[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/56 (2006.01)
H04L 29/06 (2006.01)
H04L 12/02 (2006.01)
H04Q 3/00 (2006.01)

[12] 实用新型专利说明书

专利号 ZL 200620137423.9

[45] 授权公告日 2007 年 12 月 12 日

[11] 授权公告号 CN 200990619Y

[22] 申请日 2006.10.12
[21] 申请号 200620137423.9
[30] 优先权
[32] 2005.10.12 [33] US [31] 11/249,076
[73] 专利权人 丛林网络公司
地址 美国加利福尼亚州
[72] 发明人 布鲁诺·赖斯曼

[74] 专利代理机构 北京康信知识产权代理有限责任公司
代理人 余 刚

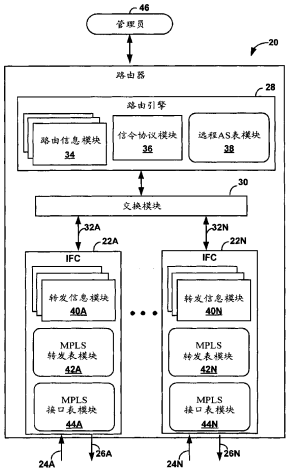
权利要求书 2 页 说明书 16 页 附图 6 页

[54] 实用新型名称

路由装置

[57] 摘要

本文描述了一种路由装置，其对多协议标签交换(MPLS)分组进行欺骗检查，以在标签交换路径(LSP)中防止 MPLS 分组的恶意的或非故意的插入。 该路由装置包括：路由引擎，用于维护反映网络拓扑结构的路由信息；以及接口卡，其插于路由设备的插槽中，电连接至路由引擎，并使用接口播发用于标签交换路径的标签，其中，一旦接收到具有标签的分组，则接口卡校验分组是否在最初用来播发标签的接口上接收到的。 其还包括与诸如资源预订协议(RSVP)、标签分发协议(LDP)、以及边界网关协议(BGP)的信令协议相关的软件模块，被扩展以应用 MPLS 转发表、MPLS 接口表、以及远程自治系统表。



1. 一种路由装置，其特征在于，包括:

路由引擎，用于维护反映网络拓扑结构的路由信息；以及

接口卡，其插于路由设备的插槽中，电连接至所述路由引擎，并使用接口播发标签交换路径的标签，

其中，一旦接收到具有所述标签的分组，则所述接口卡校验所述分组是否是在最初用来播发所述标签的所述接口上接收到的。

2. 根据权利要求 1 所述的路由装置，其特征在于，进一步包括存储有转发表的转发表模块，用于维护所述标签所针对播发的接口组，以及，所述接口卡确定接收所述分组的所述接口是否包括在所述接口组中。

3. 根据权利要求 1 所述的路由装置，其特征在于，进一步包括:

远程自治系统表模块，其存储远程自治系统表，用于将编号与远程自治系统关联起来;

转发表模块，其存储转发表，用于将标签与欺骗检查类型以及欺骗检查信息关联起来；以及

接口表模块，其存储接口表，用于将接口编号与虚拟路由器以及远程自治系统编号关联起来。

4. 根据权利要求 3 所述的路由装置，其特征在于，所述转发表模块和所述接口表模块设置在所述接口卡中，并且，所述远程自治系统表模块设置在所述路由引擎中。

5. 根据权利要求 1 所述的路由装置，其特征在于，进一步包括：交换模块和内部数据路径，用于将所述接口卡电连接至所述路由引擎。

路由装置

技术领域

本实用新型的原理涉及计算机网络，并且更具体地，涉及防止在计算机网络中的攻击行为。

背景技术

计算机网络汇集了多个相互连接的计算设备，它们交换数据并共享资源。在基于分组的网络中（例如因特网），计算设备通过将数据分成被称作分组的小块来交换数据。这些分组各自经过网络从源设备路由到目标设备。目标设备从这些分组中提取数据并把这些数据组组装为其原始格式。将数据分割为分组使得源设备可以仅重新发送在传输期间那些可能丢失的个别的分组。

基于分组的计算机网络越来越多地使用标签交换协议，该协议用于业务工程及其他目的。在标签交换网络中，标签交换路由器（Label Switching Routers，缩写为 LSR）使用多协议标签交换（Multi-Protocol Label Switching，缩写为 MPLS）信令协议来建立标签交换路径（Label Switched Path，缩写为 LSP）。所述 LSR 利用 MPLS 协议从下游 LSR 中接收 MPLS 标签映象，然后将 MPLS 标签映象播发（advertise）给上游 LSR。当 LSR 从上游路由器中接收 MPLS 分组的时候，其根据在其转发表中的信息来交换 MPLS 标签，然后传送所述分组到适当的下游 LSR。

传统的LSR通常假设所连接的任何给定的上游LSR都是“可信任的”，以仅使用实际已被播发给该上游LSR的标签发送MPLS分组。然而，这引起潜在的安全脆弱性问题，这是由于LSR可能从源而不是从已被播发标签映象的上游LSR中接收MPLS分组。换句话说，根据一个或多个LSP的相应的标签映象，通过输出MPLS分组，恶意源可以“欺骗（spoof）”上游LSR。如果下游LSR接收该欺骗的MPLS分组以及标签，交换所述分组并且传送这些分组到下游LSR的话，则出现了安全漏洞。即使并未上行发送该LSP信号给所述源，该恶意源也已经成功地(或者可能非故意地)将MPLS分组插入到了LSP中。

检测和避免MPLS欺骗会是一项困难的任务，用于基于分组系统的常规检测方案可能不适用。例如，通常应用于基于分组网络中的常规方法仅仅是检验所接收的分组的源地址。但是，在MPLS上下文中通常没有与分组相关的源地址。

因此，某些LSR试图通过检验为MPLS而启动的接口上所接收的分组来防止MPLS欺骗。如果对于特定的接口未启动MPLS，LSR就丢弃该分组。然而，在MPLS启动接口上接收欺骗的MPLS业务时，该方法将避免不了安全漏洞，对于不同服务提供商之间的接口，或MPLS是在服务提供商和客户间的接口上启动而言，这将很容易发生。

实用新型内容

本发明旨在提供一种路由装置，用于解决现有技术中在MPLS启动接口上接收欺骗的MPLS业务时所面临的安全漏洞问题。

在另一个实施例中，一种路由装置，包括：路由引擎，用于维护反映网络拓扑结构的路由信息；以及接口卡，其插于路由设备的

插槽中，电连接至路由引擎，并使用接口播发用于标签交换路径的标签，其中，一旦接收到具有标签的分组，则接口卡校验分组是否在最初用来播发标签的接口上接收到的。

在另一个实施例中，一种计算机可读介质，包括指令，其用于促使可编程处理器播发 LSP 标签，其中标签与接口相关，接收具有该标签的分组，并且校验分组是在该接口上接收到的。

本实用新型提供了维护网络安全的技术，且更具体来说，实现了检测和防范 MPLS 欺骗。这些技术允许以某种方式扩展与信令协议相关的软件模块，该方式允许路由装置检验多协议标签交换（MPLS）分组是否是从合法的、MPLS 标签实际上已被播发的上游路由装置所接收到的。所述技术可被应用到任何信令协议中，例如具有业务工程的资源预留协议（Resource Reservation Setup Protocol with Traffic Engineering，缩写为 RSVP-TE），标签分发协议（LDP），或者边界网关协议（BGP）。

