(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 1855874 B
(45)授权公告日 2010.05.26

(21)申请号 200610072475.7

(22)申请日 2006.04.17

(30)优先权数据
11/118,136 2005.04.29 US

(73)专利权人 阿尔卡特公司
地址 法国巴黎市

(72)发明人 葛安 吉里施·奇鲁沃卢
马厄·艾丽

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华

(51)Int.Cl.
H04L 12/46(2006.01)

(56)对比文件
US 2005071672 A1,2005.03.31, 全文.
COLLABORATION.IEEE STD 802.1D-1990 INST..ELECTR. & ELECTRON. ENG., NEW YORK, NY, USA USA (CHAPTER 4).1991,61-72.
RUFFEN T LEN J YANACEK CABLETRONSYSTEMSINCORPORATED D.Cabletron's SecureFast VLAN Operational Model Version1.8
rfc2643.txt.IETF STANDARD, INTERNET ENGINEERING TASK FORCE, IETF, CH.1999,7,18-20,27.
SEAN WHALEN AND MATT BISHOP.Layer 2 Authentication.INTERNET, [Online] http://www.node99.org/projects/l2auth/l2auth.pdf.2005,1-12.
同上. 同上. 同上.

审查员 曹娟

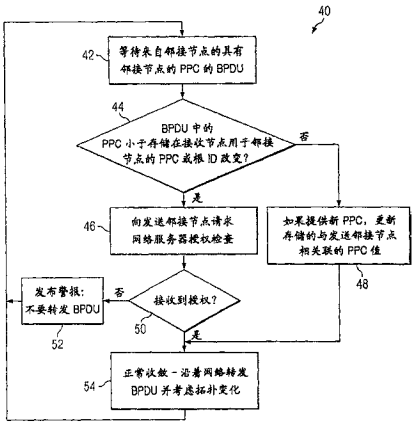
权利要求书 2 页 说明书 11 页 附图 4 页

(54)发明名称

一种桥接网络系统和桥节点

(57)摘要

一种桥接网络系统(10,10')。该系统包含多个桥节点(BRN_x)。多个桥节点的每个桥节点都被连接为与多个节点的至少一个其他邻接桥节点通信。多个桥节点的每个桥节点包含用于和多个节点的另一个桥节点或网络服务器这两者的至少一个进行通信的电路($BP_{y,z}$)。多个桥节点的每个桥节点进一步包含用于存储(邻居跟踪表)从多个节点的另一个桥节点和网络服务器这两者的至少一个接收的邻接桥节点的至少一个生成树参数的电路。



CN 1855874 B

1. 一种桥接网络系统，包括：

多个桥节点；

其中所述多个桥节点的每个桥节点都被连接为与所述多个桥节点的至少一个其他邻接桥节点通信；

其中所述多个桥节点的每个桥节点包括：

用于和所述多个桥节点的另一个桥节点或网络服务器这两者中的至少一个进行通信的电路；以及

用于存储从所述多个桥节点的另一个桥节点和所述网络服务器这两者中的至少一个接收的邻接桥节点的至少一个生成树参数的电路；

其中所述多个桥节点的每个桥节点都被编程为执行如下步骤：

从邻接桥节点端口接收第一控制消息；

响应所述第一控制消息向网络服务器发送消息；

从所述网络服务器接收响应，其中所述响应包括所述邻接桥节点的所述至少一个生成树参数；

将所述邻接桥节点的所述至少一个生成树参数存储在将所述至少一个生成树参数与所述邻接桥节点端口相对应的表中；以及

将所述至少一个生成树参数传送给所述邻接桥节点端口；

其中所述多个桥节点的每个桥节点都被进一步编程为执行如下步骤：

从邻接桥节点端口接收第二控制消息，其中所述第二控制消息包括至少一个规定的生成树参数；以及

将所述至少一个规定的生成树参数与先前存储的与所述邻接桥节点端口相对应的值相比较；以及

其中所述多个桥节点的每个桥节点都被进一步编程为执行，在所述比较步骤并且响应所述比较步骤做出第一判定之后，请求来自所述邻接桥节点的授权检查。

2. 根据权利要求 1 所述的系统，其中所述至少一个生成树参数包含根节点 ID。

3. 根据权利要求 1 所述的系统，其中所述至少一个生成树参数包含一个沿着从所述邻接桥节点到所述多个桥节点的一个选定桥节点的路径传送的代价的效率度量标准。

4. 根据权利要求 3 所述的系统，其中所述选定桥节点包含根节点。

5. 一种桥节点，为了在包括所述桥节点，作为多个桥节点的一个的桥接网络系统中使用，其中所述多个桥节点的每个桥节点都被连接为与所述多个桥节点的至少一个其他邻接桥节点通信，所述桥节点包括：

用于和所述多个桥节点的另一个桥节点或网络服务器这两者中的至少一个进行通信的电路；以及

用于存储从所述多个桥节点的另一个桥节点和所述网络服务器这两者中的至少一个接收的邻接桥节点的至少一个生成树参数的电路；

其中所述桥节点被编程为执行如下步骤：

从邻接桥节点端口接收第一控制消息；

响应所述第一控制消息向网络服务器发送消息；

从所述网络服务器接收响应，其中所述响应包括所述邻接桥节点的所述至少一个生成

树参数；

将所述邻接桥节点的所述至少一个生成树参数存储在将所述至少一个生成树参数与所述邻接桥节点端口相对应的表中；以及

将所述至少一个生成树参数传送给所述邻接桥节点端口；

其中所述桥节点进一步被编程为执行如下步骤：

从邻接桥节点端口接收第二控制消息，其中所述第二控制消息包括至少一个规定的生成树参数；以及

将所述至少一个规定的生成树参数与先前存储的与所述邻接桥节点端口相对应的值相比较；以及

其中所述桥节点被进一步编程为执行，在所述比较步骤并且响应所述比较步骤做出第一判定之后，请求来自所述邻接桥节点的授权检查。

6. 根据权利要求 5 所述的桥节点，其中所述至少一个生成树参数包括从一个集合中选择出来的参数，该集合包括根节点 ID 和沿着从所述邻接桥节点到所述多个桥节点的一个选定桥节点的路径传送的代价的效率度量标准。

一种桥接网络系统和桥节点

技术领域

[0001] 本发明涉及桥接的计算机网络，更具体地专注于探测例如在网络生成树中的某些异常。

背景技术

[0002] 桥接网络由于各种原因在网络产业中的很多应用中得到了偏爱。一个桥接网络通常包括多个节点，其中一些节点是桥节点，它们具有到网络中其他节点的连通性。在网络学习期间，每个桥节点典型地在其全部端口上广播，也就是，该桥节点从其全部端口向外发送相同的消息数据，其中这样的消息数据典型地包括网络拓扑信息。以此方式，当另一个桥节点收到一个包含拓扑信息的消息时，该接收节点不转发该消息；取而代之的是，它比较其到根的距离并决定是否将具有它自己 ID 的这个新信息通知给其他桥节点。因此，该拓扑消息类似于具有适当的本地信息的更新的消息，其中那些更新的消息可以向其他桥节点转发。在以许多消息重复这个过程后，且在各种桥节点之间时，每个桥节点被告知它到其他邻接桥节点的连通性，其中在这个文档中，术语邻居（或邻接）节点用来表示每个都有一个端口直接连接到另一个的两个桥节点。这个连通性信息由每个桥节点在一个或更多相应的表中维护，该表记录在学习过程期间从答复的桥节点接收或得出的信息。除了桥节点，桥接网络包括其他节点，这些节点以不同的名称被提及，例如用户站或客户节点。由于桥节点和客户节点的连通性，一个或更多桥节点将两个或更多客户节点连接到一起，并在客户节点之间转发消息。因此，客户节点与每个其他节点通信，就像它们直接附于同一个物理网络并且对它们之间的桥节点透明。

