



(12) 发明专利

(10) 授权公告号 CN 1790980 B

(45) 授权公告日 2012.03.21

(21) 申请号 200510134283.X

[0098]-[0100] 段.

(22) 申请日 2005.12.13

US 6286104 B1, 2001.09.04, 全文.

US 2002/0157007 A1, 2002.10.24, 全文.

(30) 优先权数据

11/011,876 2004.12.13 US

审查员 李萍

(73) 专利权人 阿尔卡特公司

地址 法国巴黎市

(72) 发明人 杰里米·W·图维

埃里克·托利维尔

(74) 专利代理机构 北京市金杜律师事务所

11256

代理人 冯谱

(51) Int. Cl.

H04L 9/00 (2006.01)

H04L 9/32 (2006.01)

(56) 对比文件

US 2002/0032855 A1, 2002.03.14, 第

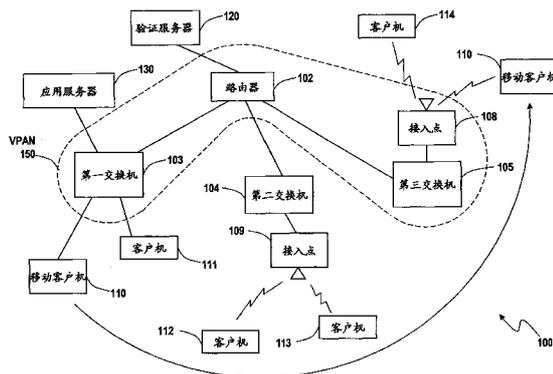
权利要求书 1 页 说明书 6 页 附图 5 页

(54) 发明名称

安全验证通告协议

(57) 摘要

本发明公开一种用于在授权节点之间分发验证信息,以便在 LAN 中的多个点上同时“预验证”某个移动用户的网络设备。当客户机尝试通过该网络设备接入网络时,该网络设备将会尝试根据用户给出的证书来对客户机进行验证。如果通过验证,那么在该网络设备上,客户机将被允许进入网络,并且客户机的预验证信息将会传送到与验证群组相关联的一个或多个网络节点。一旦接收到预验证信息,那么除了初始验证客户机的网络设备之外,在这些节点上,所述一个或多个网络节点将会被授权许可该客户机进入网络,由此在网络中的多个节点上同时预验证客户机。



1. 一种用于在网络中通告安全验证的网络设备,该网络包括一个或多个关联于验证群组的网络节点、验证服务器以及具有相关客户机标识符和证书的客户机,所述网络设备包括:

至少一个端口,用于接收来自客户机的协议数据单元以及证书;

验证管理器,包括:

共享许可表,用于保留一个或多个已验证客户机中的每一个客户机的客户机标识符;

验证状态模块,用于根据所述协议数据单元而从所述共享许可表中确定客户机是否通过验证,并且如果确定所述客户机没有通过验证,则根据从所述客户机接收的证书向所述验证服务器查询所述客户机是否通过所述验证服务器的验证;以及

预验证消息生成器,用于如果所述客户机通过所述验证服务器的验证,则将所述客户机的标识符传送到所述一个或多个网络节点。

2. 根据权利要求1所述的网络设备,其中,所述验证管理器用于根据所述协议数据单元的源地址来确定客户机是否通过验证。

3. 根据权利要求1所述的网络设备,其中,所述客户机证书包含用户标识符和口令。

4. 根据权利要求1所述的网络设备,其中,所述网络设备从包括以下设备的群组中被选出:路由器、网桥、多层交换机、有线网络接入点、无线网络接入点以及这些设备的组合。

5. 一种数据通信网络中的安全验证系统,包括:

请求接入网络的客户机,其中所述客户机与客户机标识符以及安全证书相关联;

第一节点,用于接收包含所述安全证书的接入请求以及根据所述安全证书来验证所述客户机,并且如果所述客户机在所述第一节点通过验证,则用于向所述客户机提供对所述网络的接入;以及

第二节点,用于如果所述客户机在所述第一节点处通过验证,则基于所述第一节点传送的所述客户机标识符向所述客户机提供对所述网络的接入。

6. 根据权利要求5所述的安全验证系统,其中,所述第二节点用于保留一个共享许可表,所述表包含了所述传送的客户机标识符。

7. 根据权利要求6所述的安全验证系统,其中,所述共享许可表对被授权接入网络的一个或多个已通过验证的用户进行标识。

8. 一种用于在数据通信网络中通告安全验证的方法,所述数据通信网络包括多个关联于阻止未授权接入网络的验证群组的网络节点,所述方法包括以下步骤:

