

## 隧道切换方法、装置及交换机

### 技术领域

本发明涉及通信领域，具体而言，涉及隧道切换方法、装置及交换机。

### 背景技术

5       多协议标签交换（Multi-Protocol Label Switching，简称为 MPLS）三层虚拟专用网（Layer3 Virtual Private Network，简称为 L3VPN）是服务提供商 VPN 解决方案中一种基于服务提供商边缘（Provider Edge，简称为 PE）的 L3VPN 技术，它使用边界网关协议（Border Gateway Protocol，简称为 BGP）在服务提供商骨干网上发布 VPN 路由，使用 MPLS 在服务提供商骨干网上转发 VPN 报文。

10       MPLS L3VPN 组网方式灵活、可扩展性好，并能够方便地支持 MPLS 服务质量（Quality of Service，简称为 QoS）和 MPLS 流量工程（Traffic Engineering，简称为 TE），因此得到越来越多的应用。

MPLS L3VPN 模型由三部分组成：用户边缘（Customer Edge，简称为 CE）设备、PE 设备和服务提供商（Provider，简称为 P）设备。

15       CE 设备，又称为用户网络边缘设备，有接口直接与服务提供商（Service Provider，简称为 SP）相连。CE 可以是设备或交换机，也可以是一台主机。CE “感知”不到 VPN 的存在，也不需要必须支持 MPLS。

PE 设备，又称为服务提供商边缘设备，是服务提供商网络的边缘设备，与用户的 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上。

20       P 设备，是服务提供商网络中的骨干设备，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力。

CE 和 PE 的划分主要是根据 SP 与用户的管理范围，CE 和 PE 是两者管理范围的边界。

CE 设备通常是一台路由器，当 CE 与直接相连的 PE 建立邻接关系后，CE 把本站  
25       点的 VPN 路由发布给 PE，并从 PE 学到远端 VPN 的路由。CE 与 PE 之间使用 BGP/

内部网关协议（Interior Gateway Protocol，简称为 IGP）交换路由信息，也可以使用静态路由。

PE 从 CE 学到 CE 本地的 VPN 路由信息后，通过 BGP 与其它 PE 交换 VPN 路由信息。PE 路由器只维护与它直接相连的 VPN 的路由信息，不维护服务提供商网络中的所有 VPN 路由。

P 路由器只维护到 PE 的路由，不需要了解任何 VPN 路由信息。

当在 MPLS 骨干网上传输 VPN 流量时，入口 PE 作为入口（Ingress）标签交换路由器（Label Switch Router，简称为 LSR），出口 PE 作为出口（Egress）LSR，P 路由器则作为中转（Transit）LSR。

10 基于 L3VPN 业务报文转发的可靠性考虑，在组网时可以考虑采用 VPN 快速重路由（Fast ReRoute，简称为 FRR）、线性隧道保护组和环网保护组对 L3VPN 业务进行保护，三种保护类型可以进行自由组合。

图 1 是一种三种保护类型叠加保护 L3VPN 业务的系统结构示意图，如图 1 所示，CE1 与 CE2 之间是一条 L3VPN 业务，PE1->PE2 的路径和 PE1->PE3 的路径构成 VPN FRR，其中 PE1->PE2 的路径为主 VPN，PE1->PE3 的路径为备 VPN；PE1->PE2 的两条路径 PE1->P1->PE2 与 PE1->P2->PE2 构成主 VPN 线性隧道保护组；PE1->PE3 的两条路径 PE1->P3->PE3 与 PE1->P4->PE3 构成备 VPN 线性隧道保护组；PE1->P1->PE2 构成主 VPN 环网保护组的主隧道；PE1->P1->PE2->P2->PE1 构成主 VPN 环网保护组的备隧道，也是一个环隧道；同样的，PE1->P3->PE3 构成备 VPN 环网保护组的主隧道；PE1->P3->PE3->P4->PE1 构成备 VPN 环网保护组的备隧道，也是一个环隧道。通过 VPN FRR、线性隧道保护组以及环网保护组构成了 L3VPN 业务的三层叠加保护。