附图说明

图 1 是示出根据本实用新型原理的一个系统实例的方框图，其中，标签交换路由器（LSR）对输入的多协议标签交换（MPLS）分组进行欺骗检查。

图 2 是示出根据本实用新型原理的对输入的 MPLS 分组进行欺骗检查的路由器的典型实施例的方框图。

图 3 是示出根据本实用新型原理的转发表实例的方框图，该转发表已被扩展以结合附加的欺骗检查域。

图 4 是示出用于虚拟路由器的示例性的远程自治系统表的方框图。

图 5 是示出与虚拟路由器和远程自治系统相关的接口表实例的方框图。

图 6 是示出具有欺骗检查域的另一个转发表实例的方框图。

图 7 是示出图 2 中路由器的操作实例的流程图。

具体实施方式

图 1 是示出根据本实用新型原理的一个系统 **10** 实例的方框图，其中，标签交换路由器（LSR）对输入的多协议标签交换（MPLS）分组 **15A** 和 **15B** 进行欺骗检查。在图 1 的例子中，LSR **12A**、**12B**、和 **12C** 通过 MPLS 协议进行通信，以发送标签交换路径（LSP）**17** 信号。一旦建立，LSP **17** 就将 MPLS 业务从作为源 LSR 的 LSR **12A** 携带到作为 LSP **17** 叶节点的 LSR **12C**。换句话说，MPLS 业务通过图 1 的 LSP **17** 从左向右流动。

在建立从 LSR **12A** 到 LSR **12C** 的 LSP 的进程期间，LSR **12C** 发送消息 **14B**，播发第一 MPLS 标签（例如标签 “**900**”）到其上游路由器 LSR **12B**。LSR **12B** 在接口 **16B** 上接收该标签播报，并且分配相应的第二 MPLS 标签，例如标签 “**300**”。LSR **12B** 在接口 **16A** 发送消息 **14A**，向 LSR **12A** 播发标签 **300**。

如下所述，一个或者多个 LSR **12** 可以利用与信令协议相关的软件模块，该软件模块已被扩展以实现本文描述的 MPLS 分组欺骗检查技术。此外，根据本实用新型的原理，LSR **12** 可基于每个 LSP 来指定执行欺骗检查的类型，由此提供精确级别（fine-grail level）的安全性。例如，LSR **12** 可利用与信令协议相关的软件模块来对每

个 LSP 指定是应该为特定的 LSP 执行欺骗检查、还是虚拟路由器欺骗检查、还是远程自治系统（AS）欺骗检查。

作为一个实例，假设 LSR **12** 利用扩展的软件模块要求对 LSP **17** 的接口欺骗检查。当 LSR **12B** 接收标有 MPLS 标签的 MPLS 分组时，LSR **12B** 在具有附加的欺骗检查域的 MPLS 转发表中查找所述标签，以确定接收该 MPLS 分组的接口是否就是接收具有期望的标签的 MPLS 分组的接口。这样，当 LSR **12B** 在接口 **16A** 接收具有标签 **300** 的 MPLS 分组 **12A** 时，LSR **12B** 确定接口 **16A** 是否就是该最初播发标签 **300** 的特定接口。在图 1 的例子中，LSR **12B** 确定通过接口 **16A** 播发标签 **300**。因此，LSR **12B** 接收 MPLS 分组、用第一 MPLS 标签 **900** 替换所述标签 **300**，并将得到的 MPLS 分组 **15C** 传送给 LSR **12C**。

然而，攻击者 LSR **18** 可能试图通过在接口 **16C** 上将具有标签 **300** 的 MPLS 分组 **15B** 发送给 LSR **12B**，而将 MPLS 插入到所述 LSP 中，企图将 LSR **12B** 标签交换至 **900** 并将 MPLS 分组传送到 LSR **12C** 上。在此情形中，LSR **12B** 没有在接口 **16C** 上将标签 **300** 播发给攻击者 LSR **18**。

一旦在接口 **16C** 上收到 MPLS 分组 **15B**，LSR **12B** 就确定没有在接口 **16C** 播发标签 **300**。LSR **12B** 丢弃 MPLS 分组 **15B** 且不将其传送至 LSR **12C**。在一个实施例中，将丢弃的分组计数、做日志记录、或收集，以便于进一步分析。由此，LSR **12B** 通过在转发入站的 MPLS 分组以前对其进行欺骗检查，以验证它们是在播发它们的标签的接口上接收到的，从而防止网络攻击。

虽然上面是参照一个点对点的 LSP 进行了说明，但本实用新型的原理可以很容易地应用于点对多点的（P2MP）LSP。此外，这些

技术可以应用于源发起的（source-initiated）或者叶发起的（leaf-initiated）LSP。

图2是示出根据本实用新型原理的对输入的MPLS分组进行欺骗检查的路由器**20**的典型实施例的方框图。在图2的典型实施例中，路由器**20**包括：接口卡**22A-22N**（统称IFC**22**），其分别通过网络链路**24A-24N**以及**26A-26N**接收和发送分组流。路由器**20**可包括机箱（未示出），其具有许多用于容纳一组包括IFC**22**的卡的插槽。每块卡都可插入到机箱的相应插槽中，以将卡通过高速交换模块（switch）**30**和内部数据路径**32A-32N**（统称为内部数据路径**32**）电连接（couple）至路由引擎**28**。

交换模块**30**还在每个IFC**22**之间提供互连路径。交换模块**30**可以包括，例如，交换结构（switch fabric）、交换装置（switchgear）、可配置的网络交换机或集线器、或者其它高速交换装置。内部数据路径**32**可包括任意形式的通信路径，例如在集成电路中的电路径、外部数据总线、光链路、网络连接、无线连接、或其它通信路径。通过多个物理接口（未示出），IFC**22**可以连接到网络链路**24A-24N**和**26A-26N**。

通常，路由引擎**28**用作路由器**20**的控制单元，并维护反映网络拓扑结构的路由信息，该路由信息由路由信息模块**34**保存。路由器**20**可为客户提供虚拟私人网络（VPN）服务。在多VPN的环境中，可将路由信息模块**34**保存的路由信息组织成逻辑上分离的路由信息数据结构。路由器**20**可用以下形式维护路由信息模块**34**保存的路由信息：一个或多个表、数据库、链接表、分叉树、平面文件、或者任何其他的数据结构。基于路由信息模块**34**保存的路由信息，路由引擎**28**生成IFC**22**的转发信息，这些转发信息保存于转发信息模块**40A-40N**（转发信息模块**40**）。在多VPN的环境中，

转发信息模块 **40** 中保存的转发信息可类似地组织成逻辑上分离的路由信息数据结构。

每个 IFC **22** 都包括：转发部件（未示出），用于根据转发信息模块 **40** 中保存的转发信息以及由路由引擎 **28** 生成的 MPLS 转发表来转发分组，这些转发表保存于转发表模块 **42A-42N**（MPLS 转发表 **42**）中。具体来说，IFC **22** 转发部件基于转发信息模块 **40** 中保存的转发信息来确定对每个入站分组的下一跳，确定关于该下一跳的相应 IFC，并通过交换模块 **30** 和数据路径 **32**，将这些分组中继到合适的 IFC。