在多个节点中的第一节点上接收来自请求接入网络的客户机的证书;

在第一节点确定是否验证过该客户机对网络的接入;

如果客户机通过验证:

在所述第一节点上,向所述客户机提供对所述网络的接入;

自动地从所述第一节点向关联于所述验证群组的多个节点的其他节点传送客户机信息,以便允许多个节点中的其他节点向所述客户机提供对所述网络的接入。

9. 根据权利要求8所述的方法,其中,所述客户机信息包含所述客户机的源地址。

10. 根据权利要求9所述的方法,其中,所述客户机信息包含源介质访问控制(MAC)地址。

安全验证通告协议

技术领域

[0001] 本发明涉及一种通过在网络节点之间安全地共享验证信息来简化用户接入的技术。特别地,本发明涉及一种通过在交换设备与接入点之间自动共享客户验证信息而使客户机能在网络中漫游,但却不用在每一个网络节点重新进行验证的系统和方法。

背景技术

[0002] 具有多个边缘设备或接入点的网络通常需要使用中心验证服务器来验证所有客户。因此,验证服务器成为网络瓶颈,所有已验证业务必须经由该服务器。此外,当客户机从一个接入点或边缘设备移动到另一个时,验证服务器必须重新验证该客户机,以便再次建立涉及核心网络的连通性。这种重新验证处理非常耗时、并且破坏了客户连通性,此外还有可能导致数据丢失,而当客户机只在私有网络中的安全节点之间移动时,这种处理是没有必要的。

[0003] 因此,目前需要一种用于在参与的边缘节点或接入点之间安全分发客户机验证信息的系统和方法,由此减少对于接入验证服务器的需求,并且减小反复重新验证客户机的时间和工作,其中客户机是在不同边缘节点和 / 或接入点之间的网络内部移动的。

发明内容

[0004] 本发明的特征为是一种为了在例如遍布于局域网 (LAN) 或其它网域的多个点上同时“预验证”移动用户的目的在于在授权节点之间分发验证信息的网络设备。优选实施例则是一种用于在包含了关联于验证群组的一个或多个网络节点、验证服务器以及具有相关客户机标识符和证书的客户机的网络中通告安全验证的网络设备。该网络设备优选包含了至少一个适于从客户机接收分组的端口;用于保持一个或多个已验证客户机的客户机标识符的表;以及验证管理器。验证管理器则适于通过使用源 MAC 地址之类的来自分组的信息来确定是否预先验证了客户机;如果没有执行预验证,则根据客户机证书来确定是否从验证服务器验证客户机;如果验证服务器验证了该客户机,则将客户机标识符传送到一个或多个网络节点。一旦接收到客户机标识符,则授权所述一个或多个网络节点允许客户机接入这些节点上的网络,由此在网络中的多个点上同时预验证该客户机。客户机传送的原始分组中存在的客户机证书通常包含了客户机的用户标识符和口令。该网络设备可以从包括以下设备的群组中选出的设备,其中该群组包括:路由器、网桥、多层交换机、网络接入点、无线网络接入点以及这些设备的组合。

附图说明

[0005] 本发明是以示例而非仅限于附图中的特征的方式被描述的,其中:

[0006] 图 1 是依照本发明优选实施例包含了多个适于交换预验证信息的网络设备的通信网络;

[0007] 图 2 是依照本发明优选实施例执行安全验证通告的多层交换设备的功能框图;

- [0008] 图 3 是依照本发明优选实施例执行安全验证通告的交换模块的功能框图；
- [0009] 图 4 是依照本发明优选实施例用于预验证网络内的客户机的共享许可表的示意图；
- [0010] 图 5 是依照本发明优选实施例预验证网络内的客户机的验证管理器的功能框图；以及
- [0011] 图 6 是依照本发明优选实施例在初始验证客户机以及随后在网络内预先验证该客户机时在网络内产生的消息图示。

