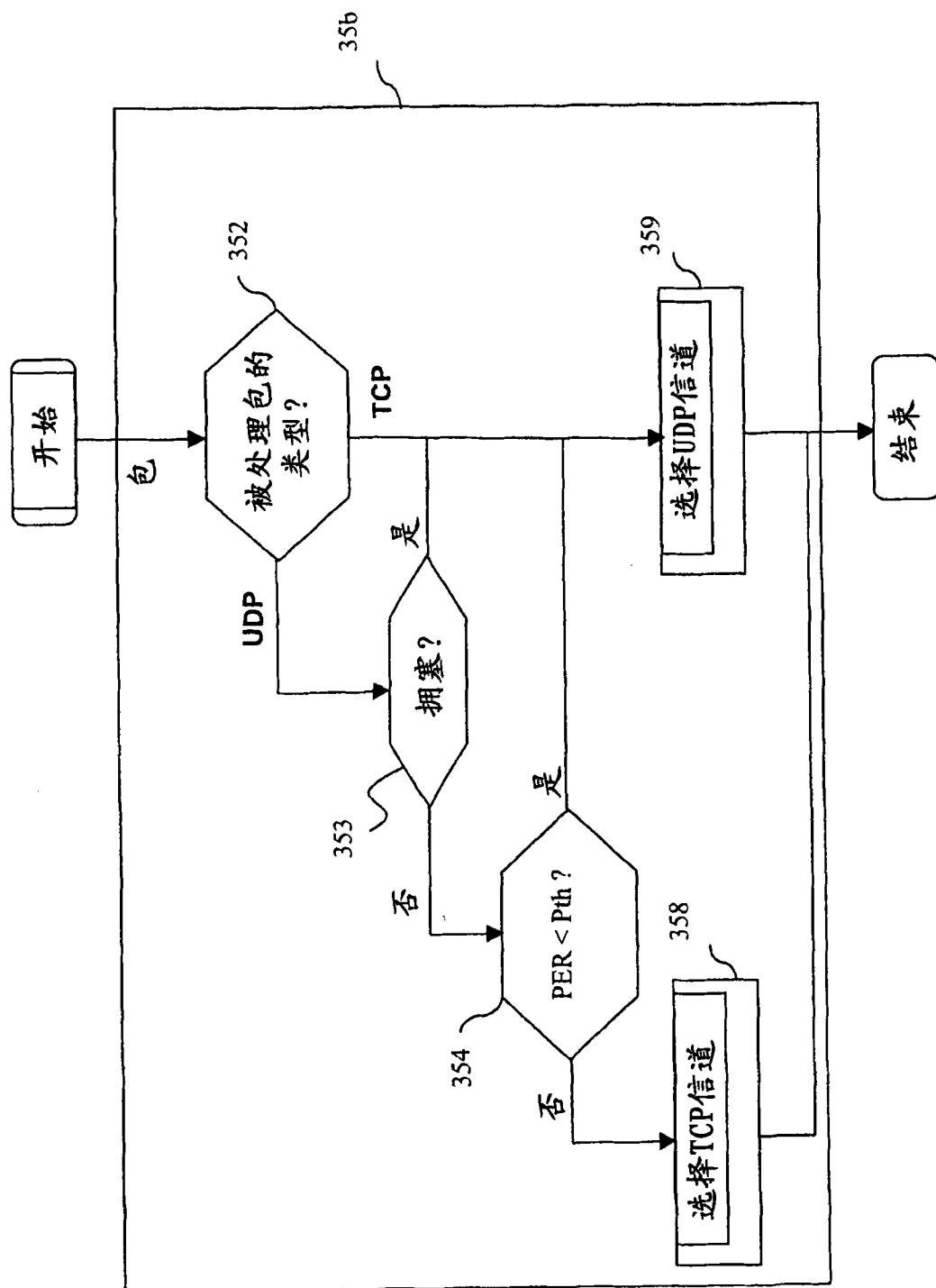


图5

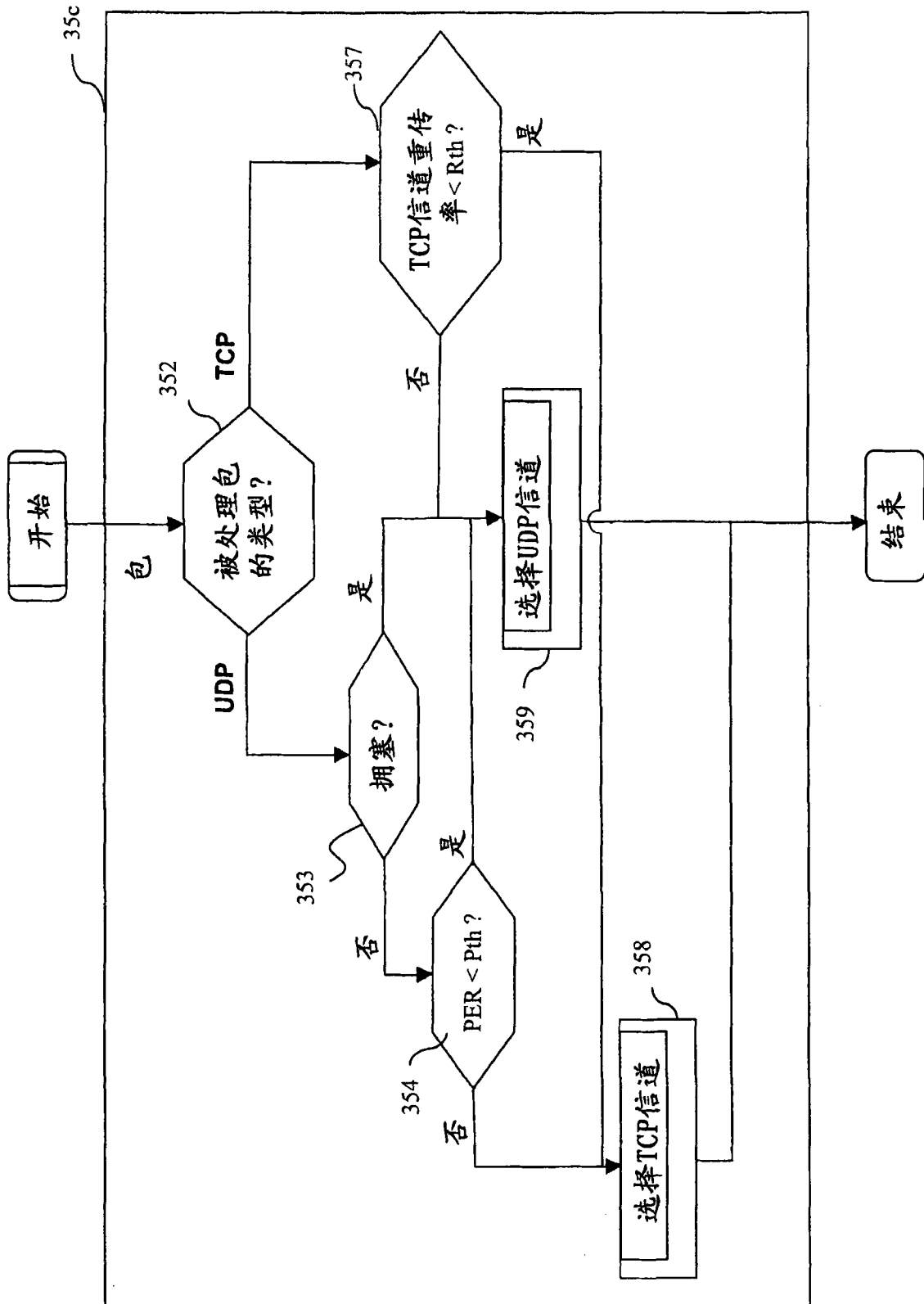


图6

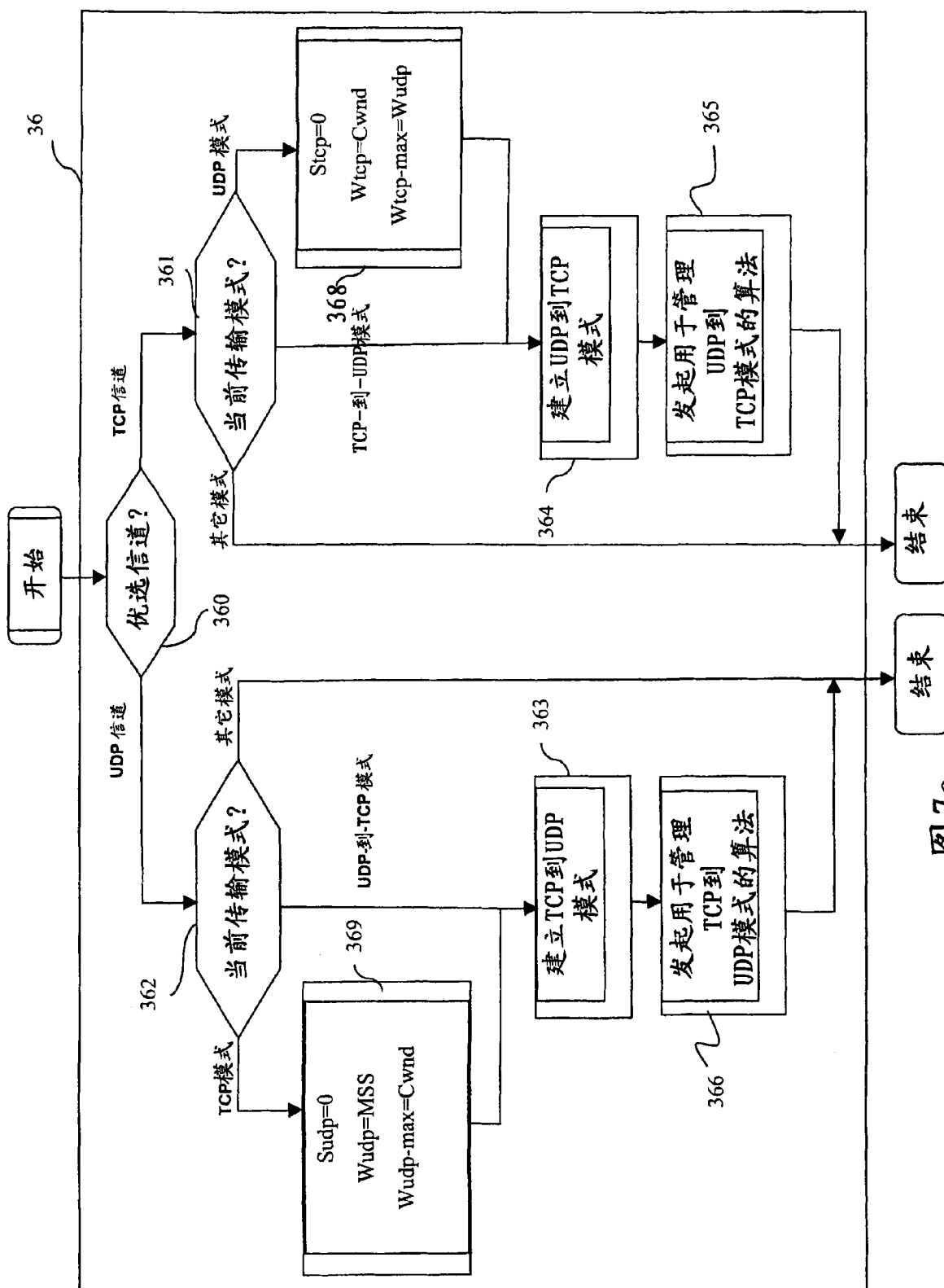


图7a

4001	类型	4002	传输模式	4003	Wtcp	4004	Stcp	4005	Wtcp_max	4006	Wudp	4007	Sudp	4008	Wudp_max
	类型 1		UDP		0		0		0		120000		120000		120000
	类型 2		UDP_to_TCP		1500		300		10000		10000		0		10000
	...														

