

1. 一种在网络装置中对不同的终端用户、服务种类、或分组呈现不同的虚拟路由器的方法，所述方法包括以下步骤：

接收具有 VLAN 域和至少一个附加域的输入分组；

由所述 VLAN 域和至少一个附加分组域形成密钥；

使用间接映射处理将所述密钥映射成虚拟路由器标识符，所述虚拟路由器标识符从多个可能的虚拟路由器配置中识别出特定虚拟路由器配置；

将所述装置配置为具有由所述虚拟路由器标识符标识的所述特定配置；以及

利用配置后的所述装置转发所述分组。
2. 根据权利要求 1 所述的方法，其中，所述 VLAN 域是入口 VLAN。
3. 根据权利要求 1 所述的方法，其中，所述 VLAN 域是扩展的或超级 VLAN。
4. 根据权利要求 1 所述的方法，其中，所述密钥是经遮蔽的密钥。
5. 根据权利要求 4 所述的方法，其中，以响应于分组域确定的密钥类型来遮蔽所述密钥。
6. 根据权利要求 1 所述的方法，其中，所述间接映射处理包括两个步骤。

7. 根据权利要求6所述的方法,其中,第一步骤包括:访问包括多个条目的表并定位具有与所述密钥匹配的内容值的条目,其中,每个所述条目都包括内容值和索引值。
8. 根据权利要求7所述的方法,其中,第二步骤包括:使用相关联的数据储存元件将所匹配的条目的所述索引值映射成所述虚拟路由器标识符。
9. 根据权利要求7所述的方法,其中,所述表储存在CAM上,所述定位的步骤包括使所述CAM搜索并定位其内容值与所述密钥匹配的条目。
10. 根据权利要求7所述的方法,其中,所述定位的步骤包括:对所述密钥应用哈希函数以确定起始条目的表索引,然后从所述起始条目开始搜索所述表以定位其内容值与所述密钥匹配的条目。
11. 根据权利要求1所述的方法,其中,所述配置的步骤包括响应于所述虚拟路由器标识符来选择用于路由所述分组的路由表,所述路由表选自多个可能的路由表。
12. 根据权利要求9所述的方法,其中,所述CAM是二进制CAM,以及所述密钥是经遮蔽的密钥。
13. 根据权利要求12所述的方法,其中,以响应于分组域确定的密钥类型来遮蔽所述密钥。
14. 根据权利要求9所述的方法,其中,所述CAM是三进制CAM,以及所述密钥是未经遮蔽的密钥。

15. 根据权利要求 11 所述的方法, 其中, 所述配置的步骤包括:
使用所述虚拟路由器标识符作为密钥来访问实现具有多条目的表的 CAM, 每个所述条目都包括内容值和索引值; 使所述 CAM 搜索并定位其内容值与所述虚拟路由器标识符匹配的条目, 然后响应于所述匹配条目的所述索引值分类和转发所述分组。
16. 一种在网络装置中对不同的终端用户、服务种类、或分组呈现不同的虚拟路由器的方法, 所述方法包括以下步骤:
接收具有 VLAN 域和 VMAN 域的输入分组;
由所述 VLAN 域和所述 VMAN 域形成密钥;
使用两步间接映射处理将所述密钥映射成虚拟路由器标识符,
其中, 第一步骤包括访问包括多个条目的表以及定位具有与所述密钥匹配的内容值的条目, 其中, 所述多个条目中的每个所述条目都包括所述内容值和索引值; 第二步骤包括使用相关联的数据储存元件将所述匹配条目的所述索引值映射成所述虚拟路由器标识符, 以及所述虚拟路由器标识符从多个可能的虚拟路由器配置中识别出特定虚拟路由器配置;
将所述装置配置为具有由所述虚拟路由器标识符标识的所述特定配置; 以及
利用配置后的所述装置路由所述分组。
17. 根据权利要求 16 所述的方法, 其中, 所述密钥由所述 VLAN 域、所述 VMAN 域、以及一个或多个附加分组域形成。
18. 根据权利要求 17 所述的方法, 其中, 所述密钥由所述 VLAN 域、VMAN 域、以及入口端口号形成。

19. 一种在网络装置中对不同的终端用户、服务种类、或分组呈现不同的虚拟路由器的方法，所述方法包括以下步骤：

接收具有 VLAN 域、VMAN 域、和入口端口域的输入分组；

由所述 VLAN 域、所述 VMAN 域、和所述入口端口域形成密钥；

使用响应于所述入口端口域确定的密钥类型来遮蔽所述密钥；

使用两步间接映射处理将经遮蔽的所述密钥映射成虚拟路由器标识符，

其中，第一步骤包括访问包括多个条目的表以及定位具有与经遮蔽的所述密钥匹配的内容值的条目，其中，所述多个条目中的每个所述条目都包括所述内容值和索引值，第二步骤包括使用相关联的数据储存元件将所匹配的条目的所述索引值映射成所述虚拟路由器标识符，以及所述虚拟路由器标识符从多个可能的虚拟路由器配置中识别出特定虚拟路由器配置；