虽然未单独示出，但转发信息模块 **40** 中保存的转发信息可以包括"全局"转发信息（例如，与公共网相关的转发信息）以及与路由器 **20** 所提供的任何 VPN 相关的 VPN 路由和转发表（VPN Routing and Forwarding table，缩写为 VRF）。在所提供的 VPN 服务中，路由器 **20** 可以对每个 VPN 维护逻辑上隔离的转发表。例如，路由器 **20** 可为每个 VPN 维护一张 VRF 表。

路由引擎 **28** 为至少一个在路由引擎 **28** 中执行的信令协议提供操作环境，该信令协议保存于信令协议模块 **36** 中。信令协议模块 **36** 中保存的信令协议可以是一个协议，例如，诸如资源预留协议（Resource Reservation Protocol，缩写为 RSVP）的协议、标签分发协议（Label Distribution Protocol，缩写为 LDP）、或者边界网关协议（Border Gateway Protocol，缩写为 BGP）。可以扩展与信令协议模块 **36** 中保存的信令协议相关的软件模块以实现本文描述的 MPLS 分组欺骗检查技术。例如，与信令协议模块 **36** 中保存的信令协议相关的软件模块可确定执行的欺骗检查类型，以用于与各自标签相关的各个 LSP，由此提供精确级别的安全性。

在一个实施例中，对于单个 LSP 而言，与信令协议模块 **36** 中保存的信令协议相关的软件模块可指定三种不同类型的MPLS欺骗检查：（1）接口欺骗检查，（2）虚拟路由器欺骗检查，或者（3）远程自治系统（AS）欺骗检查。为方便这三种类型的 MPLS 欺骗检查，路由器 **20** 维护远程自治系统表模块 **38** 中保存的远程 AS 表（“远程 AS 表模块 **38**”）、MPLS 转发表模块 **42A-42N** 中保存的转发表以及 MPLS 接口表模块 **44A-44N** 中保存的接口表。

通常，远程 AS 表模块 **38** 中保存的远程 AS 表将编号与关于路由器 **20** 的远程自治系统关联起来，以高效利用 MPLS 转发表模块 **42** 中保存的转发表欺骗检查域中的位。

在 IFC **22** 中维护 MPLS 转发表模块 **42** 中保存的转发表和 MPLS 接口表模块 **44A-44N**（MPLS 接口表模块 **44**）中保存的接口表，以用于对输入的 MPLS 分组进行欺骗检查。MPLS 转发表模块 **42** 中保存的转发表把与输入的 MPLS 分组相关的标签与下一跳关联起来。根据本实用新型的原理，将 MPLS 转发表模块 **42** 中保存的转发表扩展，使其包括附加的欺骗检查域，以存储每个转发项的欺骗检查信息。MPLS 接口表模块 **44** 中保存的接口表把接口编号与虚拟路由器或 VRF 或逻辑路由器或独立的路由表、以及远程 AS 编号关联起来。在下文中更详细地讨论这些表。

在一个实施例中，路由引擎 **28** 可维护 MPLS 转发表模块 **42** 中保存的转发表和 MPLS 接口表模块 **44** 中保存的接口表的原版拷贝，并可以分发这些表的拷贝给每个 IFC **22**。路由引擎 **28** 可对 MPLS 转发表模块 **42** 中保存的转发表和 MPLS 接口表模块 **44** 中保存的接口表增加、去除、或修改项目，并且可分发更新过的拷贝给 IFC **22**。在另一实施例中，路由引擎 **28** 可分析在 MPLS 转发表模块 **42** 中保存的转发表和 MPLS 接口表模块 **44** 中保存的接口表中的信息，并

基于与每个 IFC **22** 都相关的接口，仅仅发送每个 IFC **22** 都需要的转发信息。

当路由器 **20** 经由链路 **24A** 在 IFC **22A** 中接收输入的 MPLS 分组时，IFC **22A** 使用 MPLS 转发表模块 **42A** 中保存的转发表和 MPLS 接口表模块 **44A** 中保存的接口表对分组进行指定类型的 MPLS 欺骗检查。例如，路由器 **20** 可确定分组是否是在最初播发该标签的接口上被接收。若是，路由器 **20** 则根据相应的一个 MPLS 转发表模块 **42** 中保存的转发表来传送分组。然而，如果接收该分组接口并不是最初用来播发标签的接口的话，则路由器 **20** 可以丢弃该分组。可以对丢弃的分组计数、做日志记录、或收集，用于进一步分析。

图 2 中示出的路由器 **20** 的实施例示出了典型的用途。可选地，路由器 **20** 可以包括具备路由引擎和转发引擎的集中控制单元。在此实施例中，转发功能性没有分配给 IFC **22**，而是集中在传送引擎中。此外，本实用新型的原理可以在三层交换机（layer three switch）或者其它设备之中实现。但是，为方便图示，本实用新型的原理在路由器 **20** 的前后关系中示出。

通常，上述过程，包括所述 MPLS 分组的欺骗检查，可作为从一个或多个计算机可读介质中取出的可执行指令来实现。这种介质的实例包括随机存储器（RAM）、只读存储器（ROM）、非易失性随机存储器（NVRAM），电可擦可编程只读存储器（EEPROM）、闪存等等。此外，可通过一个或多个处理器、分立的硬件电路、固件、在可编程处理器上执行的软件、或以上的任意组合来执行计算机可读介质的指令来实现上述过程的功能。

图 3 示出了 MPLS 转发表模块 **42** 中保存的转发表实例的方框图，如图所示，扩展了 MPLS 转发表模块 **42** 中保存的转发表，使其每个转发项包括附加的欺骗检查域。路由器（例如图 1 中的 LSR

12B）在对输入的 MPLS 分组进行欺骗检查时使用 MPLS 转发表模块 **42** 中保存的转发表。

内标签（in-label）域 **52** 包括一组 MPLS 网络中可能已经播发给 LSP 的上游 LSR 的虚拟路由器的标签。下一跳（next-hop）域 **54** 包含一组与其标签相对应的分组的目标路由器。当路由器 **12B** 接收 MPLS 分组时，路由器 **12B** 就在 MPLS 转发表模块 **42** 中保存的转发表中查找该分组的标签，以确定此分组转发只何处。MPLS 转发表模块 **42** 中保存的转发表中增加了欺骗检查（spoof-check）域 **56**，以检查从上游 LSR 接收的 MPLS 分组是否包含最初播发给在接收该分组的接口上的 LSR 的 MPLS 标签。

例如，对于每个输入的标签来说，欺骗检查域 **56** 包括允许标签到达其上的接口组，即，播发该标签的接口组。当接收到标上标签 **300** 的分组时，LSR **12B** 在 MPLS 转发表模块 **42** 中保存的转发表中查找标签 **300**，确定标签 **300** 仅能在接口 **16A** 上被接收。如以上参照图 1 的说明，如果标有标签 **300** 的分组改为到达接口 **16C** 的话，则 LSR **12B** 可以丢弃该分组。

作为另一实例，当接收标上标签 **500** 的分组时，LSR **12B** 在 MPLS 转发表模块 **42** 中保存的转发表中查找标签 **500**，确定标签 **500** 可以在接口 **16B** 或 **16H** 上被接收。可使用诸如内容可寻址存储器（CAM）的硬件来检查每个输入的 MPLS 分组的欺骗检查域 **56** 中的接口组。

在 MPLS 接口为多路访问接口（例如，以太网）的情况下，欺骗检查域 **56** 还可以包括被播发标签的上游 LSR 第二层（L2）地址（如以太网介质访问控制（Media Access Control，缩写为 MAC）地址）。