图 2 是根据相关技术的一种为 PE 设备 MPLS L3VPN 上行处理的流程示意图，图中描述了 ASIC 芯片的 L3VPN 的处理流程，通过路由查找得到下一跳转发信息进行转发。

25 图 3 是根据相关技术的三层叠加保护方法的切换过程示意图，图 3 示出了传统 MPLS L3VPN VPN FRR 切换的原理，即：首先创建所有可能的下一跳转发表（最多可能有 8 个），当需要切换的时候根据线性隧道保护组状态、环网保护组状态以及 VPN 保护组三种保护组状态决定最终的转发下一跳，当 VPN 保护组状态发生变化或者每个隧道保护组状态发生变化都需要进行判断是否需要切换下一跳，在耗费了大量的下一跳资源（即创建的下一跳转发表）的同时，流程的复杂性也较大，例如，如果是隧道

保护组状态发生变化，还需要将隧道保护组上的每条业务（即业务路由）都要分别进行切换，这样在业务很多时隧道保护组的切换的时间将达不到 50ms 的要求。

针对相关技术中的三层叠加保护中分别对每条业务路由进行切换导致的时延过长的问题，目前尚未提出有效的解决方案。

## 5 发明内容

本发明实施例提供了一种隧道切换方法、装置及交换机，以至少解决相关技术中的三层叠加保护中分别对每条业务路由进行切换导致的时延过长的问题。

根据本发明实施例的一个方面，提供了一种隧道切换方法，包括：将隧道保护组上的业务路由的类标识设置为第一类标识，其中，所述隧道保护组包括第一隧道和第二隧道；根据所述第一类标识，确定所述业务路由的重定向规则；根据所述重定向规则

10 和所述第二隧道的隧道信息，将所述业务路由从所述第一隧道切换到所述第二隧道。

优选地，根据所述第一类标识，确定所述业务路由的所述重定向规则包括：根据所述第一类标识，查询访问控制列表；确定所述访问控制列表中与所述第一类标识对应的所述重定向规则。

15 优选地，在查询所述访问控制列表之前，所述方法还包括：根据所述隧道保护组的工作状态，确定将所述业务路由切换到所述第二隧道；根据所述第二隧道的隧道信息，更新所述访问控制列表中与所述第一类标识对应的所述重定向规则。

优选地，根据所述重定向规则和所述第二隧道的隧道信息，将所述业务路由从所述第一隧道切换到所述第二隧道包括：根据所述重定向规则和所述第二隧道的隧道信息，分别为所述隧道保护组中的每个业务路由配置一个下一跳信息；分别根据配置的下一跳信息，将对应的业务路由从所述第一隧道切换到所述第二隧道。

20

优选地，根据所述重定向规则和所述第二隧道的隧道信息，分别为所述隧道保护组中的每个业务路由配置一个下一跳信息包括：根据所述重定向规则中用于切换到所述第二隧道的下一跳的出端口信息，配置每个业务路由的下一跳信息中的出端口信息；根据所述第二隧道上的服务提供商边缘设备的目的媒体访问控制地址信息和所述第二隧道的三层接口信息，配置每个业务路由的下一跳信息中的目的媒体访问控制地址信息和三层接口信息。

25

优选地，所述第一隧道和所述第二隧道分别为所述隧道保护组的主隧道和备隧道中的一个和另一个。

优选地，在将所述隧道保护组上的所述业务路由的所述类标识设置为所述第一类标识之前，所述方法还包括：确定将所述业务路由切换到所述隧道保护组，其中，所述隧道保护组为线性隧道保护组或环网保护组。

优选地，在确定将所述业务路由切换到所述隧道保护组之前，所述方法还包括：

- 5 确定将所述业务路由从第一 VPN 保护组切换到第二 VPN 保护组，其中，所述第一 VPN 保护组和所述第二 VPN 保护组分别为主 VPN 保护组和备 VPN 保护组中的一个和另一个，所述第二 VPN 保护组包括所述线性隧道保护组和所述环网保护组。