将所述装置配置为具有由所述虚拟路由器标识符标识的所述特定配置；以及

根据配置后的所述装置路由所述分组。

20. 一种用于在网络装置中响应于输入分组确定虚拟路由器标识符的间接映射系统，所述虚拟路由器标识符用于从多个可能的虚拟路由器配置中识别出特定的虚拟路由器配置以用于路由所述分组，以及所述分组具有 VLAN 域和至少一个附加分组域，所述间接映射系统包括：

第一逻辑，用于由所述 VLAN 域和至少一个附加分组域形成密钥；

第一装置，用于访问包括多个条目的表，以及定位具有与所述密钥匹配的内容值的条目，所述多个条目中的每个所述条目都包括内容值和索引值；以及

第二装置，用于使用相关联的数据储存元件将所匹配的条目的所述索引值映射成所述虚拟路由器标识符。

21. 根据权利要求 20 所述的系统，还包括：第二逻辑，用于利用响应于一个或多个分组域确定的密钥类型来遮蔽所述密钥。

提供虚拟路由器功能的方法

技术领域

本申请大体涉及网络装置，并且具体地，涉及用于配置这种装置以使其提供虚拟路由器功能（即，对于不同的终端用户、服务种类或分组呈现不同的虚拟路由器配置）的方法。

背景技术

虚拟路由器功能指的是同一物理网络装置对于不同的终端用户、所需服务种类、或分组呈现不同的虚拟路由器配置的能力。作为该能力的结果，该同一物理装置表现为多个不同的虚拟路由器。为了实现该能力，当前的路由器直接将所关心的分组（packet，也称数据包）域（field，也称字段）（典型地为 VLAN 域）映射成特定路由表的标识符，然后使用该特定路由表对分组进行路由。VLAN 域指定虚拟 LAN、物理上可以独立而逻辑上相关的网络元件的集合，从而可以将它们看作用于 OSI 第二层路由/切换用途的同一 LAN 的一部分。例如，特定 VLAN 中的所有网络元件都接收来自 OSI 第二层的 VLAN 中的其他元件的广播。

只要不同的终端用户使用非交迭的 VLAN，该方法（其中，输入分组的 VLAN 被直接映射成路由表的标识符）就 very 有效，从而，可以将该 VLAN 用于对不同的终端用户呈现不同的虚拟路由器。然而，随着 VLAN 使用的激增，不同的终端用户开始使用交迭的 VLAN 集合，因此 VLAN 可能不再用于对不同的终端用户呈现不同的虚拟路由器。

另一个问题在于可能的虚拟路由器的数量受到 VLAN 域的大小的限制。例如，12 位的 VLAN 仅识别 4K 不同的路由表，这不足以用于某些应用。

第三个问题在于该方法缺乏灵活性。例如，如果 VLAN 的类型或格式随着网络使用发展或随着网络标准改变而改变，则该方法将会由于其依赖于特定的 VLAN 类型和格式而被舍弃。

第四个问题是随着需要提供的虚拟路由器数量的增加，该方法缺乏可扩展性。例如，利用该方法，允许虚拟路由器增加的 VLAN 域大小的增加与需要维护的路由表的数量直接成正比例地增加。

发明内容

本发明提供了一种对不同的终端用户、服务种类、或分组呈现不同的虚拟路由器的方法。该方法可以在任意的网络装置中执行，并使该装置能够提供虚拟路由器功能。

该方法在接收到具有 VLAN 域和至少一个附加域的分组时开始执行。一旦接收到分组，就由 VLAN 域和至少一个附加分组域（例如，VMAN 域）形成密钥。

然后，使用间接映射处理将该密钥映射成虚拟路由器标识符（VRID）。根据该间接映射处理，访问具有多个条目（多个条目中的每一个都具有一个内容值和一个索引值）的表来定位具有与该密钥匹配的内容值的条目。然后，使用相关联的数据存储元件将匹配条目的索引值映射成 VRID。结果从多个可能的虚拟路由器配置中识别出特定虚拟路由器配置的虚拟路由器标识符。

通过分析下面的附图和详细描述，本发明的其他系统、方法、特征和优点对于本领域的技术人员来说将是或将变得显而易见。意在将所有这些附加的系统、方法、特征和优点包括在该说明书中、落在本发明的范围中、并且由所附的权利要求保护。

附图说明

通过参考附图可以更好地理解本发明。图中的组件无需按比例绘制，而是将重点示出本发明的原理。此外，附图中，贯穿不同的视图，相同的参考标号表示相应的部件。

图 1 是示出根据一个实施例的在产生虚拟路由器标识符 (VRID) 中使用的方法步骤、数据结构和逻辑元件的框图，其特征在于使用间接映射处理将由一个或多个分组域产生的密钥映射成 VRID。

