



(12) 发明专利申请

(10) 申请公布号 CN 102307144 A

(43) 申请公布日 2012.01.04

(21) 申请号 201110241888.4

(22) 申请日 2011.08.19

(71) 申请人 杭州华三通信技术有限公司

地址 310053 浙江省杭州市高新技术产业开发区之江科技园六和路 310 号华为杭州生产基地

(72) 发明人 周万

(74) 专利代理机构 北京德琦知识产权代理有限公司 11018

代理人 谢安昆 宋志强

(51) Int. Cl.

H04L 12/56(2006.01)

H04L 29/12(2006.01)

H04L 12/46(2006.01)

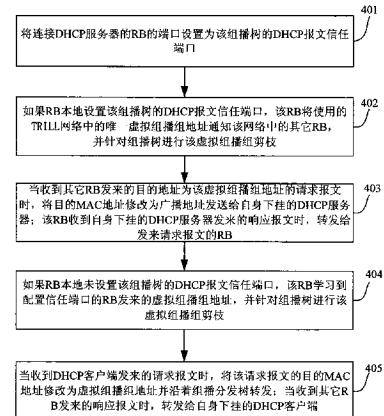
权利要求书 3 页 说明书 8 页 附图 5 页

(54) 发明名称

一种 TRILL 网络中 DHCP 报文转发方法和路由桥

(57) 摘要

本发明公开了一种 TRILL 网络中动态主机配置协议 DHCP 报文转发方法和路由桥，该方法包括：设置 DHCP 报文信任端口的 RB 将使用的 TRILL 网络中唯一虚拟组播组地址发送给 TRILL 网络中的其他 RB，各 RB 针对组播分发树进行虚拟组播组剪枝；设置信任端口的 RB 收到请求报文时，将报文的目的 MAC 地址修改为广播地址并转发；未设置信任端口的 RB 收到请求报文时，将报文的目的 MAC 地址修改为虚拟组播组地址并沿组播分发树转发。基于同样的发明构思，本发明还提出一种 RB，能够实现 DHCP 报文转发的私密性，减少网络受攻击的机会。



1. 一种多链接半透明互联 TRILL 网络中动态主机配置协议 DHCP 报文转发方法,所述 TRILL 网络至少包括一个组播树,其中,该组播树包括多个路由桥 RB,其特征在于,将连接 DHCP 服务器的 RB 的端口设置为该组播树的 DHCP 报文信任端口,所述方法包括:

如果所述 RB 本地设置该组播树的 DHCP 报文信任端口,该 RB 将使用的所述 TRILL 网络中的唯一虚拟组播组地址通知该网络中的其它 RB,并针对组播分发树进行所述虚拟组播组剪枝;当收到其它 RB 发来的目的地址为所述虚拟组播组地址的请求报文时,将所述请求报文的目的 MAC 地址修改为广播地址发送给自身下挂的 DHCP 服务器;该 RB 收到自身下挂的 DHCP 服务器发来的响应报文时,转发给发来所述请求报文的 RB;

如果所述 RB 本地未设置该组播树的 DHCP 报文信任端口,该 RB 学习到设置信任端口的 RB 发来的虚拟组播组地址,并针对组播分发树进行所述虚拟组播组剪枝;当收到 DHCP 客户端发来的请求报文时,将所述请求报文的目的 MAC 地址修改为所述虚拟组播组地址并沿着组播分发树转发;当收到其它 RB 发来的响应报文时,转发给自身下挂的 DHCP 客户端。

2. 根据权利要求 1 所述的方法,其特征在于,所述 RB 将使用的所述 TRILL 网络中的唯一虚拟组播组地址通知该网络中的其它 RB 的方法为:

所述 RB 将使用的所述 TRILL 网络中的唯一虚拟组播组地址通知给自身的多链路透明互联中间系统之间路由协议 TRILL ISIS 进程,所述 TRILL ISIS 进程将所述虚拟组播组地址作为类型长度值 TLV 封装,携带在 TRILL ISIS 的标签转发路径 LSP 报文中通知 TRILL 网络中的其他 RB。

3. 根据权利要求 2 所述的方法,其特征在于,所述针对组播分发树进行所述虚拟组播组剪枝的方法为:

遍历组播分发树的每个端口,在发送携带虚拟组播组的 TLV 的 ISIS LSP 的 RB 的端口上生成虚拟组播组转发表项;所述虚拟组播组转发表项存储组播组和未被剪掉的端口的端口号。

4. 根据权利要求 1-3 任意一项所述的方法,其特征在于,所述方法进一步包括:收到其它 RB 发来的目的地址为所述虚拟组播组地址的请求报文时,将所述请求报文携带的入口 RB 的桥标识 BRIDGE ID 号、客户端 IP 地址和客户端 MAC 地址绑定保存;

所述 RB 收到自身下挂的 DHCP 服务器发来的响应报文时,转发给发来所述请求报文的 RB 的方法为:

收到 DHCP 服务器发来的响应报文时,如果所述响应报文的目的 MAC 地址为广播地址,则将所述广播地址修改为所述绑定保存的客户端 MAC 地址,并封装所述绑定保存的入口 RB 的 BRIDGE ID 号,转发给发来所述请求报文的 RB;如果所述响应报文的目的 MAC 地址为所述绑定保存的客户端 MAC 地址,则直接封装所述绑定保存的入口 RB 的桥标识 BRIDGE ID 号,转发给发来所述请求报文的 RB。

5. 根据权利要求 1-3 任意一项所述的方法,其特征在于,本地设置 DHCP 报文信任端口的 RB,针对组播分发树进行所述虚拟组播组剪枝之后,所述方法进一步包括:生成 DHCP 报文地址转换表项;所述 DHCP 报文地址转换表项用于存储所述虚拟组播组地址;

所述当收到其它 RB 发来的目的地址为所述虚拟组播组地址的请求报文时,将所述请求报文的目的 MAC 地址修改为广播地址发送给自身下挂的 DHCP 服务器的方法为:当收到其它 RB 发来的目的地址为所述 DHCP 报文地址转换表项中存储的虚拟组播地址时,将所述请

求报文的目的 MAC 地址修改为广播地址发送给自身下挂的 DHCP 服务器；

本地未设置 DHCP 报文信任端口的 RB, 针对组播分发树进行所述虚拟组播组剪枝之后, 所述方法进一步包括 :生成相应的 DHCP 报文地址转发表项 ;所述相应的 DHCP 报文地址转发表项用于存储所述虚拟组播组地址和报文特征匹配字段 ;所述报文匹配字段用于匹配所述 DHCP 客户端发送的请求报文 ;

当收到 DHCP 客户端发来的请求报文时, 将所述请求报文的目的 MAC 地址修改为所述虚拟组播组地址并沿着组播分发树转发的方法为 :当收到 DHCP 客户端发来的报文时, 根据所述相应的 DHCP 报文地址转发表项中保存的报文特征匹配字段, 确定接收的报文为请求报文时, 将所述请求报文的目的 MAC 地址修改为所述相应的 DHCP 报文地址转发表项中存储的虚拟组播组地址并沿着组播分发树转发。