[0003] 在一个桥接网络内，可以强加一个另外的路由层。作为一个例子，用一个或更多生成树强加这样的路由，上述生成树定义了消息沿其可以在桥接网络中通信的路径。因此，每个生成树强加了一个用于消息沿着该树通信的另外的路由约束层。典型地，强加这样的约束来避免网络消息的环回，就是说，避免同一个消息的多个拷贝到达同一个桥节点，因为否则如果在网络的物理连通性中存在一个环路就会发生。例如，考虑一个桥节点的环，其中每个桥节点连接到另一个桥节点，全部桥节点形成了一个环。如果没有一个另外的约束，如果环中的一个桥节点广播一个消息，假设全部节点沿着该环向前传递该广播消息，那么将会有两个该广播消息的拷贝到达（或“环回”到）该环中的目的节点。一个生成树，然而，定义了作为桥节点之间的路由，并可以在环中实现为仅一个在环上两个桥节点之间的强加的阻塞。因此，当一个和该阻塞相邻的桥节点接收到一个消息时，阻止它在该阻塞的方向上向前发送该消息。结果，仅有一个该广播消息的拷贝可以到达目的节点。

[0004] 作为另外的背景，在先技术包括一个分配给每个桥节点的不同的桥优先级，当在该桥接网络中发生故障（例如，断路）时该优先级影响重新收敛的时间。通常，当发生故障时，在一个被称为是重新收敛的过程中，在生成树中仍旧连接着的桥节点之间通信控制消息。例如，在一个方法中的每个控制消息被称为是一个桥协议数据单元（“BPDU”），它是一个跨越桥节点交换的消息并含有这样的信息，该信息包括端口、地址和优先级，所有这些用

于指引该消息到达正确的目的地。因此，在在先技术中当一个桥节点接收到一个 BPDU 时，该节点可以更新它的表信息，从而在网络配置中做出改变。实际上，一旦完成了重新收敛，基于由在重新收敛期间收到 BPDU 的桥节点所做出的改变建立一个新的生成树。结果，另外的消息可以沿着该新生成树传递，至少到解决了造成该重新收敛的故障为止。

[0005] 作为进一步的背景，BPDU 也典型地包括生成该 BPDU 的桥节点的所谓的端口路径代价（“PPC”）。PPC 是一个沿着从产生该 BPDU 的桥节点的指定端口到该生成树中的“根”桥节点的路径的传输的代价的效率度量标准。这个代价典型地由从所讨论的该端口到该根桥节点的跳距离的值来表示，也就是，所讨论的该端口和该根之间的桥节点的数目。因此，如果所讨论的该端口直接地连接到该根桥节点，那么该跳距离是 1，然而如果所讨论的该端口通过一个中间桥节点连接到该根桥节点，那么该跳距离是 2，等等。同样在这点上，该根桥节点是一个典型地给予控制该生成树的某些级别的节点，例如通过识别该根节点具有该生成树中最高的优先级，以及为了各种检查该生成树的目的，该根节点有权访问一个网络服务器和数据库。

[0006] 作为更进一步的背景，注意在网络学习或重新收敛期间，每个桥节点从网络服务器接收到到根桥节点的桥节点的相应 PPC（或跳距离）。然而，在随后的操作期间，同一个桥节点可以再次从一个邻接桥节点接收到一个 BPDU，其中该邻接桥节点在它自己的 PPC 中指示了一个改变。例如，该邻接桥节点可以向该接收桥节点指示该邻接桥节点已经成为生成树的根，例如通过指示一个为 0 的 PPC。作为响应，因此，该接收桥节点可能改变它自己的配置，在本质上探测到它现在直接连接到根桥节点，由此对于那个现在是根的邻接桥节点给它自己一个为 1 的跳距离。更进一步，那同一个接收桥节点可以传递它自己的 BPDU 到网络中的其他桥节点，通告它们现在察觉的到根桥节点的直接连接，因此可能那些其他桥节点的某些可以关于每个这样的节点的 PPC 依次改变它们自己的网络信息。实际上，该改变的 PPC 可以导致网络生成树配置的全部的改变。

[0007] 虽然上述技术已经在许多应用中证明是有好处的，本发明人已经认识到在上面描述的与某些网络异常类型有关的操作中可以出现缺陷。例如，一个当代计算的不幸事实是用户常常寻求未授权访问计算机，以及这样的用户被认为尝试在网络环境中进行“欺骗”，就是说，连接到网络并且使他们的站提供为一个授权的网络节点而事实上它不是。实际上，这样一个作恶者可以寻求作为一个用户站来连接，但是假装一个根网络桥的行为，以具有通常提供给真正的根网络桥的访问和控制。为了促进这样一个结果，该作恶者可以使它的用户站发出一个 BPDU 以断言它是一个桥节点并且它已经获得了根桥节点的地位，因此将其放入一个来从其他桥节点接收各种信息的位置。作为另一个例子，BPDU 中的错误，例如由于真实的桥节点造成的错误而插入的，也可以造成错误的信息向其他桥节点传播。在任一种情况中，因此，网络的其他桥节点接收到该 BPDU，作为响应可以改变它们自己的表信息，以及作为相应也可以引起网络配置的改变。无疑地，这样的改变在响应错误信息而造成网络改变的程度上是不希望的，无论它是由错误的或是非法的意图而传播的。

[0008] 由于上述的缺陷，某些改善生成树协议的解决方案已经在在先技术中被提出。例如，BPDU 保护增强已经被引入以通过明确地定义域边界来增强 STP 安全。一旦该 BPDU 保护在一个端口被激活，如果从该端口接收到一个 BPDU 该端口将变为禁止 (disabled)。这种方式，任何在该具有 BPDU 保护激活的端口后面的设备都不允许参与 STP。结果，激活的以

太网拓扑是稳定的。作为另一个例子，存在一种根保护技术。在这种技术中，根保护被基于每个端口配置，并且不允许该端口成为一个 STP 根端口。这意味着端口总是 STP 指定的，并且如果在这个端口上接收到了更好的 BPDU，BPDU 保护禁止该端口，而不是考虑该 BPDU 和选择一个新的 STP 根。根保护需要在不应该出现根桥的地方的全部端口上被激活。作为另一个例子，能够在以太网中使用加密算法（例如，MAC 安全）。为了实现一个安全的 STP，BPDU 消息需要被加密。

[0009] 虽然上述的方法在各种环境中可以有帮助，它们不保护 STP 免于桥故障。端口保护仅保护用户端口。根保护需要手工设置并且不灵活或不可扩展。MAC 安全方法需要昂贵的加密和网络范围的升级。因此，需要更好的优化和应用，如由以下进一步描述的优选实施方式所实现的。