- 10 根据本发明实施例的另一个方面，还提供了一种隧道切换装置，包括：设置模块，设置为将隧道保护组上的业务路由的类标识设置为第一类标识，其中，所述隧道保护组包括第一隧道和第二隧道；确定模块，设置为根据所述第一类标识，确定所述业务路由的重定向规则；切换模块，设置为根据所述重定向规则和所述第二隧道的隧道信息，将所述业务路由从所述第一隧道切换到所述第二隧道。

根据本发明实施例的另一个方面，还提供了一种交换机，包括上述的隧道切换装置。

- 15 通过本发明实施例，采用将隧道保护组上的业务路由的类标识设置为第一类标识，其中，隧道保护组包括第一隧道和第二隧道；根据第一类标识，确定业务路由的重定向规则；根据重定向规则和第二隧道的隧道信息，将业务路由从第一隧道切换到第二隧道的方式，解决了相关技术中的三层叠加保护中分别对每条业务路由进行切换导致的时延过长的问题，降低了对业务路由进行切换的时延。

## 20 附图说明

此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

图 1 是一种三种保护类型叠加保护 L3VPN 业务的系统结构示意图；

- 25 图 2 是根据相关技术的一种为 PE 设备 MPLS L3VPN 上行处理的流程示意图；

图 3 是根据相关技术的三层叠加保护方法的切换过程示意图；

图 4 是根据本发明实施例的隧道切换方法的流程示意图；

图 5 是根据本发明实施例的隧道切换装置的结构框图；

图 6 是根据本发明实施例的隧道切换装置的优选结构框图一；

图 7 是根据本发明实施例的隧道切换装置的优选结构框图二；

图 8 是根据本发明实施例的隧道切换装置的优选结构框图三；

5 图 9 是根据本发明实施例的隧道切换装置的优选结构框图四；

图 10 是根据本发明实施例的隧道切换装置的优选结构框图五；

图 11 是根据本发明优选实施例的下一跳信息配置示意图；

图 12 是根据本发明优选实施例的三层叠加保护方法的切换过程的示意图。

## 具体实施方式

10 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本发明。

在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

15 本实施例提供了一种隧道切换方法，图 4 是根据本发明实施例的隧道切换方法的流程示意图，如图 4 所示，该流程包括如下步骤：

步骤 S402，将隧道保护组上的业务路由的类标识设置为第一类标识，其中，隧道保护组包括第一隧道和第二隧道；

步骤 S404，根据第一类标识，确定业务路由的重定向规则；

20 步骤 S406，根据重定向规则和第二隧道的隧道信息，将业务路由从第一隧道切换到第二隧道。

通过上述步骤，采用根据业务路由的第一类标识对应的重定向规则对该业务路由的工作隧道进行切换的方式，从而使得在进行隧道切换时，只需要更改相应的重定向规则，就能实现所有业务路由的同时切换，相对于相关技术中对每条业务路由分别进行切换的方式，其降低了对业务路由进行切换的时延。

25

其中，上述的隧道保护组可以是主 VPN 线性隧道保护组、备 VPN 线性隧道保护组、主 VPN 环网保护组或备 VPN 环网保护组中的任意一个。优选地，在一个包括主 VPN 线性隧道保护组、备 VPN 线性隧道保护组、主 VPN 环网保护组以及备 VPN 环网保护组的三层叠加保护系统中的各个保护组都可以采用上述的方法进行切换。

- 5 优选地，在采用访问控制列表对重定向规则进行维护的情况下，在步骤 S404 中，可以根据第一类标识查询访问控制列表，并确定访问控制列表中与第一类标识对应的重定向规则。通过本方式，可以利用系统现有的访问控制列表实现重定向规则的维护，从而提供了一种具有实际操作性的实现方式，并能够与现有的交换设备良好兼容。

- 10 优选地，业务路由的工作隧道在第一隧道上，根据隧道保护组的第一隧道和第二隧道的工作状态，确定要将业务路由从第一隧道切换到第二隧道的情况下，可以根据第二隧道的隧道信息（例如，第二隧道上的下一跳的出端口信息）更新访问控制列表中与第一类标识对应的重定向规则，例如，将重定向规则中的下一跳的出端口信息更新为第二隧道上的下一跳的出端口信息。由于每条业务路由在切换时都是根据第一类标识对应的重定向规则寻找相应的下一跳的出端口信息，因此，将该重定向规则进行  
15 更新后，所有的业务路由将同时都根据更新的重路由规则寻找下一跳，从而实现了所有业务路由的同时切换。