图 2 示出了密钥格式的实例，以及图 2b-2e 示出了通配组成密钥格式的域中的多个不同域的密钥类型的各种实例。

图 3 是示出一个实施例中的方法步骤的流程图，其特征在于响应于 VRID 来配置网络装置，以及然后根据配置的装置来路由分组。

图 4 示出了实现或使用所要求保护的方法和系统的特定交换机结构。

图 5 示出了可以用于支持虚拟路由器功能的多个路由表。

图 6a、图 6b 和图 6c 示出了可根据在入口分组中检测到的 VLAN 域的类型应用的可替换数据类型的实例。

具体实施方式

参照图 1，方框图示出了对于不同的终端用户、服务种类、或分组呈现不同的虚拟路由器配置的在网络装置中执行的方法 100 的步骤。此外，还示出了在执行该方法的过程中使用的数据结构，以及执行该方法步骤的逻辑元件。在该特定实施例中，在由分组解析器 104 对分组进行了解析后，在装置中执行该方法，从而该方法能够使用由解析器 104 成功解析的一些分组域，这些分组域包括 VLAN 106、VMAN 108、以及入口端口 110。该方法可以在能够在 OSI 第三层或以上的层对分组进行转发或分类的任何网络装置中执行，这些装置包括但不限于路由器、交换机、或组合路由器/交换机。对于本公开来说，“虚拟路由器”包括“轻量”虚拟路由器（即，在 OSI 第三层进行虚拟路由的路由器），以及“重量”虚拟路由器（即，在 OSI 第三层进行虚拟路由，但是每个虚拟路由器都还实现截然不同的 OSI 第二层功能）。此外，对于本公开来说，单个术语“装置”或“路由器”分别包括多个装置或多个路由器。

如前所述，VLAN 域 106 标明虚拟 LAN，网络元件的集合可以在物理上独立但在逻辑上相关，从而可以将其看作用于 OSI 第二层路由/交换的同一 LAN 的一部分。目前，VLAN 术语的主要用途是唯一地标识 VMAN（见下面）中的逻辑相关的终端用户设备。

VMAN 域 108 标明虚拟城域网，网络元件的集合可以在物理上独立但在逻辑上相关，从而可以将其看作同一网络的一部分。尽管该术语最初只用于城域网，但是该使用已经得到发展，使得该术语现在被用于标明任何网络（城域网或非城域网）。实际上，随着 VMAN 使用的激增，该术语现在主要由服务提供商使用来标明逻辑上相关的基础设施设备。同时，如上所述，VLAN 术语现在主要用于唯一标识 VMAN 中的逻辑相关的终端用户设备。值得注意的是，

当 VLAN 值唯一地标识 VMAN 中的 VLAN 时,同一 VLAN 值不可以用于表示 VMAN 中的不同终端用户设备。

入口端口号 **110** 是装置接收分组的物理端口的标识符。

返回图 1,该方法的目的是响应于输入分组来确定虚拟路由器标识符 (VRID) **102**,其中,虚拟路由器标识符 **102** 用于从多个可能的虚拟路由器配置中识别出特定虚拟路由器配置。

当密钥产生逻辑单元 **112** 根据 VLAN **106** 域、VMAN **108** 域和入口端口 **110** 域形成密钥时开始该方法。在所示的特定实施例中,通过将这三个域连接在一起来形成该密钥,然而,应该理解,形成该密钥的其他方法也是可能的。从而,例如,在一个实施例中,通过入口端口 X 接收的具有 VLAN Y 以及 VMAN Z 的输入分组具有图 2a 所示的格式的密钥 **200**,其具有三个连接域 (concatenated field),第一域 **202** 持有入口端口 X,第二域 **204** 持有 VLAN Y,以及第三域 **206** 持有 VMAN Z。

同时,在一个实施例中,入口端口 **110** 被输入到查询表 **114** 以确定密钥类型 **116**。在该实施例中,该密钥类型通过指示该密钥的三个域中的哪些将被通配 (wild-card) (即,在随后的处理中被忽略) 以及哪些将被使用而起遮蔽的作用。在该特定实施例中,这三个域中的每一个都可以被单独地通配或不被通配。因此,例如,图 2b 示出了其中入口端口和 VMAN 域被通配 (由在相应域中出现的 X 表示) 以及在后续处理中只使用 VLAN 域的密钥类型。类似地,图 2c 示出了其中入口端口域被通配而在后续的处理中使用 VLAN 和 VMAN 域的密钥类型。图 2d 示出了其中 VLAN 域被通配而在后续处理中使用了入口端口和 VMAN 域的密钥类型。图 2e 示出了其中 VMAN 域被通配而在后续处理中使用了入口端口和 VLAN 域的密钥类型。

在图 1 所示的实施例中，响应于将形成至查询表 **114** 的输入的入口端口域 **110** 来确定密钥类型 **116**。该表 **114** 包括多个条目，每个条目都包括索引值和指定特定密钥类型的内容值，例如，如图 2b-图 2e 所示。查询通过将入口端口域 **110** 映射成特定索引来进行，查询具有该索引的条目，并将密钥类型设置成该条目的内容值。在其他实施例中，可以响应于其他分组域以及多于一个的分组域来确定密钥类型。

图 6a 示出了以标号 **602** 标识的 3 比特域的密钥类型的实施例，该密钥类型附加于密钥，并且表示密钥的格式以及密钥中的哪些域将被通配。例如，密钥 **604** 的密钥类型表示该密钥为 9 比特，并且 VLAN 域和 VMAN 域将被通配；密钥 **606** 的密钥类型表示该密钥为 15 比特，并且入口端口域和 VMAN 域将被通配；密钥 **608** 的密钥类型表示密钥为 15 比特，并且入口端口域和 VLAN 域将被通配；密钥 **610** 的密钥类型表示密钥为 21 比特，并且 VMAN 域将被通配；密钥 **612** 的密钥类型表示密钥为 27 比特，并且入口端口域将被通配；以及密钥 **614** 的密钥类型表示密钥为 33 比特，并且没有域将被通配。