具体实施方式

[0012] 图 1 中描述的是一个数据通信网络，该网络包括多个适于交换预验证信息的网络设备。例如，在优选实施例中，网络 100 可以包括或以可操作的方式连接到局域网 (LAN)、广域网 (WAN)、城域网 (MAN)、网际协议 (IP) 网络、因特网或是这些网络的组合。网络 100 包括多个交换设备 102 ~ 105、多个客户机 110 ~ 114、应用服务器 130、验证服务器 120。任何一个交换设备 102 ~ 105 都可以包括或者以可操作的方式连接到一个无线接入点，例如接入点 108 ~ 109。同样，一个或多个客户机 110 ~ 114 可以具有有线或无线能力，由此允许设备通过网络 100 移动，正如移动客户机 110 从第一交换设备 110 移动到接入点 108。

[0013] 本优选实施例的第一交换设备 103 和第三交换设备 105 是用以太网协议和网际协议 (IP) 来运作的，但是在这里也可以实施多种其他的网络层协议——包括无连接网络协议 (CLNP) 或网络分组交换 (IPX) / 顺序分组包交换 (SPX)——以及链路层协议——包括令牌环网和异步传输模式 (ATM) WAN/ 诸如 T1/E1 之类的串行协议。

[0014] 如下文中更详细描述的那样，网络 100 的交换设备可以与一个或多个预验证网络 (VPAN) 验证群组相关联，其中每一个群组由唯一的 VPAN 标识符指定。例如，第一 VPAN110 包括第一交换设备 103、路由器 102、第三交换设备 105 以及无线接入点 108。

[0015] 图 2 描述的是用于执行安全验证通告的多层交换设备的功能框图。交换设备 103 优选包含了多个交换模块 210，这些模块借助交换结构 250 而以可操作的方式相互连接，由此在交换模块之间传送协议数据单元 (PDU)。交换模块 210 的形式可以是适于以可拆卸方式啮合到底板 252 中的某个插槽或总线系统 (未显示) 的交换处理器、交换元件或交换刀片服务器，而该底板则以可操作的方式将每一个交换模块 210 连接在一起。

[0016] 多个交换模块 210 中的每一个都包含了多个外部端口 203，这些端口以可操作的方式经由网络通信链路连接到网络 100。在优选实施例中，每一个交换模块 210 还包括至少一个交换控制器 206，一般来说，该控制器能够实施开放式系统互连 (OSI) 参考模型中定义的第二层 (数据链路) 交换和第三层 (网络) 路由操作，但是并不局限于此。同样，每一个模块 210 都适于经由端口 203 来向网络传送协议数据单元 (PDU) 以及接收来自网络的 PDU，此外还适于借助交换结构 250 而向每个其他交换模块传送 PDU 并且接收来自每个其他交换模块的 PDU。

[0017] 对本申请的目的而言，在这里将那些从朝向交换结构 250 的通信链路流入交换模块 210 的 PDU 称为输入 PDU，并且将输入 PDU 进入交换设备 103 时所经过的交换模块 210 通称为入口交换模块。此外，在这里还将那些从交换结构 250 流入通信链路的 PDU 称为输出 PDU，而输出这些 PDU 的交换模块则称为出口交换模块。对本发明中的多个交换模块 210 来

说,其中每一个模块都可以充当入口交换模块和出口交换模块,而这取决于流动及其方向。交换设备 103 是适于执行安全验证通告的多个网络节点中的一个,其中包括路由器、网桥、业务量分类器、速率警戒器、记账设备、编辑设备以及地址查找设备。

[0018] 图 3 描述的是用于执行安全验证通告的交换模块的功能框图。交换模块 210 优选包含了多个网络接口模块 (NIM) 304、至少一个交换控制器 206、管理模块 320 以及结构接口模块 308。每一个 NIM304 都以可操作的方式连接到一个或多个外部端口 203,以便接收和传送数据业务。例如,优选使用电气与电子工程师协会 (IEEE) 802. 3、IEEE802. 2 和 / 或 IEEE802. 11 所运作的 NIM304 用于执行物理层和数据链路层控制,其中所述控制以可操作的方式将交换设备 103 与包括有线、无线和光学通信链路在内的通信介质相连接。

[0019] NIM 304 所接收的输入 PDU 经过内部数据总线 305 被传送到交换控制器 206,其中在去往目的地节点的途中,在队列管理器缓存 PDU 之前,路由器引擎 330 通常会执行滤波和转发决定。而优选实施例的路由引擎则包含了分类器 332、转发处理器 334 以及出口处理器 336。分类器 332 提取输入 PDU 的一个或多个字段,并且使用包括所提取字段在内的一个或多个与输入 PDU 相关联的属性来对按内容访问存储器 (CAM) 333 进行查询,并且将 PDU 分类给多个流中的某个流。例如,PDU 属性通常包括目的地和源地址、入口端口号、协议类型、优先级信息以及包括 802. 1Q 标签在内的虚拟局域网 (VLAN) 信息。