- 优选地，在业务路由进行切换时，步骤 S406 可以包括：根据重定向规则和第二隧道的隧道信息，分别为隧道保护组中的每个业务路由配置一个下一跳信息；分别根据配置的下一跳信息，将对应的业务路由从第一隧道切换到第二隧道。在传统的业务路由  
20 由切换方式中需要对每个隧道保护组中的每个业务路由都创建两个下一跳信息（包括主下一跳和备下一跳，相当于第一隧道的下一跳和第二隧道的下一跳），并在需要的时候，选择这两个下一跳信息中的某一个。相对于在本方式中只创建一个下一跳信息的方式，本方式中每条业务路由占用的下一跳资源减少了一半，从而节约了下一跳资源，降低了设备的成本。由于对于每个业务路由只配置了一个下一跳信息，因此，在进行  
25 隧道切换前，需要根据切换的目标隧道的信息对这个下一跳信息进行配置。

- 优选地，根据重定向规则和第二隧道的隧道信息，分别为隧道保护组中的每个业务路由配置一个下一跳信息包括：根据重定向规则中用于切换到第二隧道的下一跳的出端口信息，配置每个业务路由的下一跳信息中的出端口信息；根据第二隧道上的服务提供商边缘设备的目的媒体访问控制地址信息和第二隧道的三层接口信息，配置每个  
30 业务路由的下一跳信息中的目的媒体访问控制地址信息和三层接口信息。在本方式中，提供了一种配置下一跳信息的优选方式，即仅更新下一跳信息中的出端口信息、目的媒体方位控制地质和三层接口信息。

优选地，第一隧道和第二隧道分别为隧道保护组的主隧道和备隧道中的一个和另一个，即上述方式可以应用于从主隧道向备隧道切换的过程中，也可以应用于从备隧道向主隧道切换的过程。优选地，在一个隧道保护组的某一个隧道与另一个隧道保护组的某一个隧道叠加的情况下，可以通过该叠加的隧道，间接实现两个隧道保护组之间的两个隧道之间的切换。

10 优选地，上述的隧道保护组为线性隧道保护组和环网保护组中的一个，其中，该线性隧道保护组和环网保护组都位于同一个 VPN 保护组中，该同一个 VPN 保护组可以是主 VPN 保护组，也可以是备 VPN 保护组。优选地，在将隧道保护组上的业务路由的类标识设置为第一类标识之前，可以根据线性隧道保护组和环网保护组的工作状态，确定将业务路由切换线性隧道保护组和环网保护组中的某一个，并在切换到的隧道保护组中实现上述隧道切换方法。

15 优选地，在确定将业务路由切换到线性隧道保护组和环网保护组中的某一个之前，可以先确定该线性隧道保护组和环网保护组所位于的 VPN 保护组是主 VPN 保护组还是备 VPN 保护组，例如：可以根据第一 VPN 保护组和第二 VPN 保护组的工作状态，确定将业务路由从第一 VPN 保护组切换到第二 VPN 保护组，其中，第一 VPN 保护组和第二 VPN 保护组分别为主 VPN 保护组和备 VPN 保护组中的一个和另一个。

本实施例还提供了一种隧道切换装置，该装置用于实现上述隧道切换方法。同时，装置实施例中描述的隧道切换装置对应于上述的方法实施例，其具体的实现过程在方法实施例中已经进行过详细说明，在此不再赘述。

20 图 5 是根据本发明实施例的隧道切换装置的结构框图，如图 5 所示，该装置包括：设置模块 52、确定模块 54 和切换模块 56，其中，设置模块 52，设置为将隧道保护组上的业务路由的类标识设置为第一类标识，其中，隧道保护组包括第一隧道和第二隧道；确定模块 54 耦合至设置模块 52，设置为根据第一类标识，确定业务路由的重定向规则；切换模块 56 耦合至设置模块 52，设置为根据重定向规则和第二隧道的隧道信息，将业务路由从第一隧道切换到第二隧道。