图 7b

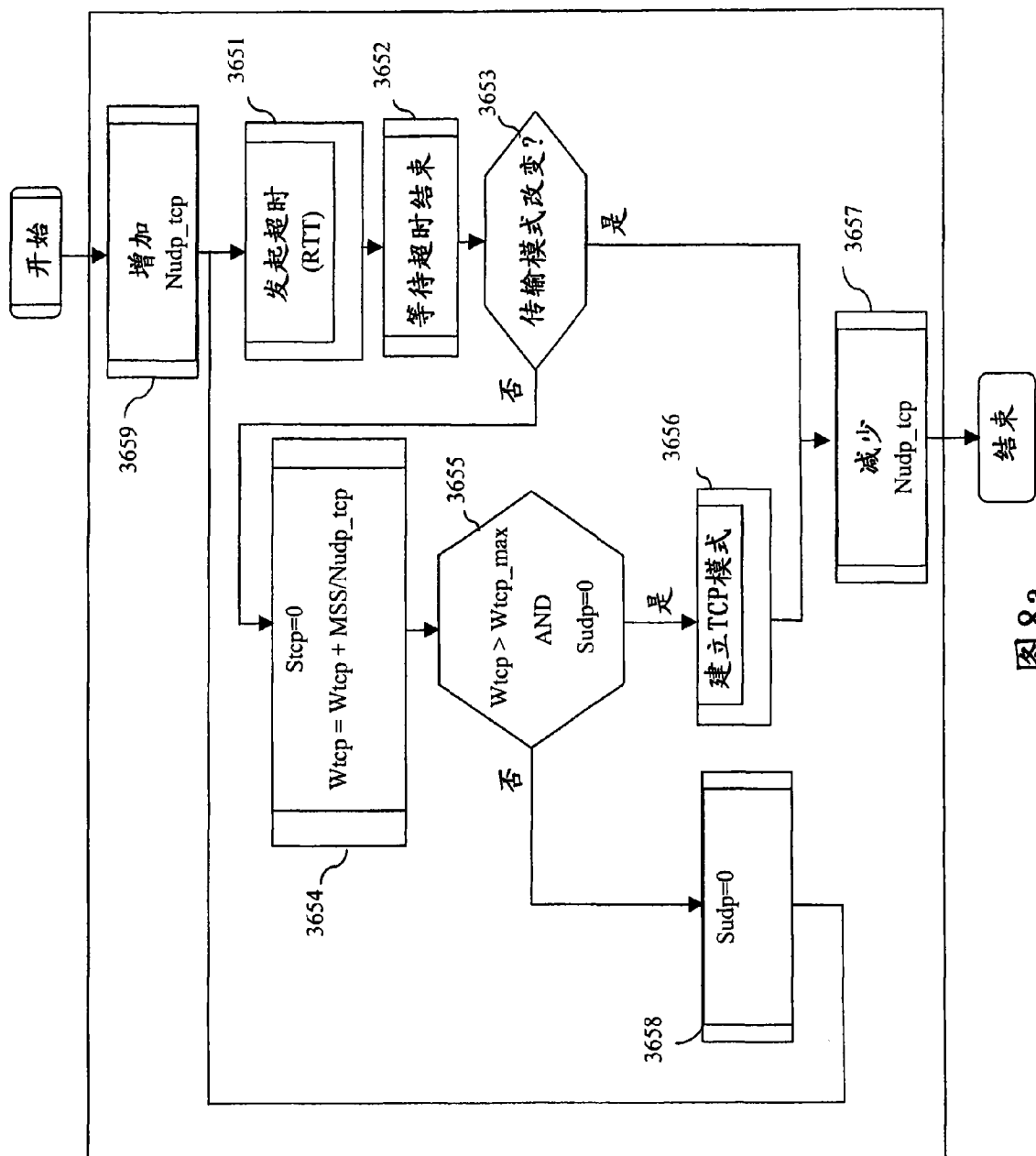