[0020] 在优选实施例中,在执行分类器 332 所识别的恰当的转发操作之前,交换控制器 206 还会使用验证管理器 360 来执行许可测试。举例来说,如果输入 PDU 来源于某个已验证客户机,并且该客户机当前登录到交换设备 103,那么该客户机的身份以及相关接入特权将会记录在交换设备 103 内部所保持的共享许可表 (SAT) 362 中。如果客户机尚未经过验证并且当前并未登录,那么这时会提示该客户机提供证书,以便从验证服务器 120 之类的外部数据库中确定客户机的接入配置文件,其中所述证书优选为用户名和口令。如果交换设备的 SAT362 或验证服务器 120 拒绝客户机所请求的接入特权,那么输入 PDU 将被过滤。

[0021] 但是,如果客户机请求的接入得到 SAT362 或验证服务器 120 的许可,那么分类器 332 将会从转发表 3354 中检索相关的 PDU 转发指令,并且会将即时的 PDU 传送到转发处理器 334。只要客户机登录或者保持客户机与目的地节点之间的会话,那么来自相同客户机的后续 PDU 同样是被允许进入交换设备 103 的。

[0022] 当进入网络 100 的客户机通过验证服务器 120 的验证时,将采用验证管理器 360 并使用相关客户机标识符 (ID) 来更新 SAT362。依照本发明的优选实施例,验证管理器 360 进一步被采用来向一个或多个与交换设备 103 关联于相同 VPAN 验证群组的网络节点传送预验证状态消息,在优选实施例中,预验证状态消息包括新近通过验证的客户机的客户机标识符以及与之关联的接入特权。一旦接收到预验证状态消息,那么接收方将会使用新近通过验证的客户机的客户机标识符以及接入特权来更新各自的共享许可表。这样一来,一旦客户机肯定地登录到 VPAN 安全群组中的某个成员,那么客户机就有效地登录到了所述安全群组中的每一个部件。

[0023] 一旦在客户机正在传送的节点上对客户机进行了验证,那么输入 PDU 将会传送到转发处理器 334,并且在该处理器中将会执行所检索的转发指令所标识的转发操作。如果目的地介质访问控制 (MAC) 地址为交换设备 103 所知并且可以通过该设备到达,那么 PDU 通常会在没有变更的情况下切换到恰当的出口端口。如果该地址未知,那么在与入口端口相

关联的 VLAN 内部,源 MAC 地址可以通过源学习机制而与入口端口 203 相关联,并且 PDU 将会广播到 VLAN 内部每一个与所述入口端口相关联的出口端口。如果 PDU 的目的地节点是在另一个网络内部,那么转发服务器 334 通常将会递减生存周期 (TTL) 计数器,并使用新的数据链路层报头来重新封装分组,例如在将分组路由到恰当目的地之前。

[0024] 举例来说,在某些实施例中,转发处理器 334 还被用于执行分组处理操作,其中包括但不限于用于重新封装数据的报头变换、用于向 PDU 附加一个或多个 VLAN 标签的 VLAN 标签推送、用于从 PDU 中删除一个或多个 VLAN 标签的 VLAN 标签弹出、用于保持网络资源的服务质量 (QoS)、用于监视客户业务量的计费 and 记账、多协议标签交换 (MPLS) 管理、用于有选择地过滤 PDU 的验证、访问控制、包括地址解析协议 (ARP) 控制在内的更高层学习、用于为业务量分析再现和重定向 PDU 的端口镜像、源学习、用于确定分配交换资源给 PDU 的相对优先级的服务等级 (CoS) 以及用于警戒和业务整形的色彩标记。

[0025] 在路由引擎 330 执行了分组处理之后,为通过交换设备 103 的其它交换模块可以到达的节点所指定的 PDU,根据它们的服务等级 (CoS) 和 / 或服务质量 (QoS) 要求,被队列管理器 340 暂时缓存在优先级队列 342 中,直至带宽可用于将 PDU 通过交换结构 250 进行传送为止。然后,PDU 然后经由结构接口模块 308 被传送到恰当的出口交换模块,以便沿着 PDU 的目的地节点方向进行传送。