此外，如下将更加详细地描述，在将三进制 CAM 用于执行间接映射处理的情况下，因为密钥被间接映射成虚拟路由器标识符，刚刚讨论的密钥类型产生和密钥遮蔽处理不是必须的，这是因为对应于三进制 CAM 条目的内容值中的各个域都可以被通配，即，被设置为与值无关。在将二进制 CAM 用于执行间接映射处理的情况下，刚刚讨论的密钥类型产生和密钥遮蔽处理通常被保留。

再次参照图 1，在被遮蔽或未被遮蔽的情况下，可以使用由逻辑 **126** 执行的两步间接映射处理将密钥 **118** 映射成虚拟路由器标识符 **102**。如所示，在第一步中，访问表 **120**（该表包括多个条目 **120a**、**120b**、**120c**，其中的每一条目都具有内容值和索引值），并且定位

具有与密钥匹配的内容值的条目。在图 1 中，条目 **120b** 的内容值被示为与密钥 **118** 匹配。以标号 **122** 标识的匹配条目的索引值将形成该处理的第二步的输入。

在第二步中，使用相关联的数据储存元件 **124** 将匹配条目 **120b** 的索引值 **122** 映射为虚拟路由器标识符 **102**。该相关联的数据储存元件 **124** 具有多个条目 **124a**、**124b**，多个条目中的每一条目都具有索引值和内容值。在一个实施例中，通过在相关联的数据储存元件 **124** 中选择其索引值与表 **120** 中的匹配条目的索引值 **122** 匹配的条目来执行映射。在图 1 所示的特定实例中，条目 **124b** 满足该条件。该条目的内容值是或包含虚拟路由器标识符 **102**。

在一个实施例中，表 **120** 被储存在 CAM 中，并且通过使 CAM 搜索并定位其内容值与密钥 **118** 匹配的条目 **120b** 来执行两步处理的第一步。在 CAM 是二进制 CAM（即，每条目的内容值中的每个比特都可以取二进制值“0”和“1”的 CAM）的情况下，由于这些功能不能通过 CAM 得到，所以通常应该执行前述的密钥类型产生和遮蔽（masking）处理。然而，在 CAM 是三进制 CAM（即，每个条目的内容值中的每个比特都可以取二进制值“0”和“1”，但是还可以取“无关”值的 CAM）的情况下，由于可以通过适当地设置 CAM 条目的内容值来执行这些功能，因此前述密钥类型产生和遮蔽处理是可选的。

在第二实施例中，表 **120** 储存在 RAM 中，并且通过应用以下处理来执行两步处理中的第一步：对密钥 **118** 应用哈希函数来确定起始条目的表索引，然后搜索表 **120**，以起始条目开始，来定位其内容值与密钥 **118** 匹配的条目 **120b**。

逻辑单元 **128** 根据 VRID **102** 来配置装置，然后配置后的装置转发分组。在一个实施例中，如下将详细地描述，逻辑单元 **128** 响

应于 VRID 102 来选择或产生 CAM 搜索密钥。CAM 搜索密钥用在对分组的分类和转发确定过程中。通过设置在响应于 VRID 102 的分类和转发处理过程中使用的密钥，逻辑单元 128 有效地选择用于路由分组的路由表。

前述实施例克服了提供虚拟路由器功能的传统方法在开始时所确定的问题。首先，由于可以通过 VLAN 域和 VMAN 域的组合形成密钥，以及 VLAN 是特定 VMAN 中的唯一标识符，因此本实施例允许再次使用 VLAN 以用于虚拟路由。

其次，该实施例急剧增加了可能的虚拟路由器的数量。例如，在表 120 储存在 CAM 的情况下，可以呈现的虚拟路由器的数量仅受 CAM 的大小限制。相比于其可以支持的虚拟路由器的数量，VLAN 域的大小不再限制虚拟路由器的数量。

第三，该实施例灵活且易于适应网络使用或标准中的变化。例如，考虑最近添加到可允许的以太网类型的列表中的超宽(24 比特) VLAN 域，即，ESID 域。这是通过在查询表 114 中限定新的密钥类型来简单实现的。例如，尽管通常的数据类型可以具有图 6b 所示的格式(即，VLAN 域和 VMAN 域中的每一个都是 12 比特，入口端口域是 6 比特)，当检测到超宽 VLAN (ESID) 时，数据类型 116 可能具有图 6c 所示的格式，即，6 比特的入口接口域，随后是 24 比特的 ESID 域。在遇到图 6c 的密钥类型时，图 1 的逻辑单元 112 将响应于来自分组解析器的域 106、108 和 110 而形成该图中所示的密钥，即，将假设 VLAN 域 106 是 24 比特的 ESID 域。

第四，因为可能的虚拟路由器数量的增加不需要被维护的路由表数量的相应增加，所以该实施例是可扩缩的。相反，通过适当地设置与表 120 中的条目 120a、120b、120c 相关联的索引值，许多不同的密钥值可以被映射成同一 VRID。例如，在图 1 中，如果期