发明内容

[0010] 根据本发明的一个方面，提出了一种桥接网络系统，包括：多个桥节点；其中所述多个桥节点的每个桥节点都被连接为与所述多个桥节点的至少一个其他邻接桥节点通信；其中所述多个桥节点的每个桥节点包括：用于和所述多个桥节点的另一个桥节点或网络服务器这两者中的至少一个进行通信的电路；以及用于存储从所述多个桥节点的另一个桥节点和所述网络服务器这两者中的至少一个接收的邻接桥节点的至少一个生成树参数的电路；其中所述多个桥节点的每个桥节点都被编程为执行如下步骤：从邻接桥节点端口接收第一控制消息；响应所述第一控制消息向网络服务器发送消息；从所述网络服务器接收响应，其中所述响应包括所述邻接桥节点的所述至少一个生成树参数；将所述邻接桥节点的所述至少一个生成树参数存储在将所述至少一个生成树参数与所述邻接桥节点端口相对应的表中；以及将所述至少一个生成树参数传送给所述邻接桥节点端口；其中所述多个桥节点的每个桥节点都被进一步编程为执行如下步骤：从邻接桥节点端口接收第二控制消息，其中所述第二控制消息包括至少一个规定的生成树参数；以及将所述至少一个规定的生成树参数与先前存储的与所述邻接桥节点端口相对应的值相比较；以及其中所述多个桥节点的每个桥节点都被进一步编程为执行，在所述比较步骤并且响应所述比较步骤做出第一判定之后，请求来自所述邻接桥节点的授权检查。

[0011] 根据本发明的另一个方面，提出了一种桥节点，为了在包括所述桥节点，作为多个桥节点的一个的桥接网络系统中使用，其中所述多个桥节点的每个桥节点都被连接为与所述多个桥节点的至少一个其他邻接桥节点通信，所述桥节点包括：用于和所述多个桥节点的另一个桥节点或网络服务器这两者中的至少一个进行通信的电路；以及用于存储从所述多个桥节点的另一个桥节点和所述网络服务器这两者中的至少一个接收的邻接桥节点的至少一个生成树参数的电路；其中所述桥节点被编程为执行如下步骤：从邻接桥节点端口接收第一控制消息；响应所述第一控制消息向网络服务器发送消息；从所述网络服务器接收响应，其中所述响应包括所述邻接桥节点的所述至少一个生成树参数；将所述邻接桥节点的所述至少一个生成树参数存储在将所述至少一个生成树参数与所述邻接桥节点端口相对应的表中；以及将所述至少一个生成树参数传送给所述邻接桥节点端口；其中所述桥节点进一步被编程为执行如下步骤：从邻接桥节点端口接收第二控制消息，其中所述第二控制消息包括至少一个规定的生成树参数；以及将所述至少一个规定的生成树参数与先前

存储的与所述邻接桥节点端口相对应的值相比较；以及其中所述桥节点被进一步编程为执行，在所述比较步骤并且响应所述比较步骤做出第一判定之后，请求来自所述邻接桥节点的授权检查。

附图说明

[0012] 图 1 示出了一个总体上指定为 10 并作为优选实施方式的一个例子的网络系统。

[0013] 图 2 示出了一个根据一个优选实施方式的描述包括在系统 10 中的功能的流程图方法 20。

[0014] 图 3 示出了一个与图 1 的系统 10 相同的且具有一处修改的系统 10'。

[0015] 图 4 示出了一个描述包括在上面介绍的系统 10 或 10' 中的另外的功能的流程图方法 40。

具体实施方式

[0016] 图 1 示出了一个总体上指定为 10 并作为优选实施方式的一个例子的网络系统。总体上在图 1 中所示的层次上，系统 10 中的每个项在本领域中都是公知的，其中所示的节点可以使用各种形式的硬件和软件编程来构造以执行与在这个文档中的讨论相一致的步骤。然而，如随后详细描述的，该操作方法和某些添加到桥节点的功能为优选实施方式提供，并工作为总体上改进系统 10，这样的方法和功能可以容易地添加到已经存在的如系统 10 的系统的硬件和软件编程中。实际上，结果，优选实施方式是灵活的并且可扩展到不同大小的网络。系统 10 总体上代表一个桥接网络，例如包括许多城域节点的城域以太网网络，它也被称为以太网交换机。注意在系统 10 中节点之间的物理连接可以以各种方式被提及并且可以以各种方式实现，但无论如何它们允许每两个相连的节点组之间的双向通信。通过数据块来通信，该数据块经常被称作消息、帧或分组。此外，在核心网络内并且如本领域内所公知的，可以强加一个另外的路由层，例如利用一个或更多生成树，其定义了消息在核心网络内沿其通信的路径，用于沿着给定的生成树通信。实际上，图 1 的连通性是为了举例说明这样一个生成树，同时理解这样的连通性因此在形式上是物理和逻辑这两者的，其中可以存在另外的物理的连接但没有表示出来，因为它们不是当前生成树的组成部分。

[0017] 然后总体上参看系统 10，它包括五个桥节点 BRN_0 到 BRN_4，其中桥节点 BRN_0 在所示的本例子中假定为根桥节点。典型地，因此，作为一个根节点，桥节点 BRN_0 应该具有最高的优先级，通常通过使每个桥节点具有相应的桥 ID 或桥优先级数字来将优先级呈现给系统 10 内的全部节点，其中该 ID 或数字代表每个节点的相应优先级，包含因此识别哪个桥节点为根的一个 ID（或优先级）。无论如何，作为根，桥节点 BRN_0 连接到一个网络服务器 NS，它由于以下中更加清楚的原因而有时被称为认证服务器，并且它连接到一个数据库 DB。以虚线的方式示出了从桥节点 BRN_0 到网络服务器 NS 的连接，因为实际上在系统 10 内的全部桥节点可以和网络服务器 NS 通信，尽管在图 1 中示出了到桥节点 BRN_0 的明确连接，仅仅因为在那个例子中桥节点 BRN_0 是根节点。另外，虽然没有示出，网络管理员（或“网络管理者”）由于各种原因也可以有权访问网络服务器 NS，包括输入某些生成树参数的能力，例如根 ID 和可供选择的根 ID，用于认证使用，如以下进一步可理解的。无论如何，桥优先级，一旦存储在每个节点中，在系统 10 中故障之后提供控制。

[0018] 在系统 10 中，每个桥节点 BRN_X 也经由相应的端口连接到一个或更多其他桥节点。例如，桥节点 BRN_0 经由端口 $BP_{0.0}$ 连接到桥节点 BRN_1，桥节点 BRN_0 也经由端口 $BP_{0.1}$ 连接到桥节点 BRN_4。注意所示的桥节点的连接可以通过直接的连接或存在仅作为路由节点而没有桥节点功能的中间节点，其中典型地，这样的中间节点不包括在桥节点之间的跳距离的度量标准中。无论如何，从图 1 的图示中，本领域熟练的人员会认识到图 1 中桥节点之间的其余的连接，这些连接连同以上讨论过的连接总结在下面的表 1 中：

[0019]

桥节点	连接的桥节点
BRN_0	BRN_1，经由端口 $BP_{0.0}$ BRN_4，经由端口 $BP_{0.1}$
BRN_1	BRN_0，经由端口 $BP_{1.4}$ BRN_2，经由端口 $BP_{1.2}$
BRN_2	BRN_1，经由端口 $BP_{2.0}$
BRN_3	BRN_4，经由端口 $BP_{3.0}$
BRN_4	BRN_0，经由端口 $BP_{4.1}$ BRN_3，经由端口 $BP_{4.3}$

[0020] 表 1

[0021] 继续关于系统 10，为了举例，也示出了多个桥节点连接到用户站节点 $US_{y.z}$，它们可以通过其他名称被提及，例如客户节点或客户站。用户站节点是可以在全球互联网内或在位于远处的网络处 - 例如在一个商业实体的不同物理位置 - 实现的节点的例子。典型地，因此，对于某些用户站节点是希望和其他节点通信的，因此一个桥节点的关键功能是以不侵入的或甚至对于用户节点可辨别的方式，促进这样的通信。结果，在系统 10 中的一个用户站可以跨越很远的距离与系统 10 中的另一个用户站通信，而对它们之间的网络层次和节点透明。图 1 中用户站的例子的连通性总结在下面的表 2 中：