6. 根据权利要求 1-3 任意一项所述的方法, 其特征在于,

所述请求报文包括 :DHCP DISCOVER 报文和 DHCP REQUEST 报文 ;

与所述 DHCP DISCOVER 报文对应的响应报文具体为 DHCP OFFER 报文 ;所述 DHCP OFFER 报文中携带了所述 DHCP 服务器为 DHCP 客户端配置的 IP 地址信息 ;

与所述 DHCP REQUEST 报文对应的响应报文具体为 DHCP ACK 报文或 NAK 报文 ;所述 DHCP ACK 报文中携带了确认将 IP 地址分配给 DHCP 客户端, 所述 DHCP NAK 报文中携带了确认没有将 IP 地址分配给 DHCP 客户端。

7. 一种多链接半透明互联 TRILL 网络中动态主机配置协议 DHCP 报文转发路由桥 RB, 所述 TRILL 网络至少包括一个组播树, 其中, 该组播树包含多个 RB, 其特征在于, 所述 RB 包括 :配置单元、第一处理单元、学习单元和第二处理单元 ;

所述配置单元, 与所述第一处理单元和所述学习单元相连, 用于将连接 DHCP 服务器的自身所在的 RB 的端口设置为该组播树的 DHCP 报文信任端口 ;

所述第一处理单元, 当所述配置单元为自身所在的 RB 配置了 DHCP 报文信任端口时, 用于将使用的所述 TRILL 网络中的唯一虚拟组播组地址通知该网络中的其它 RB, 并针对组播分发树进行所述虚拟组播组剪枝 ;用于接收到其它 RB 发来的目的地址为所述虚拟组播组地址的请求报文时, 将所述请求报文的目的 MAC 地址修改为广播地址发送给自身所在的 RB 下挂的 DHCP 服务器 ;接收到自身所在的 RB 下挂的 DHCP 服务器发来的响应报文时, 转发给发来所述请求报文的 RB ;

所述学习单元, 与所述第二处理单元相连, 当所述配置单元未为所述学习单元所在的 RB 配置 DHCP 报文信任端口时, 用于学习设置信任端口的 RB 发来的虚拟组播组地址, 并针对组播分发树进行所述虚拟组播组剪枝 ;

所述第二处理单元, 用于当收到 DHCP 客户端发来的请求报文时, 将所述请求报文的目的 MAC 地址修改为所述虚拟组播组地址并沿着组播分发树转发 ;当收到其它 RB 发来的响应报文时, 转发给自身所在的 RB 下挂的 DHCP 客户端。

8. 根据权利要求 7 所述的 RB, 其特征在于,

所述第一处理单元, 用于将使用的唯一虚拟组播组地址通知给自身所在 RB 的多链路透明互联中间系统之间路由协议 TRILL ISIS 进程, 所述 TRILLISIS 进程将所述虚拟组播组地址作为 TLV 封装, 携带在 TRILL ISIS 的标签转发路径 LSP 报文中通知 TRILL 网络中的其他 RB。

9. 根据权利要求 8 所述的 RB, 其特征在于,

所述第一处理单元, 在发送携带虚拟组播组的 TLV 的 ISIS LSP 的自身所在的 RB 的端口上生成虚拟组播组转发表项; 所述虚拟组播组转发表项存储组播组和未被剪掉的端口的端口号。

10. 根据权利要求 7-9 任意一项所述的 RB, 其特征在于, 所述 RB 进一步包括: 存储单元;

所述存储单元, 与所述第一处理单元相连, 用于将所述第一处理单元接收到目的地址为所述虚拟组播组地址的请求报文携带的入口 RB 的桥标识 BRIDGE ID 号、客户端 IP 地址和客户端 MAC 地址绑定保存;

所述第一处理单元, 收到 DHCP 服务器发来的响应报文时, 如果所述响应报文的目的 MAC 地址为广播地址, 则将所述广播地址修改为所述绑定保存的客户端 MAC 地址, 并封装所述存储单元绑定保存的入口 RB 的 BRIDGEID 号, 转发给发来所述请求报文的 RB; 如果所述响应报文的目的 MAC 地址为所述绑定保存的客户端 MAC 地址, 则直接封装所述存储单元绑定保存的入口 RB 的 BRIDGE ID 号, 转发给发来所述请求报文的 RB。

11. 根据权利要求 7-9 任意一项所述的 RB, 其特征在于, 所述 RB 进一步包括: 生成单元;

所述生成单元, 与所述第一处理单元相连, 用于生成 DHCP 报文地址转换表项; 所述 DHCP 报文地址转换表项用于存储所述虚拟组播组地址;

所述第一处理单元, 用于当收到其他 RB 发来的目的地址为所述生成单元生成的 DHCP 报文地址转换表项中存储的虚拟组播地址时, 将所述请求报文的目的 MAC 地址修改为广播地址发送给自身所在的 RB 下挂的 DHCP 服务器;

所述学习单元, 进一步用于生成相应的 DHCP 报文地址转发表项, 所述相应的 DHCP 报文地址转发表项用于存储所述虚拟组播组地址和报文特征匹配字段; 所述报文匹配字段用于匹配所述 DHCP 客户端发送的请求报文;

所述第二处理单元, 用于当收到 DHCP 客户端发来报文, 根据所述学习单元生成的相应的 DHCP 报文地址转发表项中保存的报文特征匹配字段, 确定接收的报文为请求报文时, 将所述请求报文的目的 MAC 地址修改为所述相应的 DHCP 报文地址转发表项中存储的虚拟组播组地址并沿着组播分发树转发。

12. 根据权利要求 7-9 任意一项所述的 RB, 其特征在于,

所述请求报文包括: DHCP DISCOVER 报文和 DHCP REQUEST 报文;

与所述 DHCP DISCOVER 报文对应的响应报文具体为 DHCP OFFER 报文; 所述 DHCP OFFER 报文中携带了所述 DHCP 服务器为 DHCP 客户端配置的 IP 地址信息;

与所述 DHCP REQUEST 报文对应的响应报文具体为 DHCP ACK 报文或 NAK 报文; 所述 DHCP ACK 报文中携带了确认将 IP 地址分配给 DHCP 客户端, 所述 DHCP NAK 报文中携带了确认没有将 IP 地址分配给 DHCP 客户端。

一种 TRILL 网络中 DHCP 报文转发方法和路由桥

技术领域

[0001] 本发明涉及通信技术领域，特别涉及一种多链接半透明互联 (TRILL) 网络中动态主机配置协议 (DHCP) 报文转发方法和路由桥。

背景技术

[0002] DHCP 用来为网络设备动态地分配 IP 地址等网络配置参数。DHCP 采用客户端和服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。参见图 1，图 1 为 DHCP 的典型应用结构示意图。在图 1 中，包括一台 DHCP 服务器 101 和多台 DHCP 客户端 102，如 PC 机和便携机。