望条目 **120b** 和 **120c** 的索引值被映射成同一 VRID, 则条目 **120b** 和 **120c** 的索引值将被设置为相同值。

图 3 概括了在整个方法的一个实施例中执行的步骤。步骤 302 包括由图 1 中的逻辑单元 **112** 执行的密钥产生步骤。步骤 304 包括由图 1 中的逻辑单元 **112** 执行的可选的密钥类型产生和遮蔽处理, 密钥类型是通过访问查询表 **112** 来确定的。对于本公开, 术语“逻辑”指的是以硬件、软件、或硬件和软件的组合来实现。

步骤 306 包括两步间接映射处理, 其中, 第一步包括搜索或已经执行了搜索整个表 **120** (该表可以储存在或不储存在 CAM 上), 以找到其内容值与密钥 **118** 匹配的条目 **120b**, 以及第二步包括在相关联的数据储存器 **124** (典型的为 RAM) 中定位其索引值与表 **120** 中的匹配条目的索引值 **122** 匹配的条目 **124b**。步骤 308 包括输出虚拟路由器标识符 (VRID) **102**。在图 1 中, 该步骤包括输出其索引值与表 **120** 中的匹配条目的索引值 **122** 匹配的条目 **124b** 的内容值或内容值中的指定域。

步骤 306 和 308 由逻辑 **126** (图 1 中所示) 通过适当地访问表 **120** 和相关联的数据元件 **124** 来执行, 如这些元件之间的虚线箭头所示。

步骤 310 包括将装置配置为具有由虚拟路由器标识符标识的特定配置。在一个实施例中, 当选择或产生搜索在用于分组的分类和转发确定中所使用的 CAM 搜索密钥时, 由逻辑单元 **128** (图 1 所示) 执行该步骤。通过设置在整個分类和转发处理过程中使用的密钥, 逻辑单元 **128** 有效地从用于路由分组的多个路由表中选择一个路由表。该处理理论上如图 5 所示, 该图示出了响应于 VRID 从多个可能的路由表 **502**、**504**、**506** 选择一个路由表, 例如表 **504**, 以及使用所选择的路由表来准备转发所关心的分组。

返回参照图 3, 步骤 312 包括根据进行了配置的装置转发分组。在一个实施例中, 该步骤由装置中的分组处理器执行。对于本公开, 术语“处理器”指的是能够执行一个或多个命令、指令或状态转换的任何装置, 并且包括并不限于通用或专用微处理器、有限状态机、控制器、计算机、数字信号处理器 (DSP) 等。

图 4 示出了其中可以执行前述方法的特定路由器结构的实施例 400。如图所示, 在该实施例中, 路由器被构造成分组处理系统, 其包括分组分类/转发系统 402 和分组更改系统 404。分组分类/转发系统 402 具有入口部 406 和出口部 408, 通过这些入口部和出口部, 入口 (网络侧) 分组可以分别进入和退出分组分类/转发系统 402。类似地, 分组更改系统 404 具有入口部 410 和出口部 412, 通过这些入口部和出口部, 入口 (交换机侧) 分组可以分别进入和退出分组更改系统 404。

分组分类/转发系统 402 的入口部 406 通过接口 418 连接至一个或多个网络侧装置 414, 以及分组分类/转发系统 402 的出口部 408 通过接口 420 连接至一个或多个交换机侧装置 416。类似地, 分组更改系统 404 的入口部 410 通过接口 422 连接至一个或多个交换机侧装置 416, 以及分组更改系统 404 的出口部 412 通过接口 423 连接至一个或多个网络侧装置 414。

除了入口和出口部 406、408 以外, 分组分类系统 402 还包括第一分组解析器 104 (图 1 所示的相同的分组解析器 104), 以及分组处理器 428。

解析器 104 被配置为解析入口分组并提供至分组层的开始的上下文指针, 例如, 提供至 OSI 第 2、3、和 4 层的开始的指针。

分组处理器 **428** 被配置为响应于解析器 **104** 所提供的上下文指针针对分组进行分类和转发。

内容可寻址存储器 (CAM) **442** 被分组分类/转发系统 **402** 用来执行分组搜索以得到分组的分类/转发决定。CAM **442** 可以是三进制的、二进制的、或二进制和三进制的组合。

相关联的 RAM (ARAM) **444a**、**444b** 为设置在 CAM **442** 中的每个条目提供相关数据。作为搜索操作的结果, 使用由 CAM **442** 返回的地址 (索引值) 访问 ARAM **444a**、**444b**。ARAM **444a**、**444b** 条目数据用于在对分组做出最终的分类/转发决定过程中提供由分组处理器 **428** 使用的分组的中间分类/转发信息。

可以储存在或不储存在 CAM 上的表 **120**, 以及相关联的数据储存部 **124** (它们可以被统称为虚拟路由器间接映射器 (VRIM)), 是与之前参照图 1 讨论的相同的元件。

除了入口部和出口部 **410**、**412** 之外, 分组更改系统 **404** 还包括用于解析出口分组的第二分组解析器 **430**、更改处理器 **432**、片段处理器 **436**、第三分组解析器 **436**、访问控制逻辑 (“ACL”) 单元 **438a**、以及 L3/L4 校验和逻辑单元 **438b**。