在此方式中，图 3 示出了一个实施例，其中 MPLS 转发表模块 **42** 中保存的转发表的欺骗检查域 **56** 包括整套可允许的接口。但是，在大系统中，接口的数量可能是相当大的，欺骗检查域 **56** 中包含的数据量也可能是相当大的。

图 4 是示出路由器例如图 2 的路由器 **20** 的远程 AS 表模块 **38** 中保存的远程 AS 表实例的框图。远程 AS 表模块 **38** 中保存的远程 AS 表将编号与每个远程 AS 关联，其中，路由器 **20** 可由这些远程 AS 接收 MPLS 分组。例如，编号域 **60** 包括编号 0-N。远程 AS 域 **62** 包括远程自治系统的号码、名称或其它标识符。在图 4 的实例中，路由器 **20** 从仅仅三个远程自治系统中接收 MPLS 分组。因此，没有使用编号 3-N。随着网络变化，路由引擎 **28** 可以更新远程 AS 表模块 **38** 中保存的远程 AS 表，以添加增添的远程自治系统。在一个实施例中，可以使用编号“0”指示有路由器 **20** 驻留其中的自治系统。

可将关于远程自治系统的编号（“远程 AS 编号”）用在 MPLS 转发表模块 **42** 中保存的转发表和 MPLS 接口表模块 **44** 中保存的接口表中，从而以更高效的方式指示远程自治系统。例如，在一些实施例中，远程 AS 编号可有助于高效地使用 MPLS 转发表模块 **42** 中保存的转发表欺骗检查域中的位。

图 5 是示出路由器例如图 2 的路由器 **20** 的 MPLS 接口表模块 **44** 中保存的接口表实例的框图。MPLS 接口表模块 **44** 中保存的接口表将接口与虚拟路由器和远程自治系统关联。

编号域 **68** 包括编号 0-N，其与诸如图 1 中的接口 **16** 的接口相关联。虚拟路由器域 **70** 包括号码、名称、或虚拟路由器的其它标识符，指示相应接口为其一部分的虚拟路由器。例如，根据图 5，

接口 **0** 和 **1** 为虚拟路由器 **0** 的一部分，而接口 **2**、**3**、**4** 和 **N** 为虚拟路由器 **1** 的一部分。

远程 AS 编号域 **72** 包括远程 AS 编号，指示远程 AS，其中，来自于该远程 AS 的 MPLS 业务被期望在相应接口上。如果为到另一个服务提供商的外部 BGP（EBGP）会话，其中，通过该会话交换路由和标签，则可以将特定接口与该 EBGP 会话关联。

因此，MPLS 接口表模块 **44** 中保存的接口表和远程 AS 表模块 **38** 中保存的远程 AS 表可以一起用来确定接口，其中，来自于特定的远程 AS 的 MPLS 业务被期望在该接口上。在图 5 的例子中，来自远程 AS **1000** 的 MPLS 业务被期望在接口 **0**、**1** 和 **2** 上，来自远程 AS **2000** 的 MPLS 业务被期望在接口 **3** 上，来自远程 AS **3000** 的 MPLS 业务被期望在接口 **4** 和 **N** 上。在一个实施例中，远程 AS 编号域 **72** 中的远程 AS 编号“0”可以指示该接口通往与路由器 **20** 相同的自治系统之中的路由器。这可能意味着或是 BGP 不在该接口上启动，或是该会话为内部 BGP（IBGP）会话。

图 6 是示出具有附加欺骗检查域的 MPLS 转发表 **75** 的另一个实施例的框图。类似于图 3 的 MPLS 转发表，内标签域 **76** 包括一组标签，其中，在 MPLS 网络中的虚拟路由器可已经播发给 LSP 的上游 LSR。下一跳域 **78** 包括一组与其标签相对应的分组的目标路由器。

图 6 中的 MPLS 转发表 **75** 不同于图 3 中的 MPLS 转发表模块 **42** 中保存的转发表，因为，在图 6 中，MPLS 转发表 **75** 的欺骗检查域不包括整套接口，其中，路由器 **12B** 可从这些接口接收分组。相反地，MPLS 转发表的欺骗检查域 **80** 针对欺骗检查进程的空间和时间效率进行了结构化。在图 6 的实例中，欺骗检查域 **80** 有 32 位。在另外的实施例中，欺骗检查域 **80** 可包括其他数量的位。

如图 6 所示，欺骗检查域 **80** 的头两位表示针对相应标签所要求的欺骗检查类型。在此实施例中，可以指定欺骗检查的三种类型中的任意一种。例如，欺骗检查类型可以是设计用于资源预留协议（RSVP）的接口欺骗检查、设计用于标签分发协议（LDP）的虚拟路由器欺骗检查、或者是设计用于边界网关协议（BGP）的远程 AS 欺骗检查。

在一个实施例中，由头两位为“00”指明接口欺骗检查类型。在接口欺骗检查中，欺骗检查域中余下的 30 位确定内标签栏 **76** 中的相应标签必须的接口。在此实施例中，如果接口为多路访问（multi-access）（例如，以太网），仅仅该接口进行欺骗检查，而不是 L2 地址（例如，MAC 地址）。在图 6 的实例中，标签 **300** 和 **400** 对应于接口类型欺骗检查，这是由于相应欺骗检查域项中的头两位为“00”。根据欺骗检查栏 **80** 中的欺骗检查信息，标签 **300** 必须到达接口 **4** 上，标签 **400** 必须到达接口 **5** 上。

在另一个实施例中，由头两位为“11”来表示第二类型的接口欺骗检查。在第二类型的接口欺骗检查中，欺骗检查域中余下的 30 位可以确定两个内标签栏 **76** 中的相应标签可以到达的接口。这可以用于检查例如，何处存在将传送 MPLS 业务的第一接口，以及何处存在可以将 MPLS 业务快速路由到自己的第二接口。在此实施例中，前 15 位可以确定第一接口，余下的 15 位可以确定第二接口。在图 6 的实例中，标签 N 对应于第二类型的接口欺骗检查，这是由于相应欺骗检查项的头两位为“11”。根据欺骗检查栏 **80** 中的欺骗检查信息，标签 N 可到达接口 0 或接口 5。

欺骗检查域 **80** 中的头两位为“01”表示虚拟路由器欺骗检查类型。在虚拟路由器欺骗检查中，欺骗检查域中余下的 30 位确定包含了内标签栏 **76** 中的相应标签可以到达的接口的虚拟路由器。在图 6 的实例中，标签 **500** 对应于虚拟路由器类型的欺骗检查，这

是由于相应的欺骗检查域项的头两位为“01”。根据欺骗检查栏 **80** 中的欺骗检查信息，标签 **500** 必须到达虚拟路由器 **0** 中的接口。重新参照图 5 的 MPLS 接口表模块 **44** 中保存的接口表，其示出了接口 **0** 和 **1** 在虚拟路由器 **0** 之中。因此，标签 **500** 既可以到达接口 **0** 上又可以到达接口 **1** 上。

可以由欺骗检查域 **80** 中的头两位为“10”表示远程 AS 欺骗检查类型。在远程 AS 欺骗检查中，欺骗检查域中余下的 30 位确定包含有标签内栏 **76** 中的相应标签必须到达的接口的远程自治系统组。特别地，每一位从右到左映像到图 4 的远程 AS 表的远程 AS 编号之一。如果将该位设为“1”，则指示了相应的远程 AS 编号。