图 8a

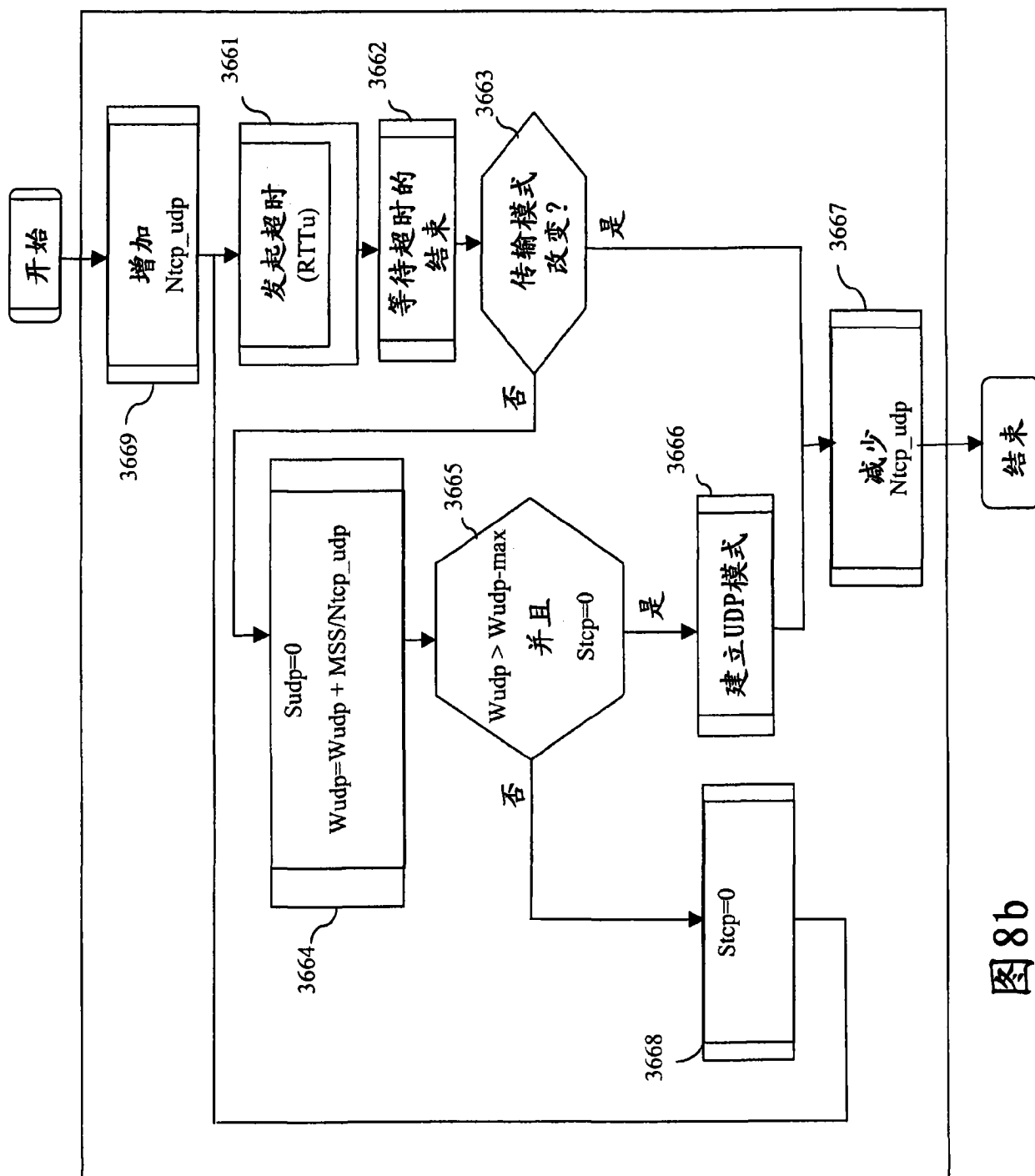