解析器 **430** 被配置为解析出口分组并提供至分组层的开始处的上下文指针, 例如, 提供至 OSI 第 2、3、和 4 层的开始处的指针。

更改处理器 **432** 在将分组分解成片段的处理中响应于由解析器 **430** 提供的上下文指针来更改出口分组中的一些或全部。分段处理器 **436** 重新装配被分段的分组。

更改 RAM (“MRAM”) **448a**、**448b** 提供数据和由更改处理器 **432a**、**432b** 执行的分组更改操作的控制结构。

解析器 **436** 被配置为解析重新装配的分组并提供至分组层的开始处的上下文指针，例如，提供至 OSI 第 2、3、和 4 层的开始处的指针。

ACL 逻辑 **438b** 响应于由解析器 **436** 提供的解析分组层做出关于分组的 ACL 决定，诸如 CPU 备份、镜像备份；以及进行取消。CPU 备份动作将分组的备份转发至连接至系统的主机 **438**。镜像备份动作实现出口镜像功能，其中，分组的备份被转发至镜像 FIFO **440**，然后被转发至分组分类/转发系统 **402** 的出口部 **408**。取消动作取消分组或对其进行标记以由下游介质访问控制 (MAC) 处理器进行取消。

L3/L4 校验和逻辑单元 **438b** 被配置为计算更改的分组的校验和。在一个实施例中，逻辑 **438b** 被配置为独立计算第三层 (IP) 和第四层 (TCP/UDP) 的校验和。

在一个实施例中，接口 **418**、**420**、**422**、**424**、和 CAM、VRIM、ARAM、或 MRAM 接口 (未标识) 中的一个或多个可以是于 2003 年 9 月 4 号提交的美国专利申请序列号为第 10/655,742 号 (通过引证全文结合于此) 描述的 QDR-或 DDR-型接口。

在一个实施例中，图 1 中所示的逻辑元件被结合到转发和分类系统 **402** (位于分组解析器 **104** 的下游，并与分组处理器 **428** 并联) 中的图 4 的路由器中。在该实施例中，图 1 中的逻辑单元 **112** 响应于由解析器 **104** 提供的解析分组数据来执行图 3 的密钥产生步骤 302。如果三进制 CAM 未包括在 VRIM **120**、**124** 中并被用作间接映射处理 **306** 的一部分，则逻辑单元 **112** 还执行可选的密钥类型产

生和遮蔽步骤 304。如果三进制 CAM 包括在 VRIM 120、124 中，并且被用作间接映射处理 306 的一部分，则可以由该 CAM 来执行密钥类型产生和遮蔽步骤 304。逻辑单元 126 还结合 VRIM 120、124 的元件执行间接映射处理 306，以及 VRID 输出步骤 308。

分组处理器 428 通过使用 VRID 作为 CAM 442 的启动密钥来执行图 3 的配置装置步骤 310，其中确定由分组处理器 306 执行的命令序列的起始地址以对入口分组做出分类和转发决定。通过使用 VRID 作为 CAM 442 的启动密钥，分组处理器 428 如图 5 所示地从多个可能的路由表中确定地选择一个路由表。

分组处理器 428 还通过响应于使用至少最初响应于 VRID 102 所确定的密钥执行的 CAM 搜索处理对入口分组进行分类和转发来执行步骤 312。

尽管已经描述了本发明的不同实施例，但是对于本领域技术人员来说，在本发明的范围内可能存在更多的实施例和实现方式。因此，本发明除了根据所附权利要求及其等同物之外不是限制性的。