在图 6 的实例中，标签 **600** 和 **700** 对应于远程 AS 欺骗检查类型，这是由于相应欺骗检查域项的头两位为“10”。根据欺骗检查栏 **80** 中的欺骗检查信息，标签 **600** 必须到达与具有编号 1 的远程 AS 相关的接口。根据 MPLS 接口表模块 **44** 中保存的接口表，接口 **3** 与远程 AS 编号 1 相关。因此，标签 **600** 必须到达接口 **3** 上。

根据欺骗检查栏 **80** 中的欺骗检查信息，标签 **700** 可以到达或是与远程 AS 编号 0 相关的接口或是与远程 AS 编号 2 相关的接口。根据 MPLS 接口表模块 **44** 中保存的接口表，接口 **0**、**1** 和 **2** 与远程 AS 编号 0 相关，接口 **4** 和 **5** 与远程 AS 编号 2 相关。因此，标签 **700** 可以到达接口 **0**、**1**、**2**、**4**、和 **5** 上。

图 7 是示出根据本实用新型原理来进行 MPLS 欺骗检查的网络设备的典型操作的流程图。该网络设备可以基本类似于图 2 中所示出的路由器 **20**。

最初，路由器 **20** 在接口 *I*（**82**）上接收具有内标签 *L* 的 MPLS 分组。如图 2 所示，路由器 **20** 在 MPLS 接口表（**84**）中查找接口 *I*。

如果路由器 **20** 在 MPLS 接口表中没找到接口 *I*，则路由器 **20** 丢弃该分组（**86**），这是由于此就指明了 MPLS 在接口 *I* 上没有启动。在一个实施例中，可以对丢弃的分组计数、做日志记录、或进行收集，用于进一步分析。如图 2 所示，如果路由器 **20** 在该 MPLS 接口表中确实找到了接口 *I*，则路由器 **20** 就在 MPLS 转发表（**88**）中查找标签 *L*。如果路由器 **20** 在所述 MPLS 转发表中没找到标签 *L*，则路由器 **20** 丢弃该分组（**86**），这是由于其表明路由器 **20** 没有播发标签 *L*。

路由器 **20** 在对应于标签 *L* 的 MPLS 转发表项中检查欺骗检查域 **80**（图 6），以确定所需的欺骗检查类型。在图 6 的实施例中，欺骗检查域中的头两位表示欺骗检查的类型。如果欺骗检查域表示欺骗检查类型为接口欺骗检查（**90**）（在一个实施例中由“00”所表示），则路由器 **20** 从欺骗检查域 **80** 中提取期望的 MPLS 接口 *I'*。路由器 **20** 将分组到达的实际接口 *I* 与期望的接口 *I'*（**92**）相比较。如果实际接口 *I* 与期望的接口 *I'*相同，则路由器 **20** 根据在用于此内标签（**94**）的 MPLS 转发表项中的下一跳来转发该 MPLS 分组。如果实际接口不同于期望的接口，则路由器 **20** 丢弃该分组（**86**），这是由于该分组是从一个路由器 **20** 并没有对其播发该标签的 LSR 所接收到的。

在另一实施例中，由“**11**”所表示的欺骗检查域可以表示第二类型的接口欺骗检查。可以使用第二类型的接口欺骗检查例如，何处存在传送 MPLS 业务的第一接口，以及何处存在可以将 MPLS 业务快速路由到自己的第二接口。在第二类型的接口欺骗检查中，路由器 **20** 可从接口欺骗检查域中提取两个期望的接口，其中标签可以到达该接口上。在此情形，路由器 **20** 将分组到达的实际接口 I 与这两个期望接口（**92**）相比较。如果实际接口与任何一个期望接口相同，则路由器 **20** 根据此内标签域（**94**）的 MPLS 转发表项中的下一跳来转发 MPLS 分组。如果实际接口不同于任意一个期望的

接口，则路由器 **20** 丢弃该分组（**86**），这是由于所述分组是从一个路由器 **20** 并没有对其播发该标签的 LSR 所接收到的。

如果在一个实施例中，通过“01”所表示的欺骗检查域表示欺骗检查类型为虚拟路由器欺骗检查（“VR 欺骗检查类型”**96**）的话，则路由器 **20** 从欺骗检查域中提取期望的虚拟路由器 *R'*。路由器 **20** 将对应于标签所实际到达的接口的实际虚拟路由器 *V* 与期望的虚拟路由器 *R'*（**32**）相比较。如果实际虚拟路由器 *V* 与期望的虚拟路由器 *R'*相同，则路由器 **20** 根据此内标签域（**94**）的 MPLS 转发表项中的下一跳来转发 MPLS 分组。如果实际虚拟路由器不同于期望的虚拟路由器，则路由器 **20** 丢弃该分组（**86**），这是由于所述分组是从一个路由器 **20** 并没有对其播发该标签的 LSR 所接收到的。

如果在一个实施例中由“**10**”所表示的欺骗检查域表示欺骗检查类型为远程 AS 欺骗检查（**100**），则路由器 **20** 从欺骗检查域中提取允许的远程 AS 编号组 *A'*。路由器 **20** 将对应于标签实际到达过的接口的实际远程 AS 编号 *A* 与允许的多个远程 AS 编号（**102**）相比较。如果实际远程 AS 编号在允许的远程 AS 编号组之中，则路由器 **20** 根据此内标签域（**104**）的 MPLS 转发表项中的下一跳来转发 MPLS 分组。如果实际远程 AS 编号不在允许的远程 AS 编号组之中，则路由器 **20** 丢弃分组（**86**），这是由于所述分组是从一个路由器 **20** 并没有对其播发该标签的 LSR 所接收到的。