[0022]

桥节点	连接的用户站节点
BRN_0	无
BRN_1	$US_{1.0}$，经由端口 $BP_{1.0}$ $US_{1.2}$，经由端口 $BP_{1.1}$
BRN_2	$US_{2.1}$，经由端口 $BP_{2.1}$ $US_{2.2}$，经由端口 $BP_{2.2}$

桥节点	连接的用户站节点
BRN_3	$US_{3.1}$，经由端口 $BP_{3.2}$ $US_{3.2}$，经由端口 $BP_{3.3}$ $US_{3.3}$，经由端口 $BP_{3.4}$
BRN_4	$US_{4.0}$，经由端口 $BP_{4.0}$ $US_{4.1}$，经由端口 $BP_{4.4}$

[0023] 表 2

[0024] 系统 10 也包括阻塞 BLK_X 以强加一个另外的路由控制层，如以上在这个文档的背景技术部分中所介绍的。在本例子中，让那个路由控制是一个生成树，其定义了消息沿其可以在桥接网络中通信的路径。例如，在桥节点 BRN_2 和 BRN_3 之间示出了一个阻塞 BLK_1。作为阻塞 BLK_1 的结果，没有经过系统 10 中的至少一个其他桥节点，桥节点 BRN_2 不可以和 BRN_3 通信。例如，从桥节点 BRN_2 到 BRN_3 的通信路径经由 BRN_1、BRN_0、BRN_4 到 BRN_3 跨越四个桥节点的跳距离。以相似的方式，在桥节点 BRN_1 和 BRN_4 之间示出了一个阻塞 BLK_2。作为阻塞 BLK_2 的结果，没有经过系统 10 中的至少一个其他桥节点，桥节点 BRN_1 不可以和 BRN_4 通信。例如，从桥节点 BRN_1 到 BRN_4 的通信路径经由 BRN_0 到 BRN_4 跨越两个桥节点的跳距离。

[0025] 现在已经介绍了系统 10，注意在正确的操作下，通过控制消息（例如，桥协议数据单元 -“BPDU”）在桥节点中的协商，创建该生成树拓扑，当它们正在启动或重新复位时。如在系统 10 中所示，一个桥节点（例如，BRN_0）被选择作为根。同样在这个过程期间，其余的桥节点每个发现到达根节点的最低代价路径并阻塞其他冗余的数据路径（例如，阻塞 BLK_1 和 BLK_2），从而创建全部的生成树。然而，各种原因可以导致生成树协议的一个异常，例如通过桥节点故障或通过在 BPDU 中断言虚假信息来欺骗系统 10 的恶意用户。关于前者的例子，假如用户站 $US_{3.1}$ 的用户寻求未授权访问网络信息，这样的访问可以通过使用户站以支持的 BPDU 的形式发布虚假的数据的方式来寻求，其中用户站 $US_{3.1}$ 提供自己作为根桥节点，而事实上它是一个用户站。如果这个尝试成功了，其他桥节点会重新收敛并且很有可能该生成树会被改变，例如通过重新定位阻塞 BLK_1 和 BLK_2 中的一个或两个，也将访问权给予不旨在用于正确的和授权的网络操作的用户站 $US_{3.1}$。因此，作为这样一个尝试或桥节点故障的结果，当生成树协议没有正确地收敛，在网状网络中会形成环回或攻击者能够利用该情形在网络业务量上进行窃听和发动拒绝服务（“DoS”）攻击。该优选实施方式，然而，寻求减少或消除这些可能性，如下面进一步所探究的。

[0026] 图 2 示出了一个根据一个优选实施方式的描述包括在系统 10 中的功能的流程图方法 20，也通过结合图 3 的例子进行解释，图 3 示出了一个与图 1 中的系统 10 相同且具有一处修改的系统 10’。具体地，在图 3 中，示出了一个另外的桥节点 BRN_5 连接到系统 10，具有多种牵连，涉及如本文档中其余部分中所描述的。在这个增加节点的例子中，因此，桥节点 BRN_2 和 BRN_5 如先前所定义的是邻居或邻接节点，其中在这个例子中，它们是这样因为桥节点端口 $BP_{2.4}$ 直接连接到桥节点端口 $BP_{5.0}$’ 所以这些桥节点可以直接地彼此传送消息，而不需要经过一个或更多中间桥节点。

[0027] 作为介绍，注意除了方法 20 之外，本领域中所公知的各种其他功能可以通过系统 10 作为一个整体或通过它的一个或更多组件来实现，其中方法 20 因此没有示出这样的另外步骤以便聚焦于本优选实施方式的新颖的方面。

[0028] 在方法 20 中，第一步骤 30 应用于每个桥节点 BRN_X，其中相应的节点等候一个到可信网络的新的桥接。通过使用术语可信网络，假设已经到达了某一稳定状态，由此例如系统 10 的网络具有确定数目的桥节点，每个桥节点经由一个或更多端口经由相应的链路连接到在网络中的其他节点，其中每个那些连接都在一个过程中核实为许可，该过程经常被称为“认证”，如下面所进一步详细描述的。作为例子，因此，在图 1 中假设每个图示出的桥节点已经认证，以及因此，那时那些桥节点的全部组成可信网络。

[0029] 当建立了一条新的桥节点链路时，那么方法 20 从步骤 30 继续到步骤 32。当通过多于一条链路已经在网络中的一个桥节点为了寻求建立到另一个已经在网络中的桥节点的另一个链路的时候，或其中一个先前没有连接到网络的新的桥节点第一次连接到网络时，这可以发生。作为举例说明这后者的例子，回想起在图 3 中的桥节点 BRN_5 是在系统 10 和 10’之间新近加入的节点并且已经建立了一个从它的端口 $BP_{5.0}$ 到桥节点 BRN_2 的端口 $BP_{2.4}$ 的新的链路。作为响应，步骤 32 如本领域所公知的操作。具体地，当一个新的桥节点链路连接到一个已经存在的桥节点时，开始以上介绍的认证过程，由此核实新连接的真实性。特别地，新链路所连接的已存在的桥节点成为关于该新桥节点的认证者，该新桥节点或新链路的桥节点上的端口是请求者。该请求者，实际上，向认证者请求认证，如果被批准，将允许该请求者链路加入可信网络。作为对该请求者的请求的响应，认证者开始和网络服务器 NS 进行通信。因此，在图 3 的例子中，桥节点 BRN_2 的端口 $BP_{2.4}$ 成为桥节点 BRN_5 的请求者端口 $BP_{5.0}$ 的认证者，因此，桥节点 BRN_2 沿着不同的端口向网络服务器 NS 和数据库 DS（经由一个或更多中间桥节点，在这个例子中例如经由 BRN_0）发送响应请求。假设各种信息正确地呈现在这个请求中，那么网络服务器 NS 根据在先技术确定用于新链路的生成树参数，就是说，充分的信息以包括新链路，该新链路包括在当前或新收敛的生成树中的请求节点端口。这些参数包括一个识别当前的根桥节点的当前根 ID 的标识，其中此处是节点 BRN_0，也包括生成该请求的桥节点端口的端口路径代价（“PPC”），其中此处请求端口是桥节点 BRN_5 的端口 $BP_{5.0}$。从这个文档的背景技术部分回想起 PPC 是一个在该生成树中沿着从产生该 BPDU 的桥节点的指定端口到一个确定位置例如“根”桥节点的路径的传输的代价的效率度量标准。因此，假设每个图示的端口到端口链路都有长度 1 的 PPC，那么会为桥节点 BRN_5 的请求者端口 $BP_{5.0}$ 确定该 PPC 等于 3。