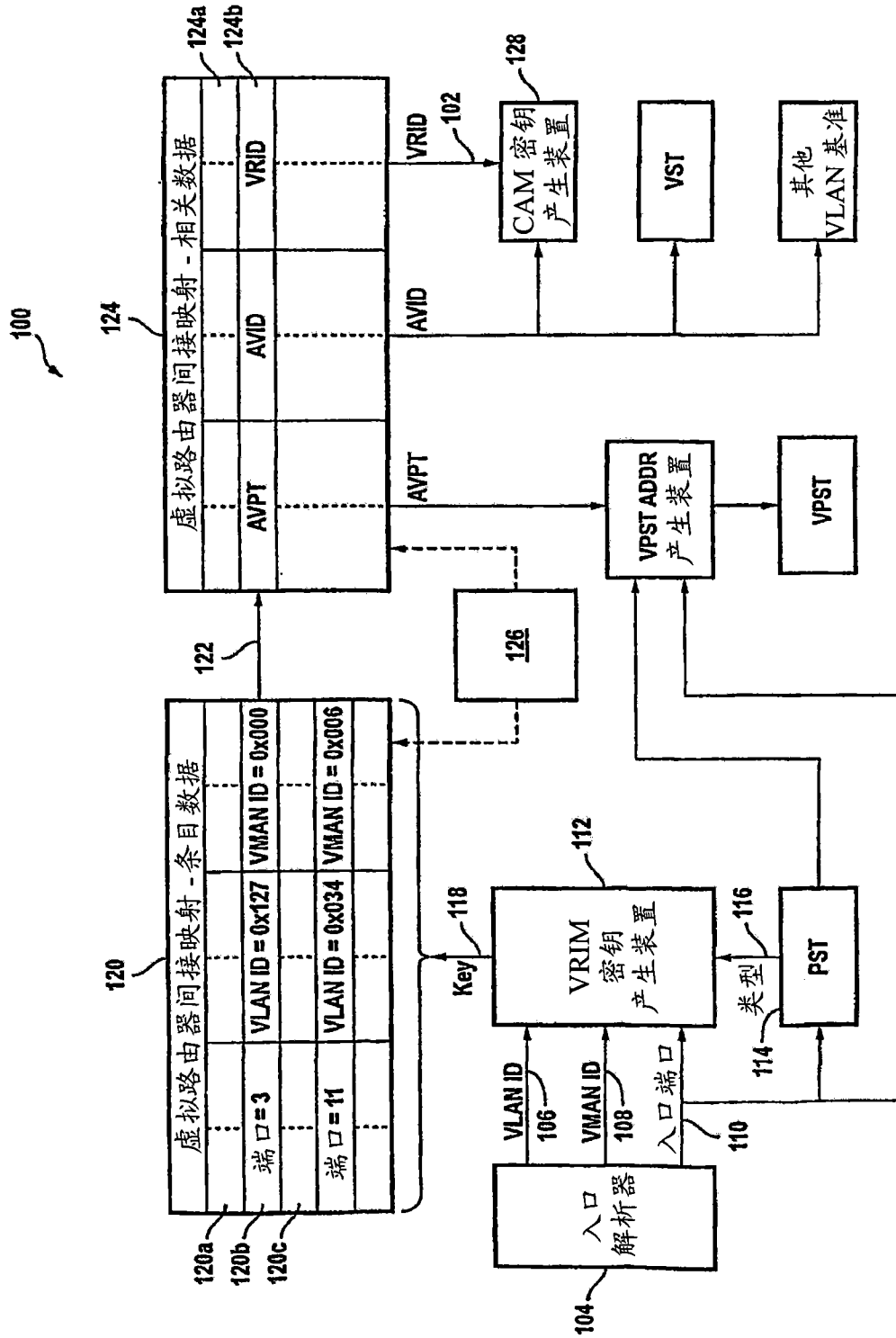


图 1

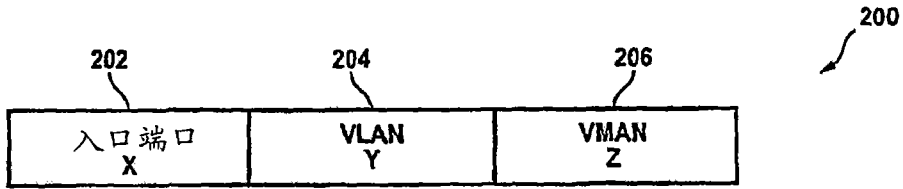


图 2A



图 2B



图 2C



图 2D



图 2E

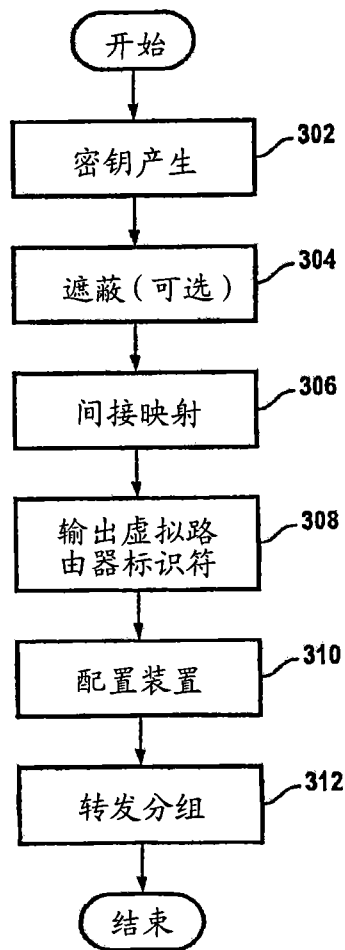