以上说明了本实用新型的各种实施例。这些及其他的实施例均包括在所附的权利要求书的范围内。

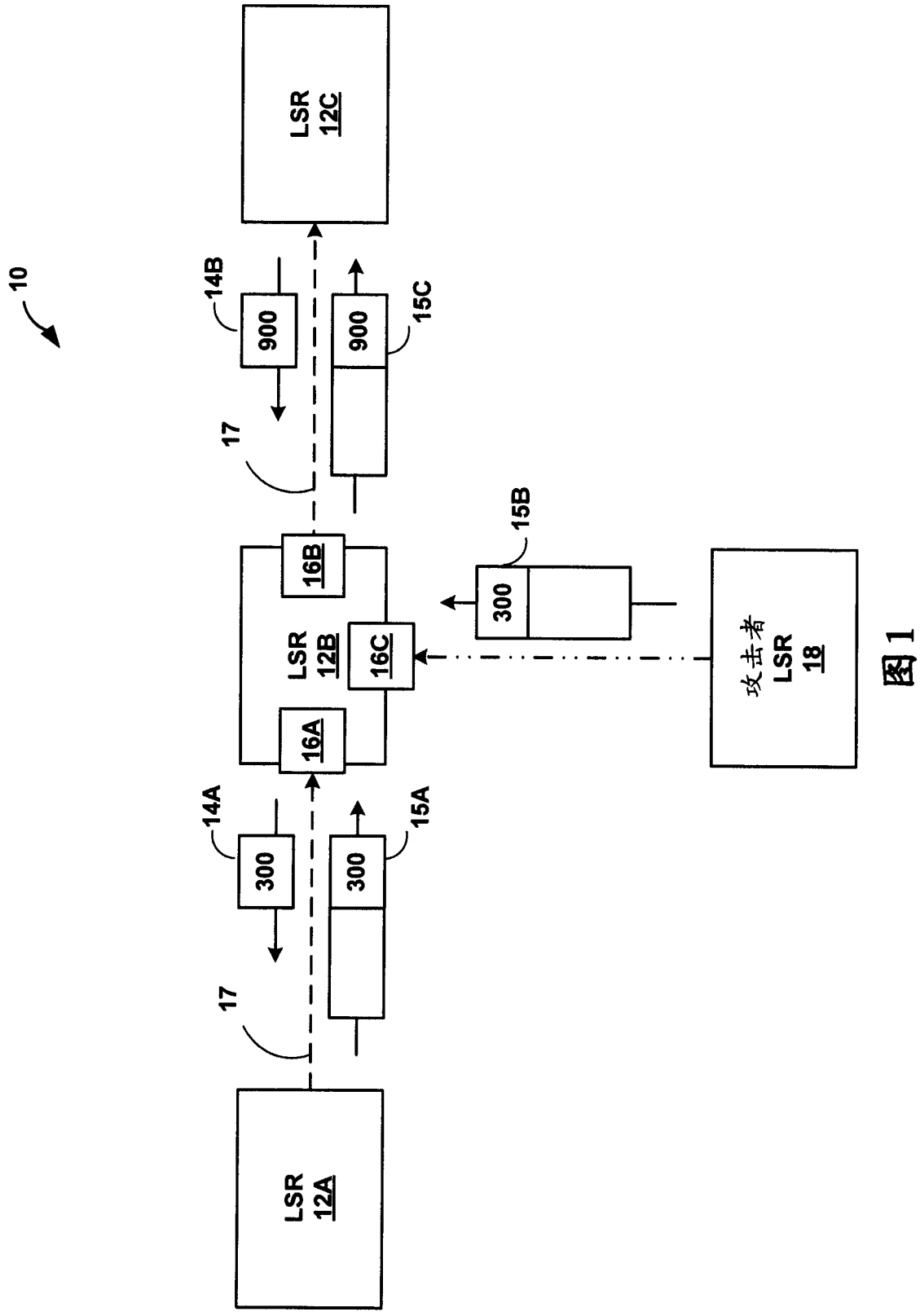

10
LSR 12C
14B
900
900
15C
17
15B
16B
300
LSR 12B
16C
攻击者 LSR 18
16A
14A
300
300
15A
17
LSR 12A

图 1

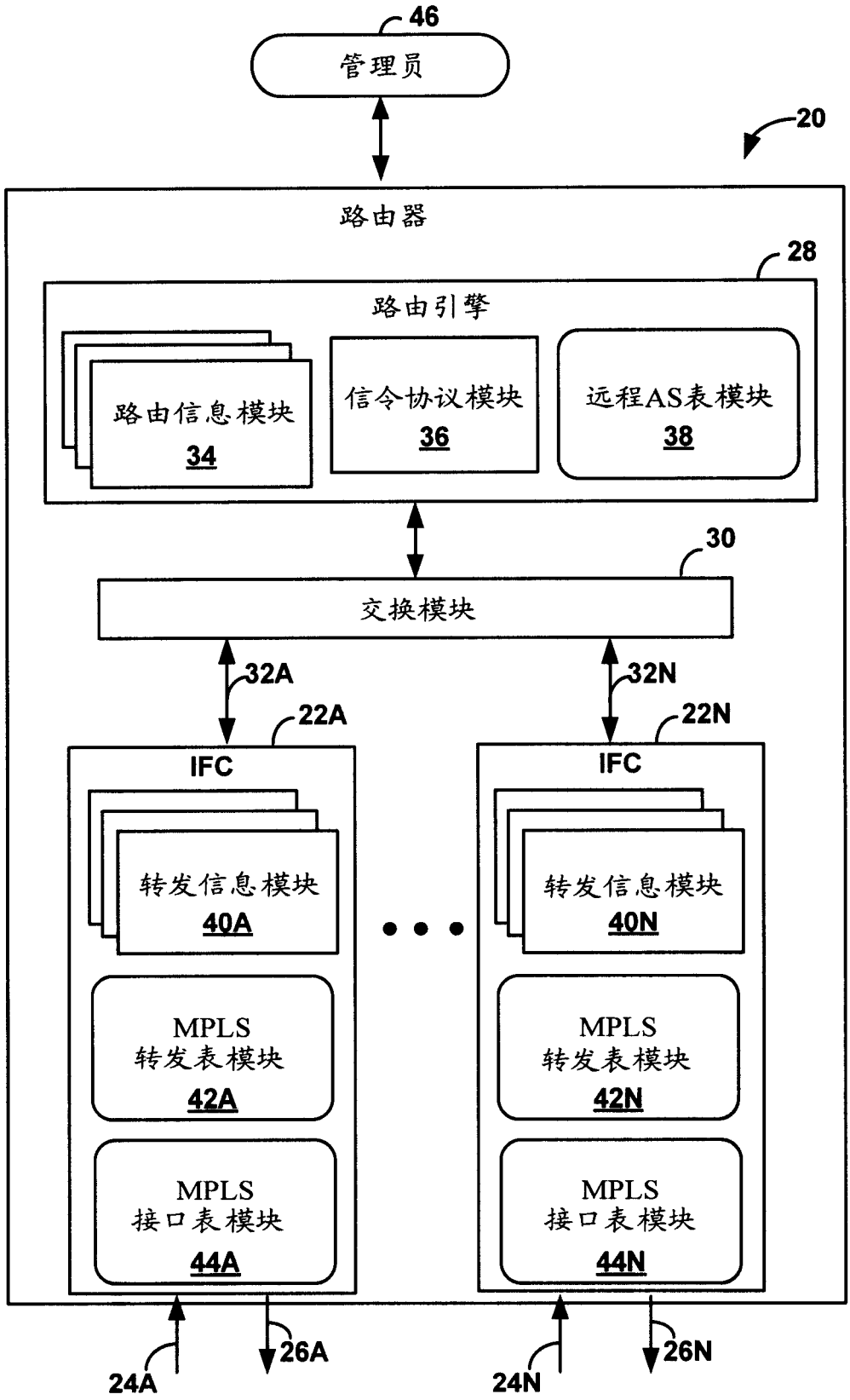

46
管理员
20
路由器
28
路由引擎
路由信息模块
34
信令协议模块
36
远程AS表模块
38
30
交换模块
32A
32N
22A
22N
IFC
IFC
转发信息模块
40A
转发信息模块
40N
MPLS
转发表模块
42A
MPLS
转发表模块
42N
MPLS
接口表模块
44A
MPLS
接口表模块
44N
24A
26A
24N
26N