[0003] 参见图 2，图 2 为现有技术中 DHCP 客户端从 DHCP 服务器动态获取 IP 地址的流程图。其具体步骤为：

[0004] 步骤 201，DHCP 客户端以广播方式发送 DHCP 发现报文。

[0005] 步骤 202，DHCP 服务器收到 DHCP 客户发送的 DHCP 发现 (DHCPDISCOVER) 报文时，根据 IP 地址分配的优先次序选择出一个 IP 地址。

[0006] 步骤 203，DHCP 服务器将选出的 IP 地址通过 DHCP 提供报文发送给客户端。

[0007] DHCP 提供报文的发送方式由 DHCP DISCOVER 报文中的 flag 字段决定，一般是单播。

[0008] 步骤 204，DHCP 客户端向 DHCP 服务器发送 DHCP 请求报文。

[0009] 如果 DHCP 客户端收到有多台 DHCP 服务器发来 DHCP 提供报文，DHCP 客户端只接受第一个收到的 DHCP 提供报文，然后以广播方式发送 DHCP 请求 (DHCP REQUEST) 报文，该报文中包含 DHCP 服务器在 DHCP 提供报文中分配的 IP 地址。

[0010] 步骤 205，DHCP 服务器收到 DHCP 客户端发来的 DHCP 请求报文后，向 DHCP 发送应答报文。

[0011] 本步骤中，只有 DHCP 客户端选择的服务器会进行如下操作：如果确认将地址分配给该客户端，则返回 DHCP 确认 (DHCP ACK) 报文；否则返回 DHCP 否定 (DHCP NAK) 报文，表明地址不能分配给该客户端。

[0012] DHCP 报文侦听 (DHCP Snooping) 是 DHCP 的一种安全特性，网络中如果存在私自架设的伪 DHCP 服务器，则可能导致 DHCP 客户端获取错误的 IP 地址和网络配置参数，无法正常通信。为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口。其中，信任端口正常转发接收到的 DHCP 报文。不信任端口接收到 DHCP 服务器响应的 DHCP ACK 和 DHCP 提供 (DHCP OFFER) 报文后，丢弃该报文。

[0013] 连接 DHCP 服务器和其他 DHCP Snooping 设备的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

[0014] 由上可见，DHCP 的发现和请求报文都是广播发送。在 TRILL 网络中，广播报文沿

着 TRILL 组播树发送到每个 RB 设备,在整个 VLAN 域内广播。参见图 3,图 3 为现有技术中组播树组网结构示意图。

[0015] 图 3 中,以 RB301 为根的组播树,其中 RB301、RB302、RB303、RB304、RB305 和 RB306 均使能 VLAN200 的 DHCP snooping,由图中可知 VLAN200 内存在 DHCP Client 311、未知设备 312、嗅探者 313、假冒 Server 314、合法 DHCP Server 315。VLAN200 内的 DHCP Client 311 发出的 DHCPDISCOVER、REQUEST 广播报文本来只需要转发给合法的 DHCP Server312 和合法 DHCP Server 315,但由于沿着 TRILL 组播树转发,从而实际会到达未知设备 312、嗅探者 313、假冒 Server 314 和合法 DHCP Server 315,这就给嗅探者 313 和假冒 Server 314 将来的攻击提供了机会。

[0016] 综上所述,如果只针对组播树进行 VLAN 剪枝,将 DHCP 的 DISCOVER 和 REQUEST 报文沿着组播树转发,则 DHCP 报文在 VLAN 内广播,RB 及下挂设备都会收到 DHCP 报文,因而给攻击者提供了机会。

发明内容

[0017] 有鉴于此,本发明提供一种 TRILL 网络中 DHCP 报文的转发方法和路由桥,能够实现 DHCP 报文转发的私密性,减少网络受攻击的机会。

[0018] 为解决上述技术问题,本发明的技术方案是这样实现的:

[0019] 一种 TRILL 网络中 DHCP 报文的转发方法,所述 TRILL 网络至少包括一个组播树,其中,该组播树包括多个路由桥 RB,将连接 DHCP 服务器的 RB 的端口设置为该组播树的 DHCP 报文信任端口,所述方法包括:

[0020] 如果所述 RB 本地设置该组播树的 DHCP 报文信任端口,该 RB 将使用的所述 TRILL 网络中的唯一虚拟组播组地址通知该网络中的其它 RB,并针对组播分发树进行所述虚拟组播组剪枝;当收到其它 RB 发来的目的地址为所述虚拟组播组地址的请求报文时,将所述请求报文的目的 MAC 地址修改为广播地址发送给自身下挂的 DHCP 服务器;该 RB 收到自身下挂的 DHCP 服务器发来的响应报文时,转发给发来所述请求报文的 RB;

[0021] 如果所述 RB 本地未设置该组播树的 DHCP 报文信任端口,该 RB 学习到设置信任端口的 RB 发来的虚拟组播组地址,并针对组播分发树进行所述虚拟组播组剪枝;当收到 DHCP 客户端发来的请求报文时,将所述请求报文的目的 MAC 地址修改为所述虚拟组播组地址并沿着组播分发树转发;当收到其它 RB 发来的响应报文时,转发给自身下挂的 DHCP 客户端。

[0022] 一种 TRILL 网络中 DHCP 报文的转发路由桥,所述 TRILL 网络至少包括一个组播树,其中,该组播树包含多个 RB,所述 RB 包括:配置单元、第一处理单元、学习单元和第二处理单元;

[0023] 所述配置单元,与所述第一处理单元和所述学习单元相连,用于将连接 DHCP 服务器的自身所在的 RB 的端口设置为该组播树的 DHCP 报文信任端口;

[0024] 所述第一处理单元,当所述配置单元为自身所在的 RB 配置了 DHCP 报文信任端口时,用于将使用的所述 TRILL 网络中的唯一虚拟组播组地址通知 TRILL 网络中的其它 RB,并针对组播分发树进行所述虚拟组播组剪枝;用于接收到其它 RB 发来的目的地址为所述虚拟组播组地址的请求报文时,将所述请求报文的目的 MAC 地址修改为广播地址发送给自身所在的 RB 下挂的 DHCP 服务器;接收到自身所在的 RB 下挂的 DHCP 服务器发来的响应报文

时,转发给发来所述请求报文的 RB ;

[0025] 所述学习单元,与所述第二处理单元相连,当所述配置单元未为所述学习单元所在的 RB 配置 DHCP 报文信任端口时,用于学习设置信任端口的 RB 发来的虚拟组播组地址,并针对组播分发树进行所述虚拟组播组剪枝;

[0026] 所述第二处理单元,用于当收到 DHCP 客户端发来的请求报文时,将所述请求报文的目的 MAC 地址修改为所述虚拟组播组地址并沿着组播分发树转发;当收到其它 RB 发来的响应报文时,转发给自身所在的 RB 下挂的 DHCP 客户端。