[0026] 在优选实施例中,结构接口模块 308 用于向交换结构 250 传送输入 PDU,并且接收来自一个或多个其他交换模块中的每一个模块的输出 PDU。在优选实施例中,从结构接口模块 308 接收的输出数据将会缓存在优先级队列 342 中,经过路由器引擎的出口处理器 336 用于进行例如统计处理,以及经由一个 NIM 304 从恰当的出口端口被传送。

[0027] 在图 4 中描述的是用于在网络内预授权客户机的共享许可表 362 的示意图。SAT400 包含了一个或多个用于识别已验证客户机以及与该客户机相关联的接入特权的字段。在优选实施例中,已验证客户机是借助其地址来进行识别的,其中所述地址优选地为 MAC 源地址 (SA) 401,但是,举例来说,该地址也可以是 IP 地址。与客户机相关联的接入特权优选地包含一个或多个 VLAN 标识符 (VID) 402,但是该接入特权也可以包括一个或多个规定用户查看、下载或变更不同文件的接入控制。

[0028] SAT362 中所列举的客户机标识符包括那些直接登录到诸如交换机 103 之类的作为 SAT362 宿主的网络节点的客户机,以及直接登录到与同一个 VPAN 验证群组相关联的其他网络节点的客户机。如下文中更详细描述的那样,对直接登录到 VPAN 中的其他网络节点的客户机来说,其客户机 ID 是在这些其他网络节点的授权管理器 360 产生的一个或多个验证状态消息中知道的。在优选实施例中,SAT362 包含在验证管理器 360 中,但是它也可以与转发表 354 的桥接和路由信息相整合,此外还可以处于中央命令处理器 260 中。例如,该客户机可以是网络 100 内部或外部的一个节点,也可以是其上运行的应用程序。

[0029] 图 5 中描述的是用于在虚拟预验证区域网络内部预先授权客户机的验证管理器 360 的功能框图。优选实施例的验证管理器 360 包括验证状态模块 502、安全模块 506、SAT 362、预验证消息生成器 510 以及预验证消息接收机 512。一旦从请求与交换设备 103 相连或是请求与可以经由设备 103 到达的节点相连的客户机那里接收到 PDU,路由引擎 330 将会确定客户机是否被验证来这样做。特别地,路由引擎 330 将一个或多个从输入 PDU 中提取的字段传送到状态模块 502,该模块用于首先查询共享许可表 362,以便确定客户机的许可

状态。

[0030] 如果状态管理器 502 不能根据 SAT 362 来验证客户机,那么状态管理器 502 会向路由引擎 330 告知暂时拒绝验证客户机,由此导致路由器引擎 330 就证书而向客户机给出提示,其中该证书优选为用户标识符和口令。一旦接收到用户标识符和口令,那么状态管理器 502,更具体地是检索代理 504,产生一个传送到外部数据库的验证查询,以便确定客户机的许可状态,其中举例来说,所述数据库可以是验证服务器 120。在优选实施例中,验证查询和后续响应分别是由安全模块 506 来进行加密和解密的。

[0031] 如果验证服务器 120 发布一个许可该验证的响应,那么状态模块 502 将会触发更新控制器 508,以便将客户机标识符添加给内部 SAT362。然后,在优选实施例中,预验证生成器将会确定第一交换设备 103 所属的验证群组表 (AGT) 514 中的每一个其他成员的目的地址。随后,预验证生成器 510 向 VPAN 验证群组中的每一个部件发送一个经过安全模块 506 加密的预验证许可消息。同样,当客户机注销以及以其他方式取消验证的时候,预验证生成器 510 同样会向验证群组中的每一个成员传送一个预验证废止消息。

[0032] 更新控制器 508 还用于从验证群组中的其他成员接收预验证许可和废止消息。一旦接收到预验证许可消息,更新控制器 508,具体地预验证接收机 512,将其中的客户机标识符以及相关的接入特权添加给本地 SAT 362。同样,一旦接收到废止特权的预验证指示,即来自验证群组的另一个成员的废止消息,那么预验证接收机 512 就会使得客户机标识符以及特权从本地 SAT362 中被删除。