图2

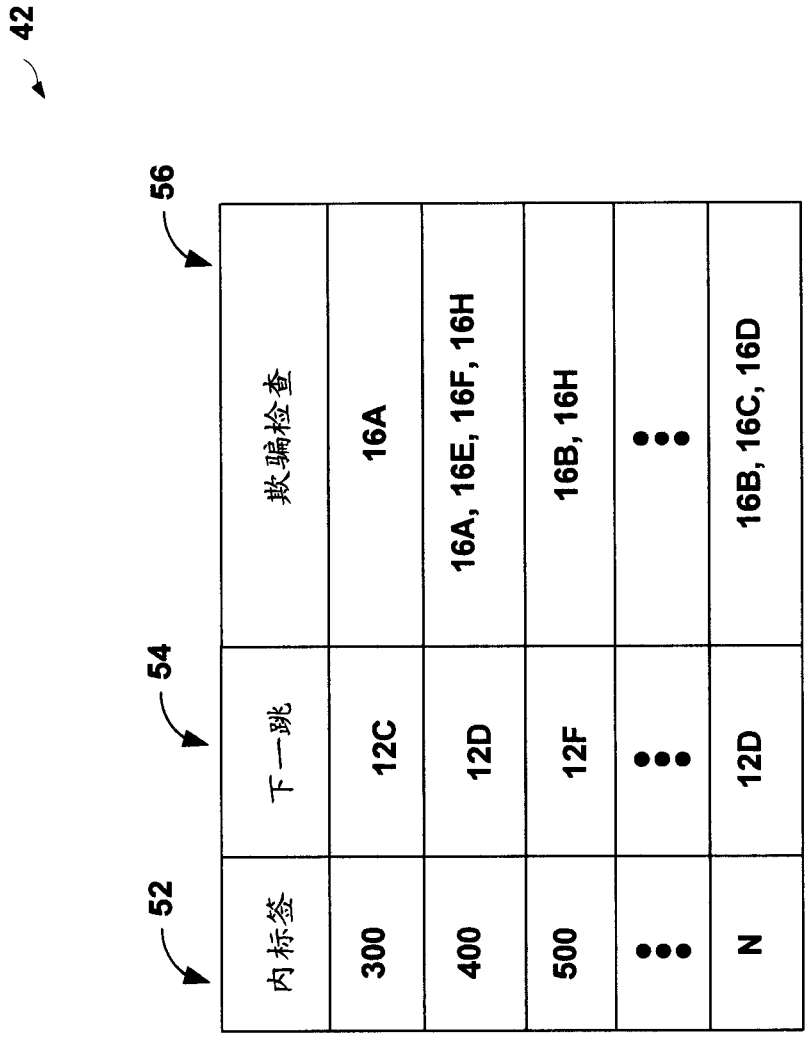

42
52
54
56
内标签
下一跳
欺骗检查
300
12C
16A
400
12D
16A, 16E, 16F, 16H
500
12F
16B, 16H
N
12D
16B, 16C, 16D

图3

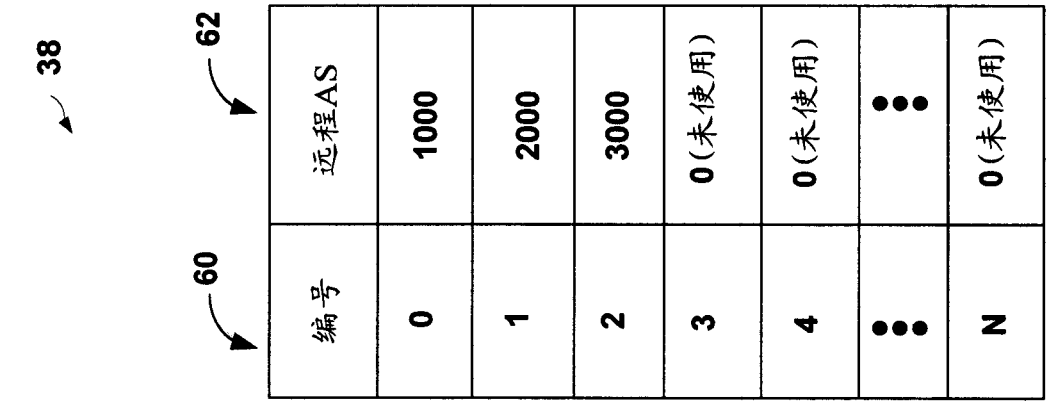

38
60
62
编号
远程AS
0
1000
1
2000
2
3000
3
0(未使用)
4
0(未使用)
N
0(未使用)