[0027] 综上所述,在 TRILL 组网中,使能 DHCP snooping 功能,设置 DHCP 报文信任端口;设置 DHCP 报文信任端口的 RB 将使用的唯一虚拟组播组地址发送给 TRILL 网络中的其他 RB,TRILL 网络中的所有 RB 针对组播分发树进行 VLAN 剪枝后,进行虚拟组播组剪枝;设置 DHCP 报文信任端口的 RB 收到请求报文时,将报文的目的 MAC 地址修改为广播地址并转发;未设置 DHCP 报文信任端口的 RB 收到请求报文时,将报文的目的 MAC 地址修改为虚拟组播组地址并转发。本发明将 TRILL 网络中的 DHCP 报文交互过程限制在特定的转发路径上,不进行泛洪,能够实现 DHCP 报文转发的私密性,减少网络受攻击的机会。

附图说明

- [0028] 图 1 为 DHCP 的典型应用结构示意图;
- [0029] 图 2 为现有技术中 DHCP 客户端从 DHCP 服务器动态获取 IP 地址的流程图;
- [0030] 图 3 为现有技术中组播树组网结构示意图;
- [0031] 图 4 为本发明 TRILL 网络中 DHCP 报文的转发流程图;
- [0032] 图 5 为本发明具体实施例中 DHCP 报文转发的流程图;
- [0033] 图 6 为本发明构建配置的 TRILL 网络结构示意图;
- [0034] 图 7 为报文封装格式示意图;
- [0035] 图 8 为子 TLV 的集合示意图;
- [0036] 图 9 为组播记录示意图;
- [0037] 图 10 为本发明 TRILL 网络中 DHCP 报文的转发 RB 结构示意图。

具体实施方式

[0038] 为使本发明的目的、技术方案及优点更加清楚明白,以下参照附图并举实施例,对本发明所述方案作进一步地详细说明。

[0039] 本发明实施时,预先构建配置 TRILL 网络,TRILL 网络中至少包括一个个组播树,其中,该组播树包含多个 RB。本发明中的具体实施例均针对一个组播树来进行说明和描述。

[0040] 参见图 4,图 4 为本发明 TRILL 网络中 DHCP 报文的转发流程图。具体步骤为:

[0041] 步骤 401,将连接 DHCP 服务器的 RB 的端口设置为该组播树的 DHCP 报文信任端口。

[0042] 本步骤中 DHCP 报文信任端口通过使能 DHCP snooping 功能设置的。对未下挂 DHCP 服务器的 RP 本地不设置 DHCP 报文信任端口。如未下挂设备的 RB,或则下挂主机设备但不是 DHCP 服务器的 RB。

[0043] 步骤 402,如果 RB 本地设置该组播树的 DHCP 报文信任端口,该 RB 将使用的所述 TRILL 网络中的唯一虚拟组播组地址通知该网络中的其它 RB,并针对组播树进行该虚拟组

播组剪枝。

[0044] 步骤 403, 当收到其它 RB 发来的目的地址为该虚拟组播组地址的请求报文时, 将目的 MAC 地址修改为广播地址发送给自身下挂的 DHCP 服务器; 该 RB 收到自身下挂的 DHCP 服务器发来的响应报文时, 转发给发来请求报文的 RB。

[0045] 步骤 404, 如果 RB 本地未设置该组播树的 DHCP 报文信任端口, 该 RB 学习到配置信任端口的 RB 发来的虚拟组播组地址, 并针对组播树进行该虚拟组播组剪枝。

[0046] 步骤 405, 当收到 DHCP 客户端发来的请求报文时, 将该请求报文的目的 MAC 地址修改为虚拟组播组地址并沿着组播分发树转发; 当收到其它 RB 发来的响应报文时, 转发给自身下挂的 DHCP 客户端。

[0047] 下面结合附图, 以具体实施例来详细说明本发明中如何实现 DHCP 报文的转发。参见图 5, 图 5 为本发明具体实施例中 DHCP 报文转发的流程图。具体步骤为:

[0048] 步骤 501, 构建配置 TRILL 网络。

[0049] 参见图 6, 图 6 为本发明构建配置的 TRILL 网络结构示意图。图 6 中, 以 RB601 为根的组播树, 其中 RB601、RB602、RB603、RB604、RB605、RB606 和 RB607 皆为运行 TRILL 的 RB, 运行 TRILL ISIS 进程。各 RB 之间运行多链路透明互联中间系统之间路由协议 (TRILL ISIS) 协议, 交互单播和组播标签转发路径 (LSP) 信息, 网络中所有的 RB 之间 LSP 同步完成之后, 每个 RB 进行单播拓扑, 单播路由计算, 组播拓扑和组播路由计算。对于组播路由计算, 形成了一个组播分发树, 未知单播、广播和组播报文在该分发树转发, 并针对 VLAN200 的组播分发树进行 VLAN 剪枝。

[0050] 图 6 中, RB601、RB602、RB603、RB604 和 RB605 均使能 VLAN200 的 DHCP snooping, VLAN200 内存在 DHCP Client 611、未知设备 612、嗅探者 613、假冒 Server 614、合法 DHCP Server 615。VLAN200 内的 DHCP Client 611 发出的 DHCP DISCOVER、REQUEST 广播报文本来只需要转发给合法 DHCP Server 615, 但由于沿着 TRILL 组播树转发, 从而实际会到达未知设备 612、嗅探者 613、假冒 Server 614 和合法 DHCP Server 615。本步骤中 TRILL 网络的构建配置同现有技术, 这里不再赘述。

[0051] 步骤 502, 在下挂服务器和主机设备的 RB 上且需要动态申请 IP 地址的 VLAN 内使能 DHCP Snooping 功能, 运行 DHCP Snooping 进程, 设置连接 DHCP 服务器的 RB 的端口为 DHCP 报文信任端口。

[0052] 如图 6 中的 RB601、RB602、RB603、RB604 和 RB605 的 VLAN200 使能 DHCP Snooping。对于连接了合法 DHCP Server 的端口, 使能 DHCP 信任功能, 即 RB605 连接合法 DHCP Server 615 的端口设置为 DHCP 报文信任端口。

[0053] 步骤 503, 本地设置了 DHCP 报文信任端口的 RB, 将使用的唯一虚拟组播组地址发送给 TRILL 网络中的其他 RB。

[0054] 本步骤中的唯一虚拟组播组地址可以是该 RB 自身设置的, 也可以是预先分配的, 只要在整个 TRILL 网络中是唯一的即可。

[0055] RB 将使用的唯一的虚拟组播组地址通知自身的 TRILL ISIS 进程, TRILL ISIS 进程将该虚拟组播组地址作为类型长度值 (TLV) 封装, 携带在 TRILL ISIS 的 LSP 报文中发送给 TRILL 网络中其他 RB, 在全网同步。如图 6 中 RB605 生成虚拟组播组地址为 0100-0000-00EE。