图 3

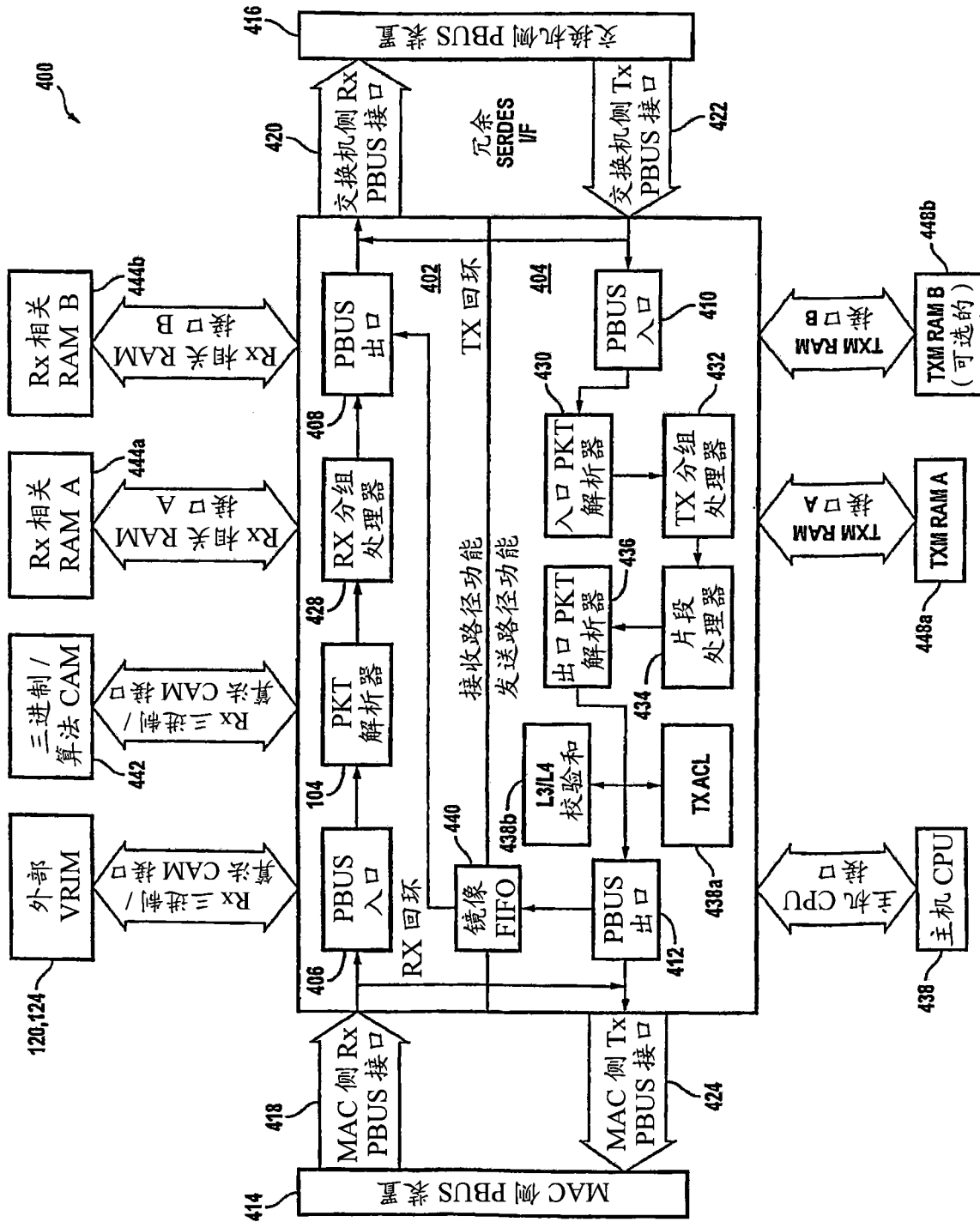


图 4

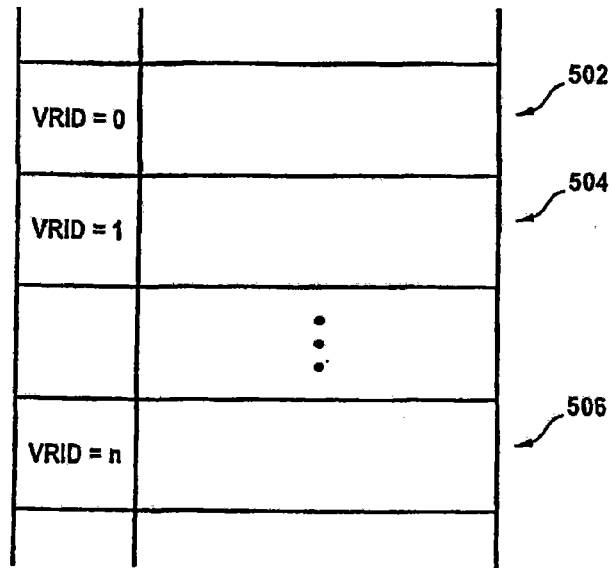


图 5

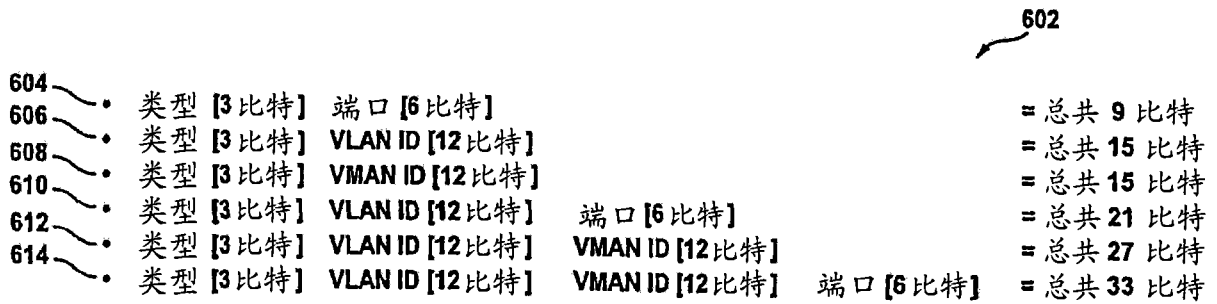


图 6A



图 6B



图 6C