[0033] 由此,客户机可以在不执行用户登录过程的形式的情况下快速接入验证群组中的每一个成员。虽然在优选实施例中对验证管理器 360 进行配置,使之临时拒绝 SAT362 中未曾显性列举的每一个客户机的验证,但是本领域技术人员将会了解,验证管理器 360 是可以以不同的缺省验证规则来进行配置的。

[0034] 图 6 中描述的是在客户机最初经过验证并且随后在网络内进行预验证时在网络内产生的消息图示。例如,在这里将移动客户机 110 传送到的 VPAN 内部的某个节点的第一消息称为接入请求消息 602。一旦接收到接入请求消息 602,则第一交换设备 103 将会使用移动节点 110 的 MAC 源地址来查询 SAT 362。如果源地址不存在并且移动客户机 110 临时拒绝验证,那么交换设备 103 会发送一个标识符请求消息 604,以便提示客户机 110 输入用户 ID 和口令 606。如果验证服务器 120 能够根据接收到的用户 ID 和口令 606 来验证客户机 103,那么服务器 412 将会传送一个包含验证确认的验证消息 610 ~ 611。一旦接收到验证确认,那么第一交换设备 103 将会允许移动客户机 110 向应用服务器 130 之类的被请求资源传送和建立一个通信会话 612。

[0035] 依照优选实施例,第一交换设备 103 还会向 VPAN 授权群组 150 中的每一个成员传送预验证许可消息 614,其中该群组包含了用于将许可消息转发到第三交换设备 105 的路由器 102,而第三交换设备 105 则将该消息转发到接入点 108。在 VPAN 150 中,每一个接收许可消息的节点都会使用移动用户的客户机 ID 来更新其 SAT362,以便表示移动客户机 110 登录到该节点。

[0036] 随后,如果移动客户机 110 以图 1 所示方式在 VPAN 150 内部移动,那么移动客户机 110 可以实时无中断地与应用服务器 130 继续正在进行的会话。举例来说,在移动客户机 110 使用连至接入点 108 的无线连接来调换连至第一交换设备 103 的连接时,作为预先

存在的会话 612 的一部分,移动客户机 110 会继续向应用服务器 130 传送会话消息 620 ~ 621 以及接收来自应用服务器 130 的消息。如上所述,接入点 108 根据从会话管理 620 中提取的 MAC 源地址以及 VLAN 相关信息来验证移动用户,而不用再次就用户 ID 以及口令向移动客户机 110 发出提示,而这种提示会破坏与应用服务器 130 正在进行的会话,此外还会导致数据丢失以及为用户带来不便。

[0037] 应该指出的是,网络管理员为依照优选实施例的网络节点分配了多个 VPAN 验证群组标识符中的至少一个。这样一来,网络可以分成多个虚拟预验证子网。例如,在这里可以相应于工程部门、财务部门以及销售部门而将企业网络细分成存在一定程度重叠的独立子网。然后,如果请求接入的节点具有与当前验证客户机的网络部分不同的 VPAN 关联,那么,在一部分网络中通过验证的客户机有可能需要登录到不同部分的网络。以图 1 为例,移动客户机 110 需要通过执行登录来连接到第二交换设备 104 或是其相关接入点 109,这是因为客户机的预验证只在第一交换设备 103、路由器 102、第三交换设备 105 以及接入点 108 中有效。

[0038] 随后,如果移动客户机 110 从相连的节点注销,那么该节点会在相连节点以及其他每一个关联于 VPAN 验证群组的节点撤销预验证。如果移动客户机 110 从接入点 108 注销,那么举例来说,接入点 108 将会产生传送到 VPAN 150 中的每一个其他成员的预验证废止消息,这些成员包括向路由器 102 转发废止消息 632 的第三交换设备,而路由器 102 则将该消息转发到第一交换设备 103。一旦接收到废止消息 632,那么每一个节点都会从它的 SAT 中删除移动客户机 ID,由此在没有再次登录的情况下阻止移动客户机 110 接入网络 110。