[0030] 在步骤 32 中完成 PPC 的确定之后，方法 20 继续到步骤 34。此处，根据在先技术，包括那个 PPC 和当前根节点 ID 的生成树参数从网络服务器 NS 传送给请求者桥节点，该节点为了将来网络操作的目的存储那个 PPC。注意最好经由一个认证者桥节点传送这个信息，在图 3 的例子中认证者桥节点是桥节点 BRN_2。对本优选实施方式的进一步，然而，请求者桥节点的 PPC 信息和当前根节点 ID 不仅通过认证者向请求者传递，而且最好该相同信息也由认证者桥节点存储和维护。换句话说，根据本优选实施方式，将被给新链路请求桥节点端口的生成树参数不仅由该 PPC 所适用的请求桥节点存储，在某种程度上，也由作为认证者操作的邻接节点存储，该邻接节点可以归结或跟踪那些关于该新链路请求桥节点的参数，在本文档中为了参考和一致性的目的但没有限制，假设由邻接节点进行的存储被称为在邻居

跟踪表中的存储，就是说，这些被存储在一个节点（例如，认证者）的存储器等中的信息跟踪最初事实上属于并发送给该邻接（例如，请求者）节点的信息。每个桥节点的真正的物理邻居跟踪表为了简化说明而没有示出，但本领域熟练的人员会容易的认识到这种设备的硬件容易有权访问存储器的存储。无论如何，另外，其他旨在用于请求请求者桥节点的信息也可以由该邻接认证者桥节点存储。这个存储信息的原因和使用将在随后详细描述。

[0031] 已经说明了请求者桥节点和认证该请求者桥节点的认证者节点的生成树参数的通信和存储，注意方法 20 最好当每个桥节点或节点端口连接添加到可信网络时应用。结果，每次建立一个新的链路时，经由新链路请求连接的桥节点端口会得到它的 PPC 和当时存在的根节点 ID 的通知，它的邻接桥（即，直接地连接到请求桥节点的认证者桥节点）也一样会得到通知。因此，随着时间过去，以及当网络中的链路数目随同本优选实施方式的执行而增长，那么每个桥节点将会存储有它自己的 PPC 值和那些用于任何它直接连接的邻接节点，其中这样的直接连接包括中间桥到桥连接，或此时一个桥节点通过一个或更多透明的非桥节点连接到另一个桥节点，在这种情况下在后者中，两个桥节点逻辑上还是直接连接的。从 PPC 和根节点 ID 信息的分发产生了各种好处，如下面进一步展现的。

[0032] 图 4 示出了一个描述包括在以上介绍的系统 10 或 10’中的另外的功能的流程图方法 40，那也将通过结合图 3 例子来解释，同时应当理解它同样适用于图 1。由于具有方法 20 的一部分，方法 40 最好应用于系统 10 和 10’中的每个桥节点。在桥节点已经加入可信网络和生成树收敛发生之后，预期在未来的某个时刻那个桥节点会再次发送一个具有断言作为生成树参数的控制消息（例如，BPDU），就是说，它会包括声明或提议作为网络根节点 ID 和它自己 PPC。因此，方法 40 的步骤 42 代表一个等待状态，其中每个桥节点可以提供其他功能例如路由网络业务量等，同时也等待来自网络中任何其他桥节点的这样的 BPDU。

[0033] 当由桥节点从邻接桥节点接收到 BPDU 时，那么方法 40 从步骤 42 继续到步骤 44。作为步骤 44 响应的介绍，注意可以由于各种原因接收到这样的 BPDU。作为第一组例子，可以出现某些普通的和正确的事件并可以导致 BPDU 的发布，例如可以在系统 10 和 10’中寻求新的链路，或可能已经发生故障，例如失败的链路。然而，作为第二组和相反的例子，可以发生不正确的事件，例如其中 BPDU 代表节点的非法尝试以获取不正确的对系统 10 或 10’的资源的部分的访问或控制。无论如何，如当前说明的，步骤 44 开始了一个过程来从第二个例子组区别和辨别第一个例子组。通常，步骤 44 基于它察觉到由接收到的 BPDU 所代表的这两组中的哪一个来指引流程，其中通过检查接收到的 BPDU 中的一个或更多生成树参数实现确定。在本优选实施方式中，通过查询关于两个生成树参数发展了这个察觉，以及至少为了易于当前的解释，下面分别讨论每个查询。

[0034] 在第一查询中，在 BPDU 接收节点处步骤 44 将接收到的 BPDU 中的 PPC 与预先存储的（来自步骤 34）用于那个邻接节点的 PPC 相比较，就是说，和先前存储在接收桥节点的邻居跟踪表中的 PPC 的值比较。换句话说，回想起来自图 2 的步骤 34 的先前发生的事情中的接收桥节点在它自己的邻居跟踪表中存储了最初传送给该桥节点的 PPC 值（和根节点 ID）。因此，在步骤 44 中，接收桥节点参考这个表来将那先前存储的 PPC 值，先前给予并由此归于该邻居节点，与现在从该邻居节点接收到的值相比较。对本优选实施方式的进一步，如果当前接收到的 PPC 值小于对应邻居跟踪表的 PPC 值，那么该较小的 PPC 值代表一种情况，其中会触发生成树的改变；换句话说，该邻居节点当前发送的实际上是提议的 PPC 的减小，这典

型地会触发生成树重新收敛同时节点将寻求最优化路径以利用好像现在可用的全部较低的PPC。如果这样的提议是正确的，那么当然按照它行动会是有利的，但是它是不正确的，因此它可能不必要引起生成树改变和实际上将授权给予不需要真正授权的地方。结果，当步骤44进行它的PPC比较时，如果该当前接收到的PPC值小于相对应的邻居跟踪表PPC值，那么步骤44将方法40的控制继续向前到步骤46，但是如果该当前接收到的PPC值等于或大于相对应的邻居跟踪表PPC值，那么步骤44将方法40的控制向前继续到步骤48。两个可选择的结果步骤46和步骤48在后面论述。

[0035] 在第二查询中，在BPDU接收节点处步骤44将接收到的BPDU中的根节点ID与用于该邻接节点的存储在接收桥节点的邻居跟踪表中的根节点ID相比较。回想起用于该邻接节点的并存储在接收桥节点的邻居跟踪表中的根节点ID在图2的步骤34的在先发生的事件中被存储，或者，作为选择，如果已经经由网络管理者等对根ID进行了合法的改变，那么在本优选实施方式中在该过程期间，每个桥节点用该改变的ID更新对应于其邻接节点的它的邻居跟踪表。无论如何，在步骤44中，该接收桥节点参考这个表来将先前存储的根节点ID值和现在从该邻接节点接收到的值相比较。对本优选实施方式的进一步，如果这两个节点值不同，那么这也代表一种情况，其中会触发生成树的改变。因此，如果接收的BPDU的根节点ID值不同于邻居跟踪表中相对应的一个，那么步骤44将方法40的控制向前继续到步骤46。相反地，如果相比较的根节点ID值相同，那么步骤44将方法40的控制向前继续到步骤48。