[0056] 参见图 7, 图 7 为报文封装格式示意图。图 1 中, Type 表示 TLV 类型, 为 GADDR-TLV = 142 ;Length 表示该类型信息的总长度 ;sub-TLVs 表示子 tlv 集合, 包含虚拟组播组 tlv, 二层组播组 tlv 等信息。其定义参见图 8, 图 8 为子 TLV 的集合示意图。

[0057] 图 8 中, Type 表示 sub-TLV Type, 其值由 IETF 分配。Length 表示该类型 TLV 总长度 ;Topology-Id/Nickname-Id 表示生成该虚拟组播组 tlv 的 RB ;RESV 为预留字节 ;VLAN-ID 表示组播组所在的 VLAN ;Number of Group Records 表示组播记录的项数 ; 表示组播组记录。Group Record 的定义参见图 9, 图 9 为组播记录示意图。图 9 中记录组播源数目和组播源地址。

[0058] 步骤 504, 该 RB 进行组播分发树计算, 针对组播分发树进行的 VLAN 剪枝后, 进行虚拟组播组剪枝。

[0059] 图 6 中带箭头的方向为 DHCP 请求报文转发路径 ; 与箭头相反的方向为组播组地址发布方向。遍历分发树的每个端口, 在发布携带虚拟组播组的 TLV 的 ISIS LSP 的 RB 的端口上生成虚拟组播组转发表项 ; 该虚拟组播组转发表项存储组播组和未被剪掉的端口的端口号。

[0060] 图 6 中, 端口 620 是被剪掉的端口 ; 端口 630 是虚拟组播组转发路径上的端口, 即未被剪掉的端口。

[0061] 步骤 505, 该 RB 的 DHCP Snooping 进程生成 DHCP 报文地址转换表项, 用于将所有从 TRILL 隧道终结后的, 且目的 MAC 地址为虚拟组播组地址的请求报文的目的 MAC 地址修改为广播地址。

[0062] 本步骤中的 TRILL 隧道终结, 是指剥掉 TRILL 网络隧道头, DHCP 客户端发送的报文。该步骤中的 DHCP 报文地址转换表项记录了 RB 自身生成虚拟组播组地址。

[0063] 步骤 506, 该 RB 收到目的 MAC 地址为虚拟组播组地址的请求报文时, 根据 DHCP 报文地址转换表项, 将该报文的目的 MAC 地址修改为广播地址, 并转发给下挂的 DHCP 服务器。

[0064] 本步骤中, 如果收到目的 MAC 地址为组播转发表中存储虚拟组播组地址, 则修改该目的 MAC 地址。同时将请求报文中携带的入口 RB 的桥标识 (BRIDGE ID) 号、客户端 IP 地址和客户端 MAC 地址绑定保存。

[0065] 这里的请求报文包括 :DHCP DISCOVER 报文和 DHCP REQUEST 报文。其中, DHCP DISCOVER 报文为 DHCP 客户端寻找 DHCP 服务器阶段发送的报文 ;DHCP REQUEST 报文为客户端选择 IP 地址的阶段, 如果收到多台 DHCP 服务器发来的 DHCP OFFER 报文, 客户端只接受第一个收到的 DHCPOFFER 报文, 并发送 DHCP REQUEST 报文。客户端收到 DHCP OFFER 报文, 发送 DHCP REQUEST 报文的过程同现有技术, 这里不再赘述。

[0066] 步骤 507, 当该 RB 收到下挂的 DHCP 服务器发来的响应报文, 根据请求报文的客户端 MAC 地址将收到的响应报文转发。

[0067] 本步骤中当 RB 收到 DHCP 服务器的响应报文时, 如果该响应报文的目的 MAC 为广播地址, 则将广播地址修改为绑定保存的客户端 MAC 地址, 并封装绑定保存的入口 RB 的 BRIDGE ID 号, 转发给发来该请求报文的 RB ; 如果该响应报文的目的 MAC 地址为绑定保存的客户端 MAC 地址, 则直接封装绑定保存的入口 RB 的 BRIDGE ID 号, 转发给发来请求报文的 RB。

[0068] 与 DHCP DISCOVER 报文对应的响应报文具体为 DHCP OFFER 报文 ;DHCP OFFER 报

文中携带了 DHCP 服务器为 DHCP 客户端配置的 IP 地址信息；与 DHCP REQUEST 报文对应的响应报文具体为 DHCP ACK 报文或 NAK 报文；DHCP ACK 报文中携带了确认将 IP 地址分配给 DHCP 客户端，DHCPNAK 报文中携带了确认没有将 IP 地址分配给 DHCP 客户端。

[0069] DHCP 客户端收到 DHCP DISCOVER 报文根据 IP 地址分配选择一个 IP 地址并发送 DHCP OFFER 报文；以及收到 DHCP REQUEST 报文，并决定发 DHCP ACK 报文还是 NAK 报文的过程同现有技术，这里不再赘述。

[0070] 步骤 508，未地未设置 DHCP 报文信任端口的 RB 的 TRILL ISIS 进程学习到虚拟组播组地址，进行组播分发树计算，针对组播分发树进行 VLAN 剪枝后，进行虚拟组播组剪枝。

[0071] 步骤 509，该 RB 的 DHCP Snooping 进程生成相应的 DHCP 报文地址转换表项，用于将收到的请求报文的目的 MAC 地址修改为虚拟组播组地址。

[0072] 本步骤中的 DHCP 报文转发表项中存储报文特征匹配字段和虚拟组播组地址。

[0073] 步骤 510，该 RB 收到下挂的 DHCP 客户端发来的请求报文时，根据相应的 DHCP 报文地址转换表项，将请求报文的目的 MAC 地址修改为虚拟组播组地址并沿着组播分发树转发。

[0074] 当 RB 收到报文时，通过 DHCP 报文转发表中报文特征匹配字段进行匹配，如果确定报文为 DHCP 请求报文时，则修改该报文的目的 MAC 地址，同时为该请求报文封装入口 RB 的 BRIDGE ID 号，并沿着组播分发树转发。

[0075] 步骤 511，该 RB 收到其他 RB 发来的响应报文时，转发给自身下挂的 DHCP 客户端。

[0076] 基于上述同样的发明构思，本发明还提出一种基于 TRILL 网络中 DHCP 报文的转发 RB，该 TRILL 网络至少包括一个组播树，该组播树包括多个 RB，该 RB 包括：配置单元 1001、第一处理单元 1002、学习单元 1003 和第二处理单元 1004。

[0077] 配置单元 1001，与第一处理单元 1002 和学习单元 1003 相连，用于将连接 DHCP 服务器的自身所在的 RB 的端口设置为该组播组的 DHCP 报文信任端口；