30 本发明的实施例中所涉及到的模块、单元可以通过软件的方式实现，也可以通过硬件的方式来实现。本实施例中的所描述的模块、单元也可以设置在处理器中，例如，可以描述为：一种处理器包括设置模块 52、确定模块 54 和切换模块 56。其中，这些模块的名称在某种情况下并不构成对该模块本身的限定，例如，设置模块还可以被描述为“设置为将隧道保护组上的业务路由的类标识设置为第一类标识的模块”。

图 6 是根据本发明实施例的隧道切换装置的优选结构框图一，如图 6 所示，优选地，确定模块 54 包括：查询单元 542，设置为根据第一类标识，查询访问控制列表；第一确定单元 544，设置为确定访问控制列表中与第一类标识对应的重定向规则。

图 7 是根据本发明实施例的隧道切换装置的优选结构框图二，如图 7 所示，优选地，确定模块还包括：第二确定单元 546，设置为根据隧道保护组的工作状态，确定将业务路由切换到第二隧道；更新单元 548 耦合至第二确定单元 546 和查询单元 542，设置为根据第二隧道的隧道信息，更新访问控制列表中与第一类标识对应的重定向规则。

图 8 是根据本发明实施例的隧道切换装置的优选结构框图三，如图 8 所示，优选地，切换模块 56 包括：配置单元 562，设置为根据重定向规则和第二隧道的隧道信息，分别为隧道保护组中的每个业务路由配置一个下一跳信息；切换单元 564 耦合至配置单元 562，设置为分别根据配置的下一跳信息，将对应的业务路由从第一隧道切换到第二隧道。

优选地，配置单元 562 包括：第一配置子单元，设置为根据重定向规则中用于切换到第二隧道的下一跳的出端口信息，配置每个业务路由的下一跳信息中的出端口信息；第二配置子单元，设置为根据第二隧道上的服务提供商边缘设备的目的媒体访问控制地址信息和第二隧道的三层接口信息，配置每个业务路由的下一跳信息中的目的媒体访问控制地址信息和三层接口信息。

优选地，第一隧道和第二隧道分别为隧道保护组的主隧道和备隧道中的一个和另一个。

图 9 是根据本发明实施例的隧道切换装置的优选结构框图四，如图 9 所示，优选地，该装置还包括：另一确定模块 62，耦合至设置模块 52，设置为确定将业务路由切换到隧道保护组，其中，隧道保护组为线性隧道保护组或环网保护组。

图 10 是根据本发明实施例的隧道切换装置的优选结构框图五，如图 10 所示，优选地，该装置还包括：再一确定模块 72，耦合至另一确定模块 62，设置为确定将业务路由从第一 VPN 保护组切换到第二 VPN 保护组，其中，第一 VPN 保护组和第二 VPN 保护组分别为主 VPN 保护组和备 VPN 保护组中的一个和另一个，第二 VPN 保护组包括线性隧道保护组和环网保护组。

本实施例还提供了一种交换机，其中，该交换机包括上述的隧道切换装置。

下面结合优选实施例进行描述和说明。

本优选实施例涉及交换机等网络设备，在本优选实施例中提出了一种实现简单、高效的 MPLS L3VPN VPN FRR、线性隧道保护组和环网保护组三层叠加保护的方法及系统。

5 下面对本优选实施例的方案实现进行描述：

图 11 是根据本发明优选实施例的下一跳信息配置示意图，如图 11 所示，线性隧道保护组或者环网保护组切换后，转发下一跳表项其实只有 3 个地方需要改变，分别是：1、物理出端口信息；2、三层接口信息，包含虚拟局域网（Virtual Local Area Network，简称为 VLAN）、源媒体访问控制（Media Access Control，简称为 MAC）地址和隧道  
10 标签信息；3、目的 MAC 信息。其中的目的 MAC 信息和三层接口信息是三层接口上面所有业务对应的转发下一跳索引到同一个复用表项，和路由的数目无关，可以直接修改，但是每个下一跳的出端口信息需要每个下一跳逐个修改。