[0036] 在步骤46中，由于探测到PPC的减小或根节点ID的改变而到达该步骤，接收桥节点向发送邻接节点请求授权检查，其中最好通过网络服务器NS满足该授权检查。因此，响应这个授权检查请求，现在发送引起在步骤44中识别的BPDU的桥节点的同一个端口被请求通过与网络服务器NS的通信和提供某些形式的认证来证明它的授权，仅在如果核实了该桥节点端口在系统10或10’内的情况下，网络服务器NS大概会将所述认证提供给该桥节点。例如，这样的认证可以以提供网络密钥或授权令牌的形式出现。因此，在来自步骤46的授权请求之后，方法40继续到步骤50。

[0037] 步骤50描述了用于在步骤46中发布授权请求的桥节点的等待状态，其中在一定时间段之后，步骤50确定是否已经由在步骤46中发送请求的端口返回有效的授权。如果没有收到该授权，那么方法40从步骤50继续到步骤52。如果接收到该授权，那么方法40从步骤50继续到步骤54。

[0038] 步骤52，由于在步骤46中请求的授权没有正确的返回而到达该步骤，描述了一个对于该授权缺乏的优选反应。具体地，在步骤52中，发布警报来向网络管理者等表明接收到了可疑的BPDU（在先前的步骤42中）。另外，注意步骤52表明阻止接收到的BPDU在系统10和10’中向前转发。因此，除了该警报，网络管理者可以得知关于所讨论的BPDU的各种详细信息，并且他或她同样会得知该BPDU没有在所讨论的生成树中被向前转发。在步骤52之后，方法40返回步骤42，就是说，刚才接收到BPDU的接收桥节点，确定它为可疑的，报告一个警报，并且不转发它，然后返回到等待状态，因此它可以接收下一个BPDU并且基于该下一个BPDU中的生成树参数与方法40的步骤相一致地行动，这个类型的操作反复用于系统10或10’中的全部桥节点并用于未来有关的BPDU。

[0039] 现在返回步骤48，回想起当不满足步骤44时到达该步骤，就是说，当接收到的

BPDU 不包括发送邻接桥节点的较低的 PPC 或根节点 ID 的改变时。在步骤 48 中，接收节点更新存储在接收桥节点的邻居跟踪表中的发送邻接桥节点的 PPC 的值。换句话说，回想起图 2 的方法 20 为每个桥节点建立邻居跟踪表，其中特定的桥节点存储任何邻接节点的 PPC。因此，注意当由发送邻接桥节点在 BPDU 中表明一个较大（或相同）的 PPC 值时，到达步骤 44，那么接收桥节点因此更新它的存储的用于该发送邻接桥节点的 PPC 值。接下来，方法 40 从步骤 48 继续到步骤 54。

[0040] 在步骤 54 中，步骤 48 之后或对于步骤 50 的肯定的判定之后到达此步骤，每个桥节点操作为允许正常的生成树协议（“STP”）收敛。因此，由桥节点在步骤 42 中接收到的且在步骤 44 中引起否定的判定的 BPDU，或经由步骤 50 返回授权的 BPDU，会由接收桥节点继续向前转发，其他节点会按照 STP 技术做出响应。此外，注意收敛过程可以重新创建链路以便调用方法 20，由此在各个邻居跟踪表中存储根 ID 和 PPC 值的新值。之后，方法 40 返回到步骤 42，因此每个桥节点，收敛之后，再次等待另一个 BPDU，并且方法 40 以以上描述的方式重复。

[0041] 为了进一步认识方法 40，现在考虑一些它的应用的例子。注意这样的例子不意在是穷尽的，但它们说明了优选实施方式发明范围的各个方面的灵活性和好处。因此，考虑如下情况：(i) 合法的新桥节点加入网络；(ii) 向网络加入新链路，包括失败的链路恢复；或 (iii) 非法的 STP 攻击。下面进一步探究这些例子的每一个。

[0042] 当合法的新桥节点加入网络系统 10 或 10’时，根据以上讨论的优选实施方式，该新桥节点从其端口沿着将它连接到系统的链路发布 BPDU。例如在图 3 的系统 10’中，当桥节点 BRN_5 加入系统 10’，它向桥节点 BRN_2 的端口 $BP_{2.4}$ 发送 BPDU。作为新桥，节点 BRN_5 到此时为止不会断言其 PPC 或根节点 ID，因此，当桥节点 BRN_2 将步骤 44 应用于接收到的 BPDU 时，既不涉及该 PPC 也不涉及该根 ID，因此，流程继续到步骤 48。由于在当前 BPDU 中没有提供新 PPC，方法 40 继续到步骤 54，其中正常的收敛会将该新节点（即，BRN_5）的 BPDU 向根节点传递。一旦该 BPDU 到达根节点，该根节点确定用于该新加入的节点的 PPC，并且连同根节点 ID 一起，该信息返回到该新节点。因此，在这个例子中，方法 40 不影响或阻止新的网络链路的正常创建。而且，当该新确定的 PPC 返回到该请求节点（例如，BRN_5）时，然后根据方法 20 的步骤 34，认证者桥节点（例如，BRN_2）会将该 PPC 值存储在它自己的邻居跟踪表的条目中并与该请求节点相对应，同时也向该请求邻接节点发送这个信息。因此，为了未来的目的，为了稍后对由认证者桥节点从它的邻接桥节点接收到的另外的 BPDU 进行分析而更新该邻居跟踪表。

[0043] 当向网络添加新链路时，根据以上讨论的优选实施方式，操作类似于用于新节点的操作，尽管该 BPDU 可以已经包括根节点 ID 的标识。在该情况下，假设正确地和合法地寻求该期望的新链路，那么当由接收建立新链路的请求的邻接节点执行步骤 44 时，该 BPDU 识别的根节点 ID 应该和该接收邻接节点所知道的相匹配。因此，再次否定地回答步骤 44，所以流程继续到步骤 48。由于在当前 BPDU 中没有提供新 PPC，方法 40 继续到步骤 54，其中正常的收敛会将该新链路的 BPDU 向根节点传递。一旦该 BPDU 到达根节点，根据方法 20 的步骤 32，该根节点确定用于该新加入的链路的 PPC，并且连同根节点 ID，该信息返回到该节点。因此，同样在这个例子中，方法 40 不影响或阻止新的网络链路的正常创建。而且，如同前面的例子，当该新确定的 PPC 和根节点 ID 返回到该新链路请求节点时，那么根据方法 20

的步骤34，认证者桥节点会将那些PPC和根节点ID值存储在它自己的邻居跟踪表的条目中并与该请求节点的链路相对应，同时也向该请求节点发送这个信息。

[0044] 当作恶者在桥节点层次寻求未授权的访问时，很有可能该实体会发布一个意图呈现很低的PPC或该根节点ID的改变的BPDU；如果该作恶者尝试影响未来的网络业务量以达到它作为通往根节点的路径，或作为实际的根节点，就有可能是该情况。当发布了这样的BPDU时，然而，该接收邻接节点会应用方法40，步骤44会得到肯定的回答。因此，该接收邻接节点会向该恶意的发送邻接节点请求授权，假设后者不能提供这样的授权，那么会由该接收节点发布报警，且不向前转发该BPDU，所以它不会否则影响或扰乱系统10（或10'）的其余部分。因此，这样的报警可以得到监控，例如通过将它们存储在日志等中，并且能够采取进一步的努力来保证网络的完整性和消除不受欢迎的网络访问。