[0078] 第一处理单元 1002，当配置单元 1001 为自身所在的 RB 配置了 DHCP 报文信任端口时，用于将使用的 TRILL 网络中的唯一虚拟组播组地址通知该网络中的其它 RB，并针对组播分发树进行所述虚拟组播组剪枝；用于接收到其它 RB 发来的目的地址为所述虚拟组播组地址的请求报文时，将请求报文的目的 MAC 地址修改为广播地址发送给自身所在的 RB 下挂的 DHCP 服务器；接收到自身所在的 RB 下挂的 DHCP 服务器发来的响应报文时，转发给发来请求报文的 RB；

[0079] 学习单元 1003，与第二处理单元 1004 相连，当配置单元 1001 未为学习单元 1004 所在的 RB 配置该组播树的 DHCP 报文信任端口时，用于学习设信任端口的 RB 发来的虚拟组播组地址，并针对组播分发树进行所述虚拟组播组剪枝；

[0080] 第二处理单元 1004，用于当收到 DHCP 客户端发来的请求报文时，将请求报文的目的 MAC 地址修改为虚拟组播组地址并沿着组播分发树转发；当收到其它 RB 发来的响应报文时，转发给自身所在的 RB 下挂的 DHCP 客户端。

[0081] 较佳地，

[0082] 第一处理单元 1002，用于将使用的唯一虚拟组播组地址通知给自身所在 RB 的多链路透明互联中间系统之间路由协议 TRILL ISIS 进程，TRILL ISIS 进程将虚拟组播组地址作为 TLV 封装，携带在 TRILL ISIS 的 LSP 报文中通知 TRILL 网络中的其他 RB。

- [0083] 较佳地，
- [0084] 第一处理单元 1002，在发送携带虚拟组播组的 TLV 的 ISIS LSP 的 RB 的端口上生成虚拟组播组转发表项；所述虚拟组播组转发表项存储组播组和未被剪掉的端口的端口号。
- [0085] 较佳地，该 RB 进一步包括：存储单元 1005；
- [0086] 存储单元 1005，与第一处理单元 1002 相连，用于将第一处理单元 1002 收到目的 MAC 地址为所述虚拟组播组地址的请求报文携带的入口 RB 的 BRIDGE ID 号、客户端 IP 地址和客户端 MAC 地址绑定保存；
- [0087] 第一处理单元 1002，收到 DHCP 服务器发来的响应报文时，如果该响应报文的目的 MAC 地址为广播地址，则将广播地址修改为所述绑定保存的客户端 MAC 地址，并封装存储单元 1005 绑定保存的入口 RB 的 BRIDGE ID 号，转发给发来请求报文的 RB；如果该响应报文的目的 MAC 地址为存储单元 1005 绑定保存的客户端 MAC 地址，则直接封装存储单元 1005 绑定保存的入口 RB 的 BRIDGE ID 号，转发给发来请求报文的 RB。
- [0088] 较佳地，该 RB 进一步包括：生成单元 1006。
- [0089] 生成单元 1006，用于生成 DHCP 报文地址转换表项；该 DHCP 报文地址转换表项用于存储虚拟组播组地址；
- [0090] 第一处理单元 1002，用于当收到其他 RB 发来的目的地址为生成单元 1006 生成的 DHCP 报文地址转换表项中存储的虚拟组播地址时，将请求报文的目的 MAC 地址修改为广播地址发送给自身所在的 RB 下挂的 DHCP 服务器；
- [0091] 学习单元 1003，进一步用于生成相应的 DHCP 报文地址转发表项，该相应的 DHCP 报文地址转发表项用于存储所述虚拟组播组地址和报文特征匹配字段；其中，报文匹配字段用于匹配 DHCP 客户端发送的请求报文；
- [0092] 第二处理单元 1004，用于当收到 DHCP 客户端发来报文，根据学习单元 1004 生成的相应的 DHCP 报文地址转发表项中保存的报文特征匹配字段，确定接收的报文为请求报文时，将请求报文的目的 MAC 地址修改为相应的 DHCP 报文地址转发表项中存储的虚拟组播组地址并沿着组播分发树转发。
- [0093] 较佳地，
- [0094] 请求报文包括：DHCP DISCOVER 报文和 DHCP REQUEST 报文；
- [0095] 与 DHCP DISCOVER 报文对应的响应报文具体为 DHCP OFFER 报文；DHCP OFFER 报文中携带了 DHCP 服务器为 DHCP 客户端配置的 IP 地址信息；
- [0096] 与 DHCP REQUEST 报文对应的响应报文具体为 DHCP ACK 报文或 NAK 报文；DHCP ACK 报文中携带了确认将 IP 地址分配给 DHCP 客户端，DHCP NAK 报文中携带了确认没有将 IP 地址分配给 DHCP 客户端。
- [0097] 上述实施例的单元可以集成于一体，也可以分离部署；可以合并为一个单元，也可以进一步拆分成多个子单元。
- [0098] 综上所述，本发明在设置了 DHCP 报文信任端口的 RB 上，使用针对到达 DHCP 服务器流量的唯一虚拟组播组地址，并且将该地址通过 TRILL ISIS 的 LSP 在整网泛洪到所有的 RB 设备。TRILL 网络中所有的 RB 在组播分发树上针对该虚拟组播组地址进行剪枝运算，构建该虚拟组播组流量在 TRILL 网络的转发路径树，该转发路径树是一个以具有 DHCP TRUST

功能的 RB 为根的逆向树。

[0099] 设置 DHCP 报文信任端口的 RB 收到请求报文时,将报文的目的 MAC 地址修改为广播地址并转发;未设置 DHCP 报文信任端口的 RB 收到请求报文时,将报文的目的 MAC 地址修改为虚拟组播组地址并转发。本发明将 TRILL 网络中的 DHCP 报文交互过程限制在特定的转发路径上,不进行泛洪,能够实现 DHCP 报文转发的私密性,减少网络受攻击的机会。

[0100] 以上所述,仅为本发明的较佳实施例而已,并非用于限定本发明的保护范围。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。