在本优选实施例中，为了解决隧道保护组上的每个下一跳的出端口都要逐个修改的问题，采用了访问控制列表（Access Control List，简称为 ACL）进行重定向的方法，  
15 包括：每个隧道保护组对应一个类标识（classid），设置 ACL 规则，该规则匹配 classid 并根据隧道保护组的主备状态将报文重定向到主或备隧道的出端口。当隧道保护组中添加一条路由时，只需设置路由的 classid 为隧道保护组的 classid 便可以将报文重定向到正确出端口，这样当隧道保护组切换时，不论保护组中有多少条路由，只需更新 ACL 规则的出端口就可以实现所有下一跳出端口的切换。

20 当隧道保护组切换的时候，只要更新上述提及的下一跳表项中的 3 个部分就可用了，即：不管有多少个路由，多少个 VPN FRR 组，一个隧道保护组只要切换 3 个表项就可以实现隧道保护组的切换。

图 12 是根据本发明优选实施例的三层叠加保护方法的切换过程的示意图，如图 12 所示，如果 VPN FRR 需要切换，建立 4 个下一跳，分别为主 VPN 线性隧道保护组  
25 下一跳、主 VPN 环网保护组下一跳、备 VPN 线性隧道保护组下一跳，以及备 VPN 环网保护组下一跳。当 VPN FRR 切换的时候，首先根据 VPN FRR 状态选择工作在主 VPN 还是备 VPN，然后根据线性隧道保护组及环网保护组状态选择线性隧道保护组下一跳还是环网保护组下一跳，然后将当前业务下一跳更新，从而实现隧道的切换。

由此可见，本优选实施例的方案较传统的 ASIC 芯片实现方法更简单、高效，对于多条业务被保护时可以实现隧道保护组的快速切换，不需要逐条业务更改出端口，同时可以节约一半的下一跳资源。

本优选实施例提供的方案主要包括如下步骤：

- 5        步骤 A，如果存在 L3VPN VPN FRR 、线性隧道保护组、环网保护组三层叠加保护的情况，那么建立 4 个下一跳，主 VPN 两个下一跳，备 VPN 两个下一跳，供 4 个隧道保护组使用。

- 10       步骤 B，对于叠加的线性隧道保护组和环网保护组，设置 ACL 重定向规则，规则动作为：匹配报文的 classid，并将报文重定向到隧道的出端口。其中，隧道保护组与 classid 一一对应，在隧道保护组上添加业务时，设置该条业务路由的 classid 与隧道保护组的 classid 一致。

步骤 C，如果协议检测到需要进行 L3VPN VPN FRR 切换，首先判断工作在主 VPN 还是备 VPN，然后根据 VPN 工作的隧道保护组情况选择线性隧道保护组的下一跳还是环网保护组的下一跳，然后将该下一跳更新至路由表。

- 15       步骤 D，如果协议检测到需要进行线性隧道保护组切换或者环网隧道保护组切换，那么直接更新 ACL 重定向规则的出端口信息、更新对应的工作目的 MAC 信息，以及更新三层接口信息，其中三层接口信息包括：源 MAC 地址、VLAN ID (VID) 和外层 MPLS 标签。

- 20       与相关技术相比较，本优选实施例提出了一种实现 MPLS L3VPN VPN FRR、线性隧道保护组、环网保护组三层叠加保护的方法，线性隧道保护组和环网保护组切换时间和 L3VPN 业务的数量没有关系，同时实现了隧道保护组切换和 VPN FRR 切换的分离，大大地降低了切换时间，降低了系统复杂度，同时节约了大量的硬件资源，可以节约成本。

- 25       下面结合附图对本优选实施例在交换芯片上实现一种 MPLS L3VPN 三层叠加保护的方法及系统进行说明。

如图 1 所示，CE1 去往 CE2 的路径有四条。PE1->PE2 的路径和 PE1->PE3 的路径构成 VPN FRR，其中 PE1->PE2 的路径为主，PE1->PE3 的路径为备；PE1->P1->PE2 与 PE1->P2->PE2 构成主 VPN 线性隧道保护组；PE1->P1->PE2 与 PE1->P1->PE2->P2->PE1 构成主 VPN 环网保护组；PE1->P3->PE3 与 PE1->P4->PE3