图 8b

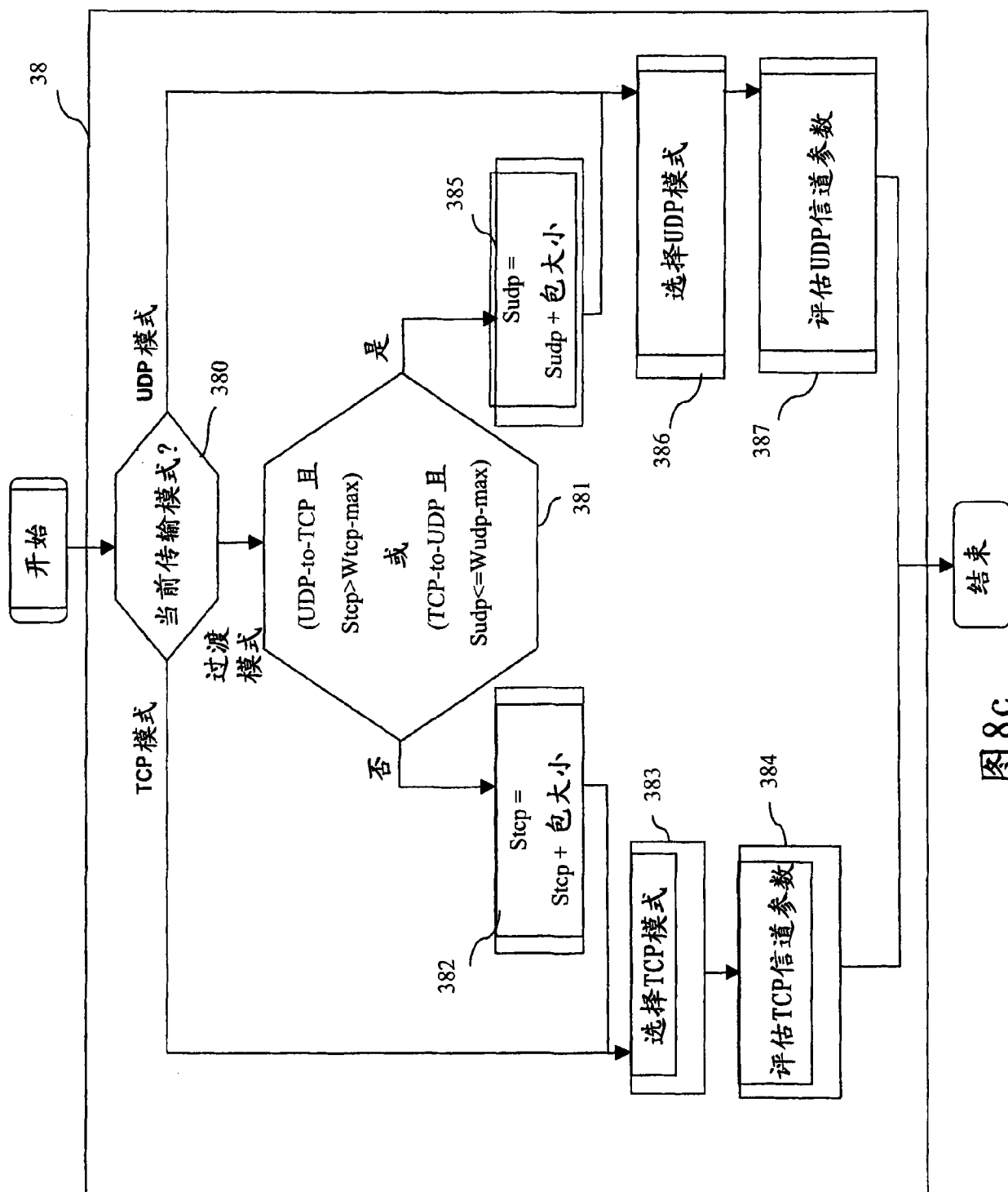