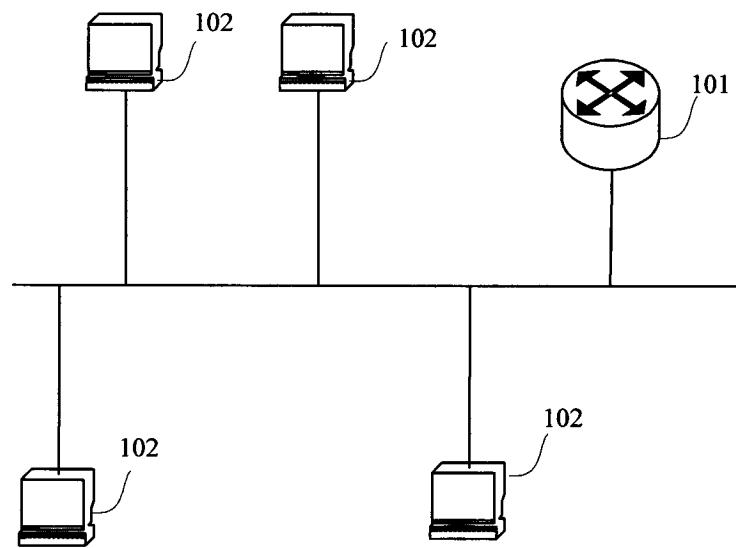


图 1



图 2

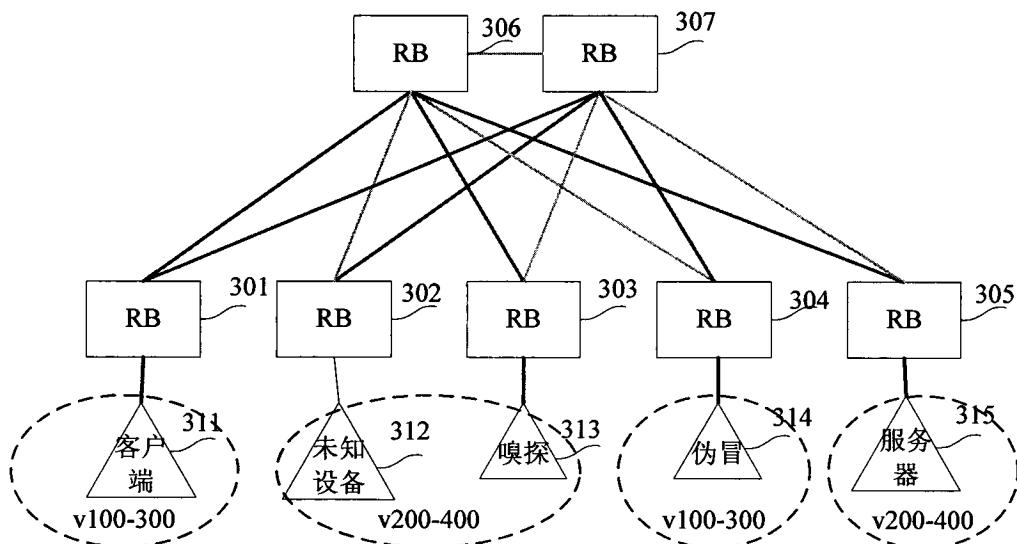


图 3

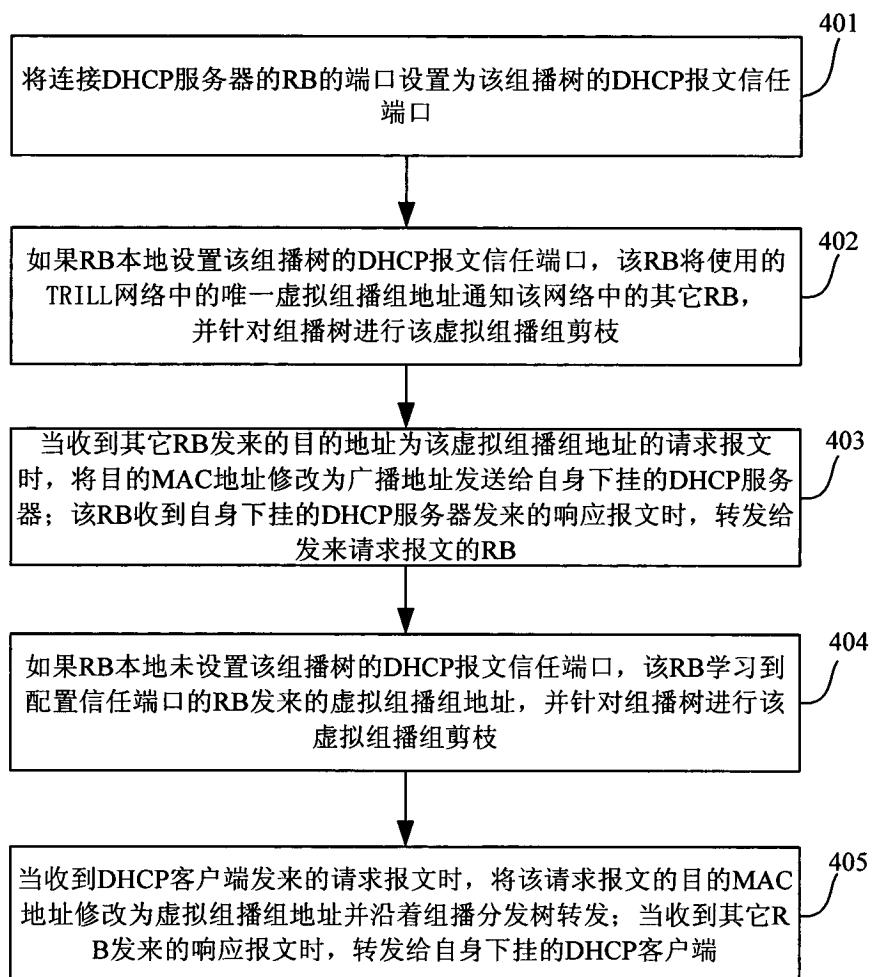


图 4

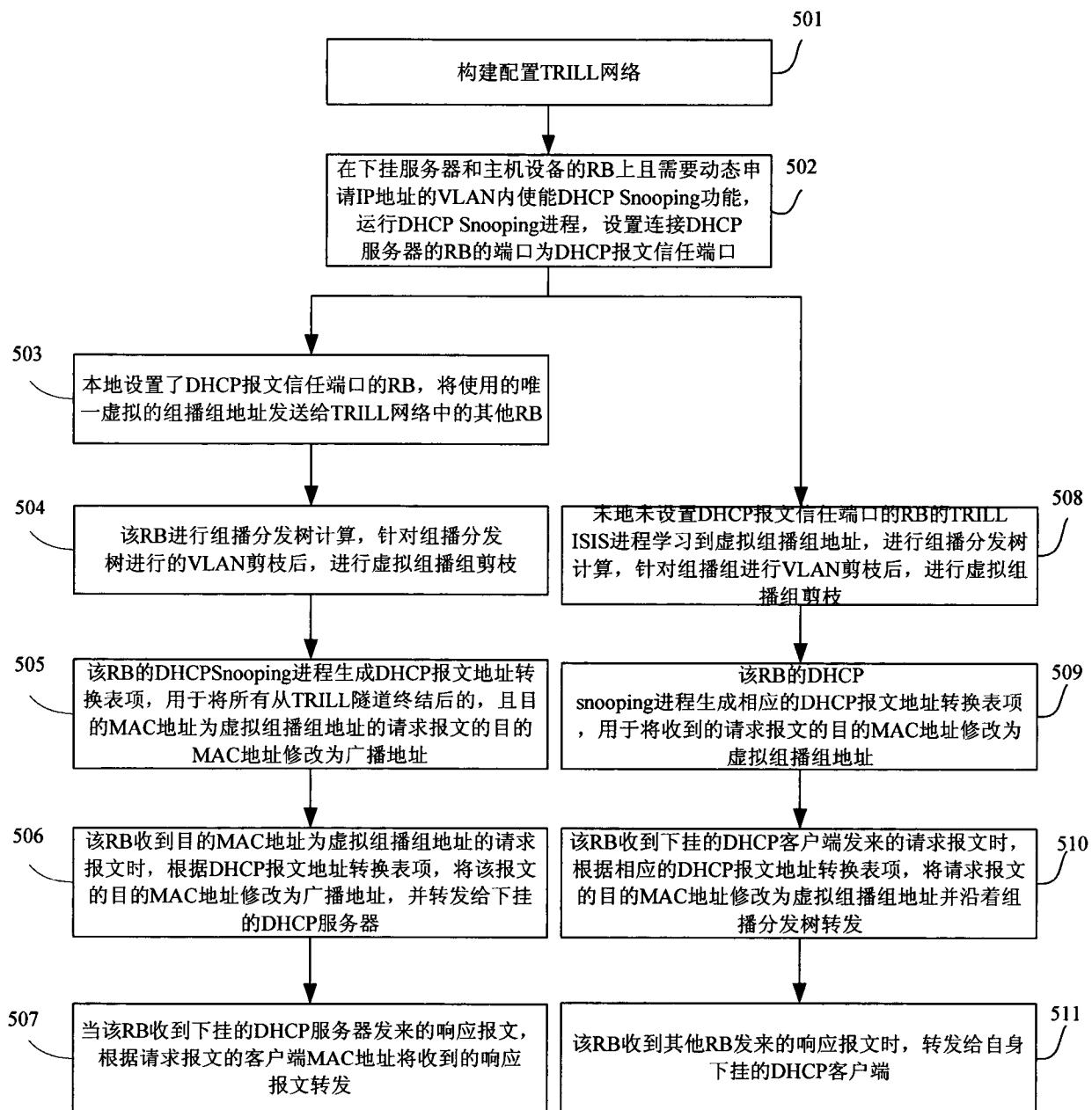


图 5

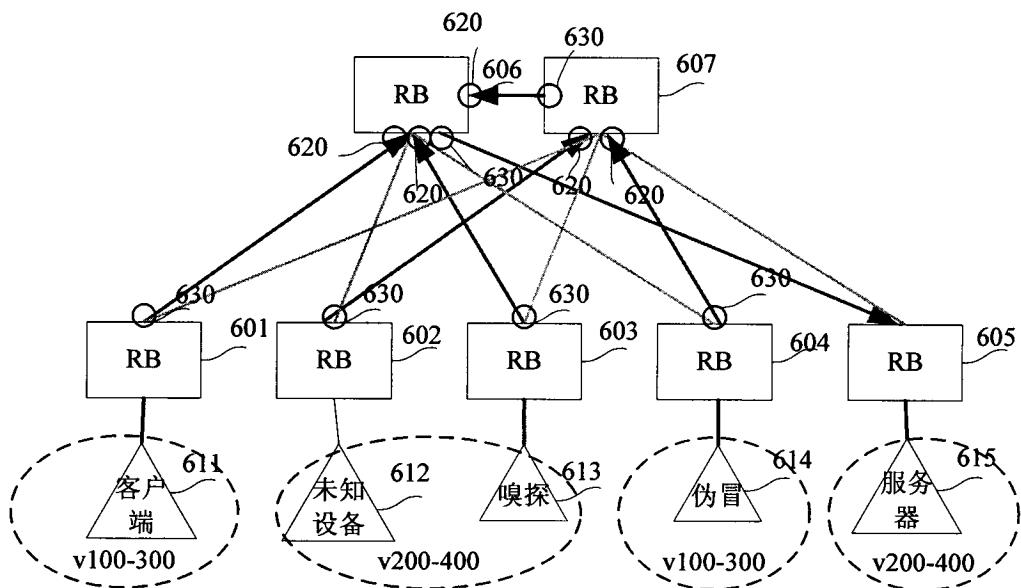


图 6

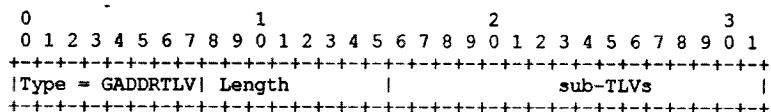