[0045] 从以上中，本领域熟练的人员应该认识到优选实施方式向桥接计算机网络提供了改善的例如在网络生成树中某些异常的探测。确定的好处是改善的探测和防止未授权的尝试改变生成树配置。其他好处是报告未授权的改变生成树配置的尝试。还有其他好处包括当寻求合法的改变网络配置时生成树收敛和正常操作，例如新的桥节点或桥链路的加入。作为其他好处，最小化或避免了各种其他在先技术方法的缺点。这些好处和其他的都会被本领域熟练的人员所认识到。实际上，作为最终的好处，尽管已经详细地描述了本优选实施方式，但是能够对以上给出的描述进行各种替换、修正或改变，而不会偏离下面权利要求所定义的本发明范围。

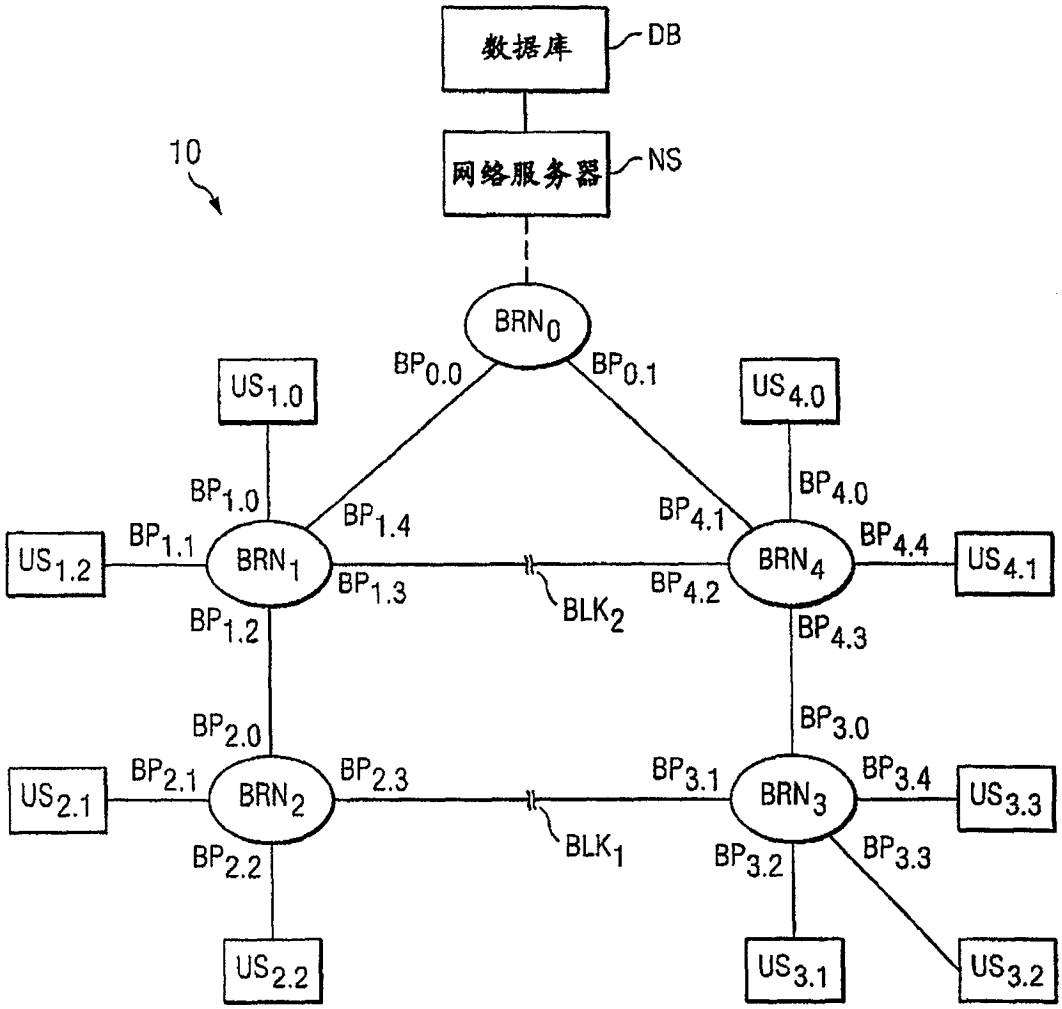

数据库
DB
网络服务器
NS
10
BRN0
BP0.0
BP0.1
US1.0
US4.0
BP1.0
BP4.0
BP1.4
BP4.1
BP1.1
US1.2
BRN1
BRN4
BP4.4
US4.1
BP1.3
BLK2
BP4.2
BP1.2
BP4.3
BP2.0
BP3.0
BP2.1
BP2.3
BP3.1
BP3.4
US2.1
BRN2
BRN3
US3.3
BLK1
BP2.2
BP3.2
BP3.3
US2.2
US3.1
US3.2

图 1

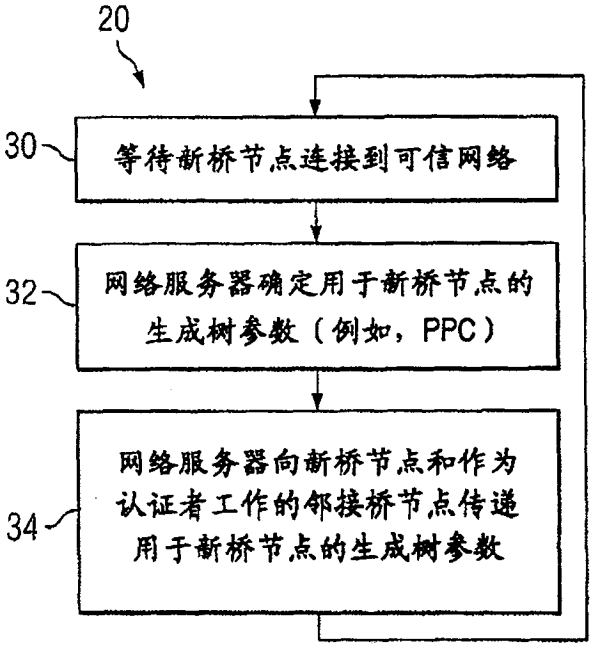

20
30
等待新桥节点连接到可信网络
32
网络服务器确定用于新桥节点的生成树参数（例如，PPC）
34
网络服务器向新桥节点和作为认证者工作的邻接桥节点传递用于新桥节点的生成树参数