构成备 VPN 隧道 FRR；PE1->P3->PE3 与 PE1->P3->PE3->P4->PE1 构成备 VPN 环网保护组，从而在 PE1 上形成了 L3VPN 三层叠加保护。

下面对 PE1 设备上的处理过程进行说明：

假设 PE1->PE2 的出端口分别为 1、2、3，分别代表主 VPN 线性隧道保护组的主备端口及环网保护组的备端口。由于环网保护组的主隧道与线性保护组的主隧道叠加，所以环网保护组的主端口也是 1，同样，PE1->PE3 的出端口分别为 4、5、6，分别代表备 VPN 线性隧道保护组的主备端口及环网保护组的备端口；假设 PE1->PE2 之间存在的线性隧道保护组为隧道保护组 1，环网保护组为隧道保护组 2，PE1->PE3 之间存在的线性隧道保护组为隧道保护组 3，环网保护组为隧道保护组 4；假设存在 1K 条路由，都形成了 L3VPN VPN FRR 叠加线性隧道保护组叠加环网保护组，那么本优选实施例的一个实施方法可以是：

步骤 1、ASIC 芯片添加路由信息，同时建立主备下一跳信息。由于存在 1K 条路由，所以形成 1K 条路由表，4K 条下一跳转发，4 条 ACL 重定向规则（分别对应 4 个隧道保护组）。

步骤 2、由于 L3VPN VPN FRR 同时都叠加了线性隧道保护组及环网保护组，所以修改 4K 条下一跳的端口信息：根据当前保护组的工作状态，设置每条路由的 classid 为对应的工作隧道保护组 classid，根据隧道保护组工作状态设置 ACL 重定向规则的出端口为当前工作端口。

步骤 3、如果隧道保护组 1 切换到主，只需要更新对应的 ACL 规则 1 的出端口为 1，更新隧道保护组对应的目的 MAC 为 P1 的目的 MAC，同时更新隧道保护组对应的三层接口信息（所有 L3VPN VPN FRR 的主下一跳都指向这个三层接口索引）。

步骤 4、如果隧道保护组 1 切换到备，只需要更新 acl 规则 1 的出端口为 2，更新隧道保护组对应的目的 MAC 为 P2 的目的 MAC，同时更新隧道保护组对应的三层接口信息（所有 L3VPN VPN FRR 的主下一跳都指向这个三层接口索引）。

步骤 5、如果隧道保护组 2 切换到主，只需要更新对应的 ACL 规则 2 的出端口为 1，更新隧道保护组对应的目的 MAC 为 P1 的目的 MAC，同时更新隧道保护组对应的三层接口信息（所有 L3VPN VPN FRR 的备下一跳都指向这个三层接口索引）。

步骤 6、如果隧道保护组 2 切换到备，只需要更新 ACL 规则 2 的出端口为 3，更新隧道保护组对应的目的 MAC 为 P2 的目的 MAC，同时更新隧道保护组对应的三层接口信息（所有 L3VPN VPN FRR 的备下一跳都指向这个三层接口索引）。

5 步骤 7、对于隧道保护组 3 和 4 的切换如步骤 3—6 的过程一样，根据保护组的状态更新 ACL 重定向规则的出端口（4 到 7 端口中的某个），并更新三层接口信息。

步骤 8、如果某条路由的 L3VPN VPN FRR 切换到主，如果主 VPN 工作在线性隧道保护组，切换到线性隧道保护组下一跳，如果主 VPN 工作在环网保护组，切换到环网保护组下一跳。

10 步骤 9、如果某条路由的 L3VPN VPN FRR 切换到备，如果备 VPN 工作在线性隧道保护组，切换到线性隧道保护组下一跳，如果备 VPN 工作在环网保护组，切换到环网保护组下一跳。

在上述步骤中，步骤 3—7 属于隧道保护组切换，虽然和 1K 条路由都有关系，但是只和切换时，不关心路由信息，只需要切换 3 个表项目，切换时间和路由条目无关，切换迅速；步骤 8—9 属于 VPN FRR 切换，VPN FRR 都是针对某条触发路由的，一条  
15 路由切换一次，无需关心关联的隧道保护组状态，两个流程独立，切换流程简单。