图4

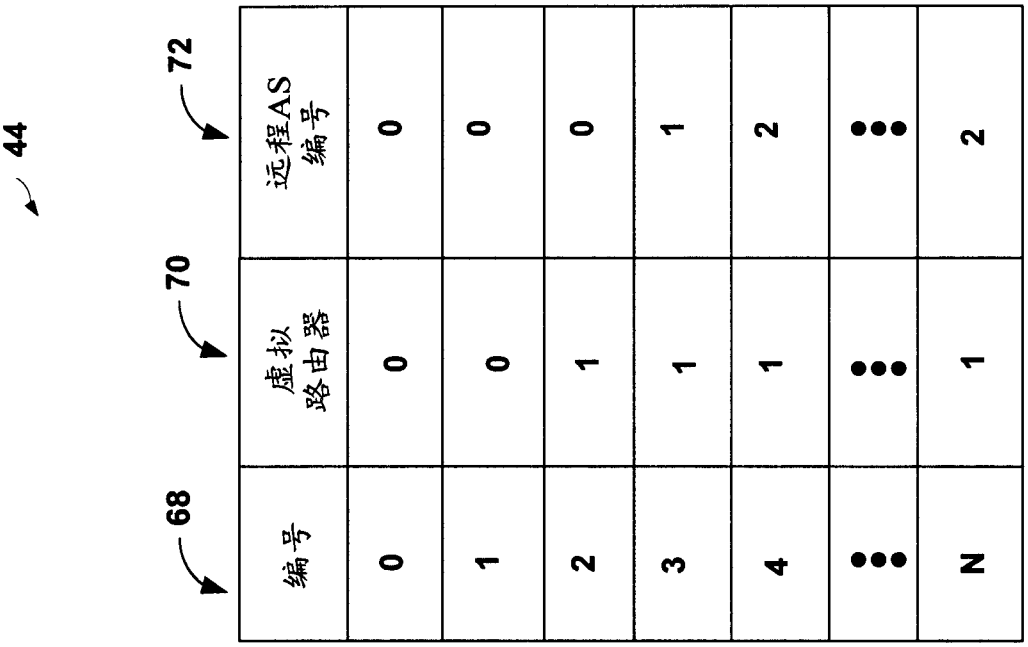

44
68
70
72
编号
虚拟路由器
远程AS编号
0
0
0
1
0
0
2
1
0
3
1
1
4
1
2
N
1
2

图5

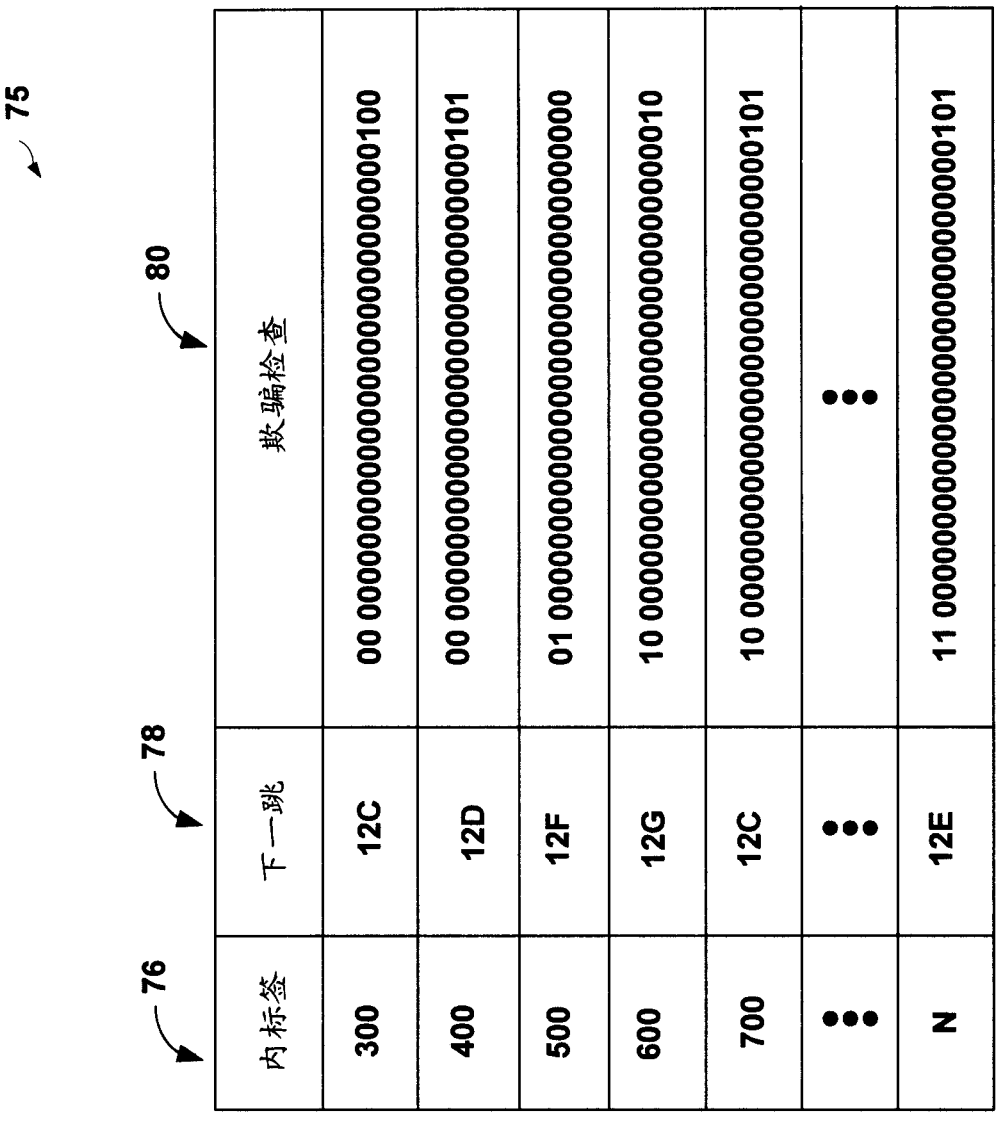

75
76
78
80
内标签
下一跳
欺骗检查
300
12C
00 0000000000000000000000000100
400
12D
00 0000000000000000000000000101
500
12F
01 0000000000000000000000000000
600
12G
10 0000000000000000000000000010
700
12C
10 0000000000000000000000000101
N
12E
11 0000000000000000000000000101

图6

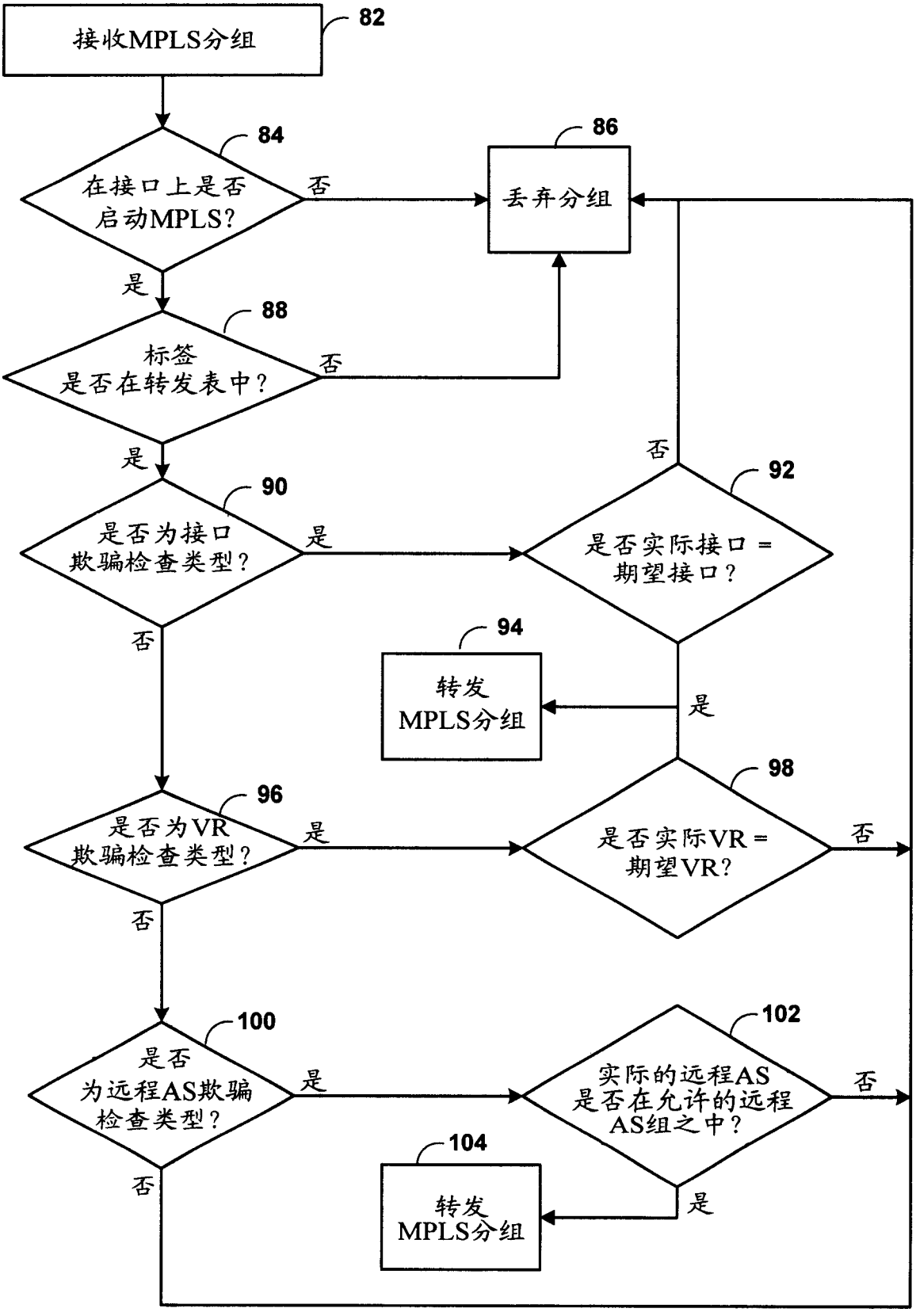

接收MPLS分组
82
在接口上是否启动MPLS?
84
否
丢弃分组
86
是
标签是否在转发表中?
88
否
是
是否为接口欺骗检查类型?
90
是
否
是否实际接口=期望接口?
92
否
转发MPLS分组
94
是
是否为VR欺骗检查类型?
96
是
否
是否实际VR=期望VR?
98
否
是否为远程AS欺骗检查类型?
100
是
否
实际的远程AS是否在允许的远程AS组之中?
102
否
是
转发MPLS分组
104

图7