图 7

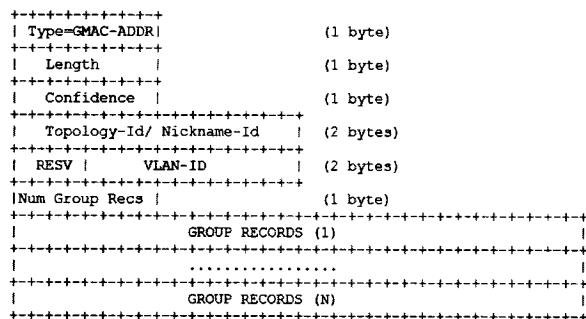


图 8

RESERVED	(1 byte)
Num of Sources	(1 byte)
Group Address	(6 bytes)
Source 1 Address	(6 bytes)
Source 2 Address	(6 bytes)
Source M Address	(6 bytes)

图 9

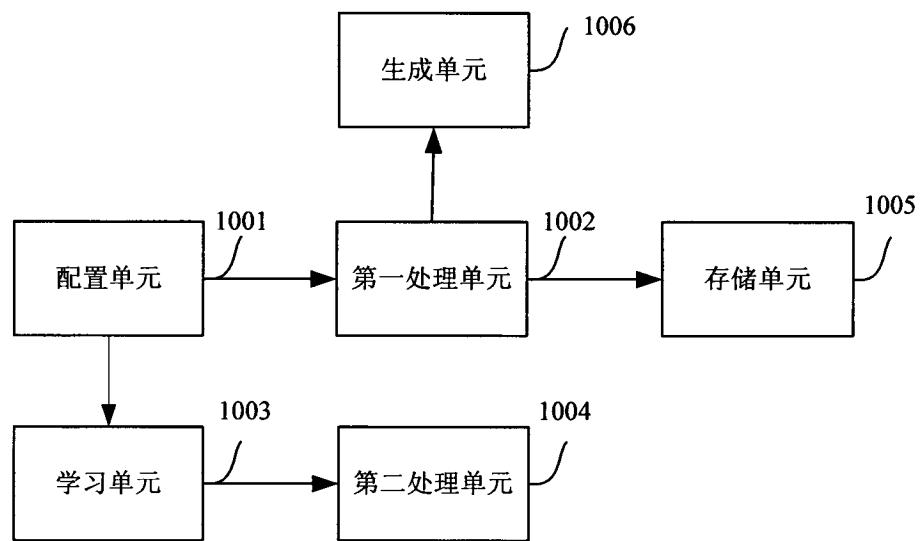


图 10