图8c

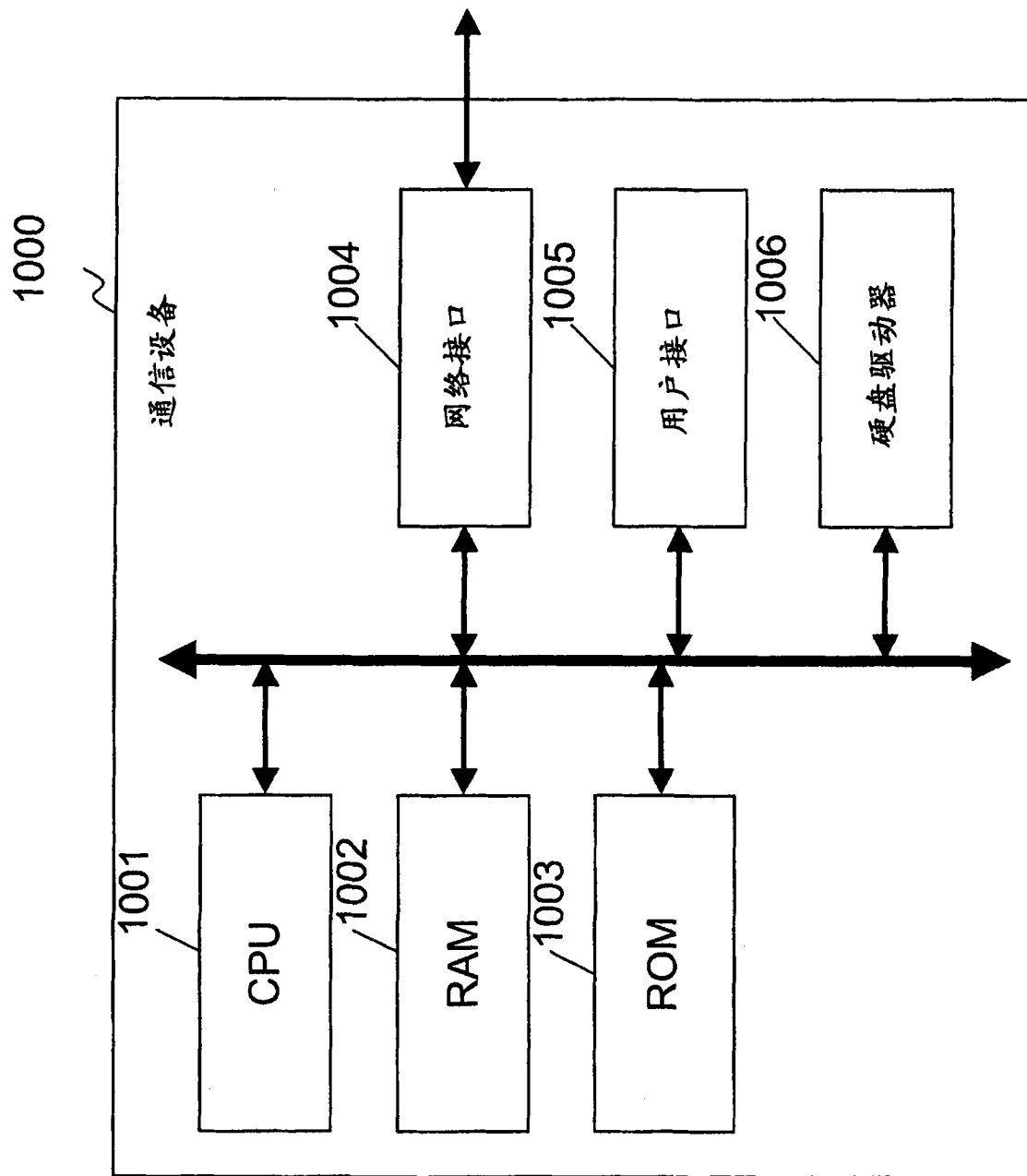


图9