图 2

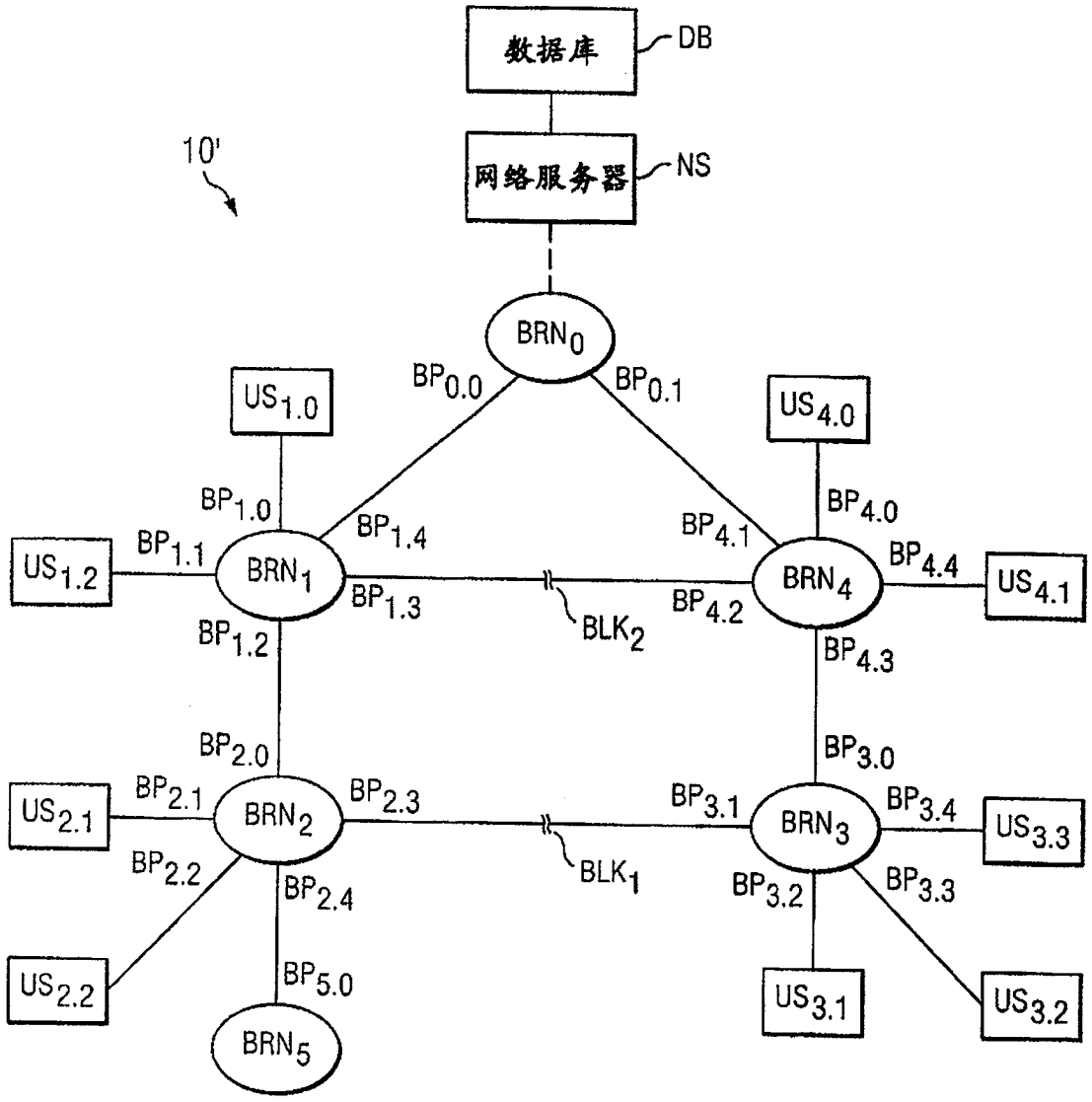

数据库
DB
10'
网络服务器
NS
BRN0
BP0.0
BP0.1
US1.0
US4.0
BP1.0
BP4.0
BP1.4
BP4.1
US1.2
BP1.1
BRN1
BRN4
BP4.4
US4.1
BP1.3
BP4.2
BLK2
BP1.2
BP4.3
BP2.0
BP3.0
US2.1
BP2.1
BP2.3
BP3.1
BRN2
BRN3
BP3.4
US3.3
BLK1
BP2.2
BP2.4
BP3.2
BP3.3
US2.2
BP5.0
US3.1
US3.2
BRN5

图 3

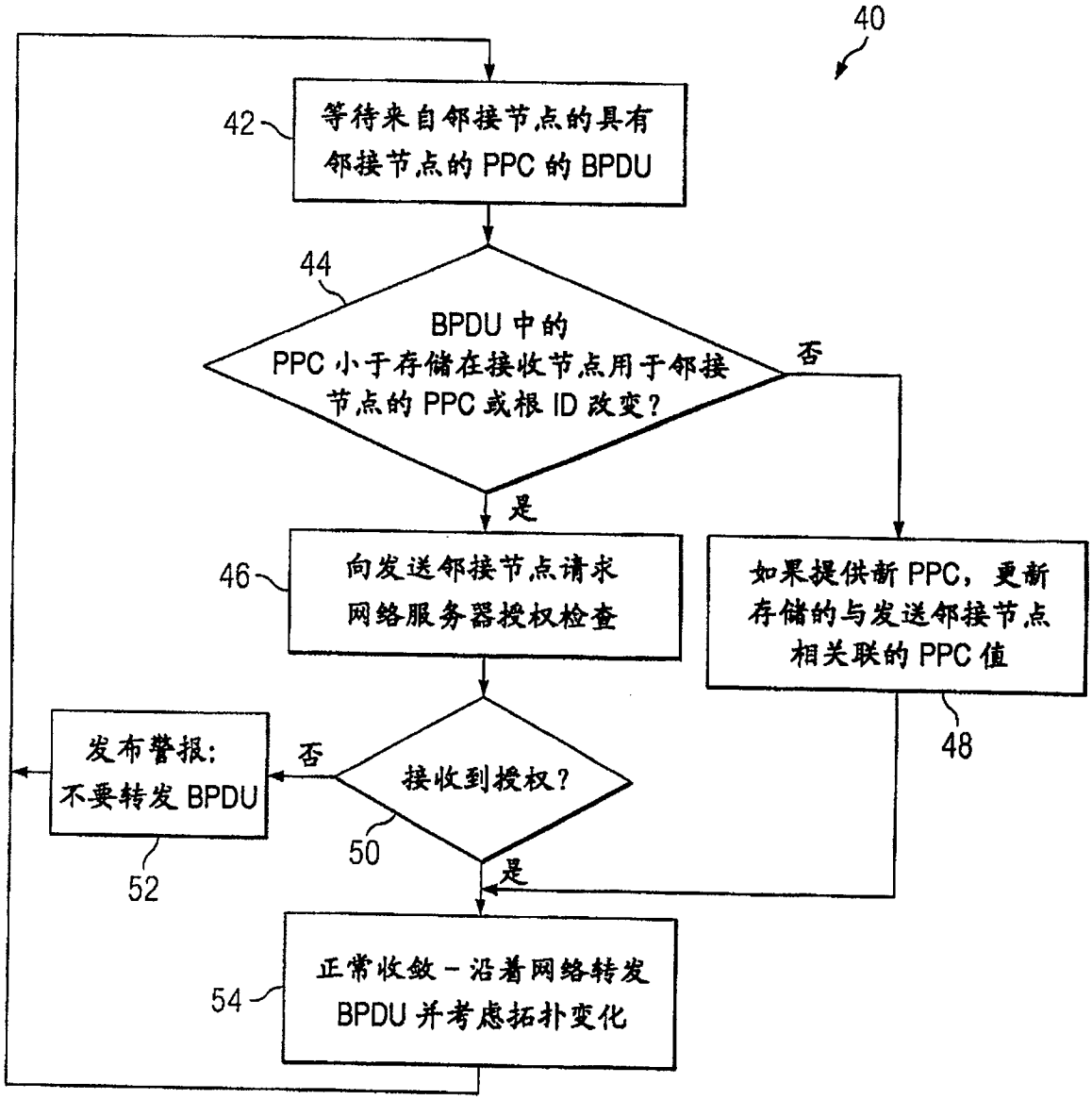

40
42
等待来自邻接节点的具有邻接节点的 PPC 的 BPDU
44
BPDU 中的 PPC 小于存储在接收节点用于邻接节点的 PPC 或根 ID 改变？
否
是
46
向发送邻接节点请求网络服务器授权检查
如果提供新 PPC，更新存储的与发送邻接节点相关联的 PPC 值
48
发布警报：不要转发 BPDU
否
接收到授权？
50
52
是
正常收敛 - 沿着网络转发 BPDU 并考虑拓扑变化
54

图 4