### 工业实用性

通过本发明实施例，采用将隧道保护组上的业务路由的类标识设置为第一类标识，其中，隧道保护组包括第一隧道和第二隧道；根据第一类标识，确定业务路由的重定向规则；根据重定向规则和第二隧道的隧道信息，将业务路由从第一隧道切换到第二  
20 隧道的方式，解决了相关技术中的三层叠加保护中分别对每条业务路由进行切换导致的时延过长的问题，降低了对业务路由进行切换的时延。

显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以  
25 将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

## 权 利 要 求 书

1. 一种隧道切换方法，包括：

将隧道保护组上的业务路由的类标识设置为第一类标识，其中，所述隧道保护组包括第一隧道和第二隧道；

根据所述第一类标识，确定所述业务路由的重定向规则；

根据所述重定向规则和所述第二隧道的隧道信息，将所述业务路由从所述第一隧道切换到所述第二隧道。

2. 根据权利要求 1 所述的方法，其中，根据所述第一类标识，确定所述业务路由的所述重定向规则包括：

根据所述第一类标识，查询访问控制列表；

确定所述访问控制列表中与所述第一类标识对应的所述重定向规则。

3. 根据权利要求 2 所述的方法，其中，在查询所述访问控制列表之前，所述方法还包括：

根据所述隧道保护组的工作状态，确定将所述业务路由切换到所述第二隧道；

根据所述第二隧道的隧道信息，更新所述访问控制列表中与所述第一类标识对应的所述重定向规则。

4. 根据权利要求 1 所述的方法，其中，根据所述重定向规则和所述第二隧道的隧道信息，将所述业务路由从所述第一隧道切换到所述第二隧道包括：

根据所述重定向规则和所述第二隧道的隧道信息，分别为所述隧道保护组中的每个业务路由配置一个下一跳信息；

分别根据配置的下一跳信息，将对应的业务路由从所述第一隧道切换到所述第二隧道。

5. 根据权利要求 4 所述的方法，其中，根据所述重定向规则和所述第二隧道的隧道信息，分别为所述隧道保护组中的每个业务路由配置一个下一跳信息包括：

根据所述重定向规则中用于切换到所述第二隧道的下一跳的出端口信息，配置每个业务路由的下一跳信息中的出端口信息；

根据所述第二隧道上的服务提供商边缘设备的目的媒体访问控制地址信息和所述第二隧道的三层接口信息，配置每个业务路由的下一跳信息中的目的媒体访问控制地址信息和三层接口信息。

6. 根据权利要求 1 至 5 中任一项所述的方法，其中，所述第一隧道和所述第二隧道分别为所述隧道保护组的主隧道和备隧道中的一个和另一个。

7. 根据权利要求 1 至 5 中任一项所述的方法，其中，在将所述隧道保护组上的所述业务路由的所述标识设置为所述第一标识之前，所述方法还包括：

确定将所述业务路由切换到所述隧道保护组，其中，所述隧道保护组为线性隧道保护组或环网保护组。

8. 根据权利要求 7 所述的方法，其中，在确定将所述业务路由切换到所述隧道保护组之前，所述方法还包括：

确定将所述业务路由从第一 VPN 保护组切换到第二 VPN 保护组，其中，所述第一 VPN 保护组和所述第二 VPN 保护组分别为主 VPN 保护组和备 VPN 保护组中的一个和另一个，所述第二 VPN 保护组包括所述线性隧道保护组和所述环网保护组。

9. 一种隧道切换装置，包括：

设置模块，设置为将隧道保护组上的业务路由的标识设置为第一标识，其中，所述隧道保护组包括第一隧道和第二隧道；

确定模块，设置为根据所述第一标识，确定所述业务路由的重定向规则；

切换模块，设置为根据所述重定向规则和所述第二隧道的隧道信息，将所述业务路由从所述第一隧道切换到所述第二隧道。

10. 一种交换机，包括如权利要求 9 所述的隧道切换装置。