[0039] 在优选实施例中,对与某个 VPAN 相关联的网络节点,也就是 VPAN 验证群组中的成员而言,这些网络节点用于使用本领域技术人员已知的邻居发现协议来发现对方。优选地,所述邻居发现协议是第二层协议,该协议使用了传送到被保留的多播 MAC 地址的“hello”消息而使每一个网络设备能够向 LAN 中的其他节点通告其自身标识,其中该标识优选为 IP 地址,此外,还使每一个网络设备能够发现其邻居的标识,并且能够确定哪些邻居正在运行本发明的预验证协议以及一个或多个 VLAN 中的哪些是邻居所支持的或者一个或多个 VPAN 中的哪些是可以通过这些邻居到达的节点所支持的。在优选实施例中,每一个希望共享验证的设备被提供一个对于 VPAN 唯一的加密密钥,该密钥用于打开通过其可以共享客户机标识信息的网络节点之间的加密通信流。本发明可以使用的例子邻居发现协议是 IEEE802.1A/B,由此该协议在此引入作为参考。

[0040] 虽然上文中的描述包含了很多规定,但是这些规定不应当解释为是对发明范围进行的限制,而是仅仅提供了关于本发明的一些优选实施例的例子。

[0041] 因此,在这里是以示例而不是限制的方式公开本发明的,并且在这里应该通过参考下列权利要求来确定本发明的范围。

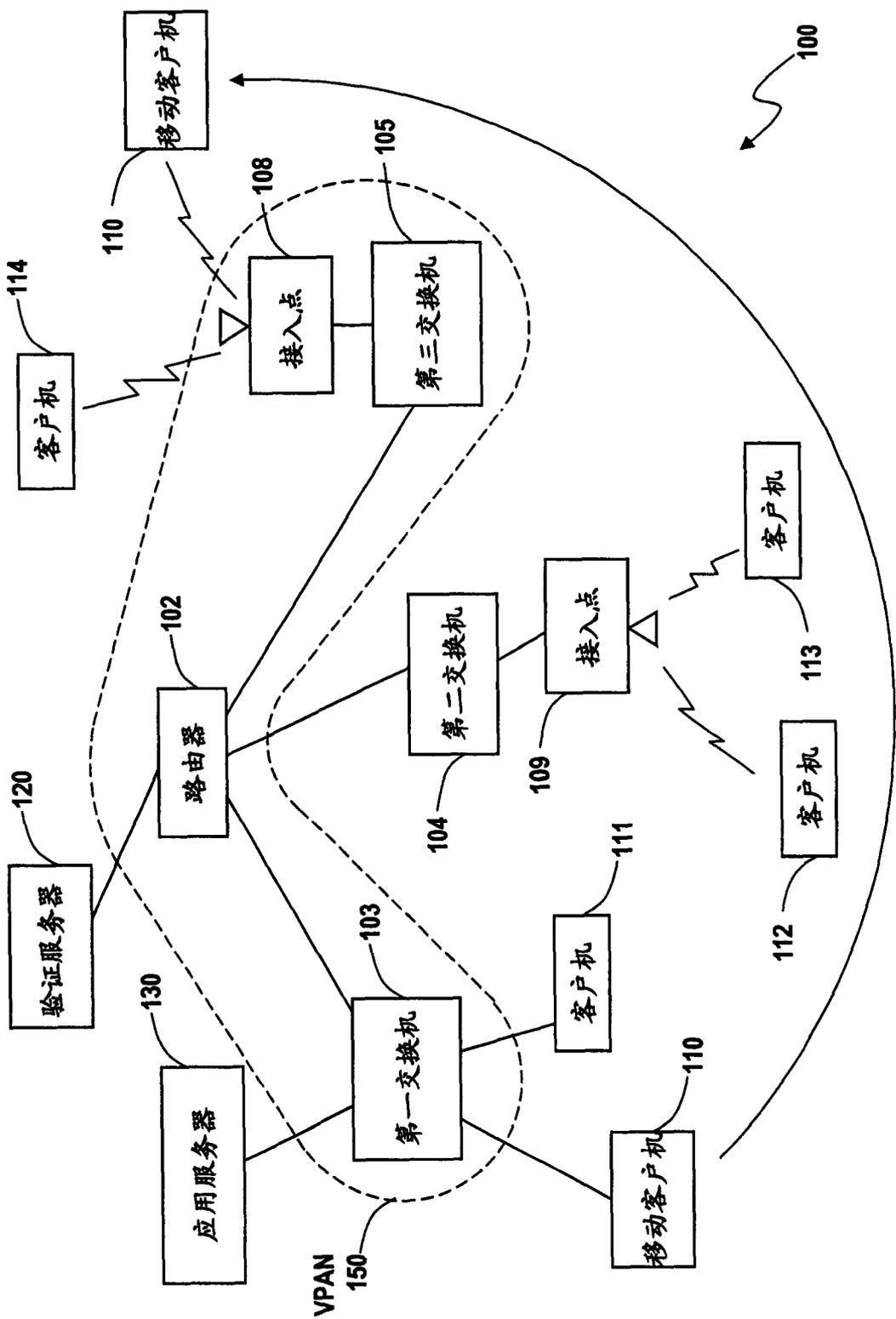


图1

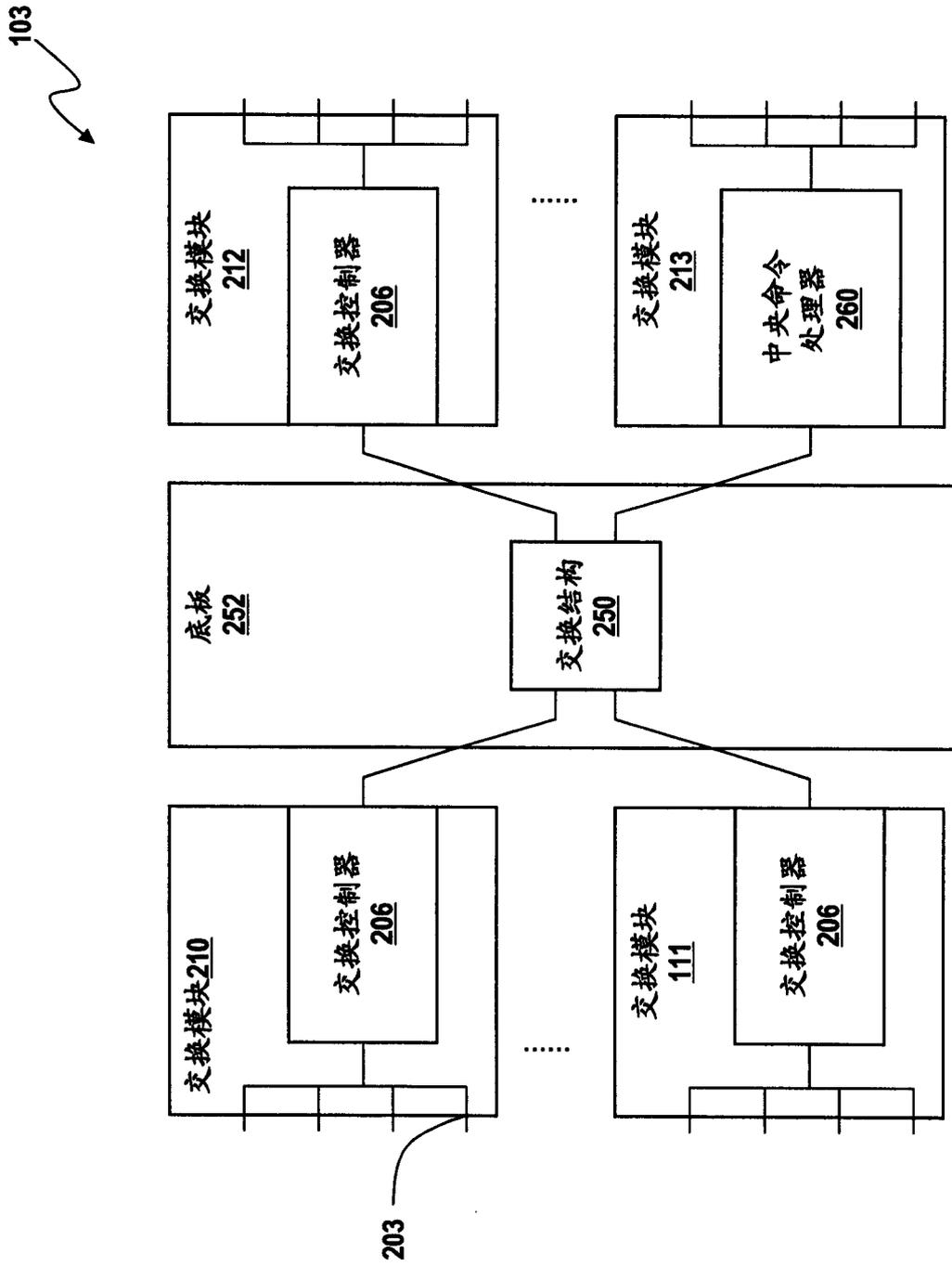


图2

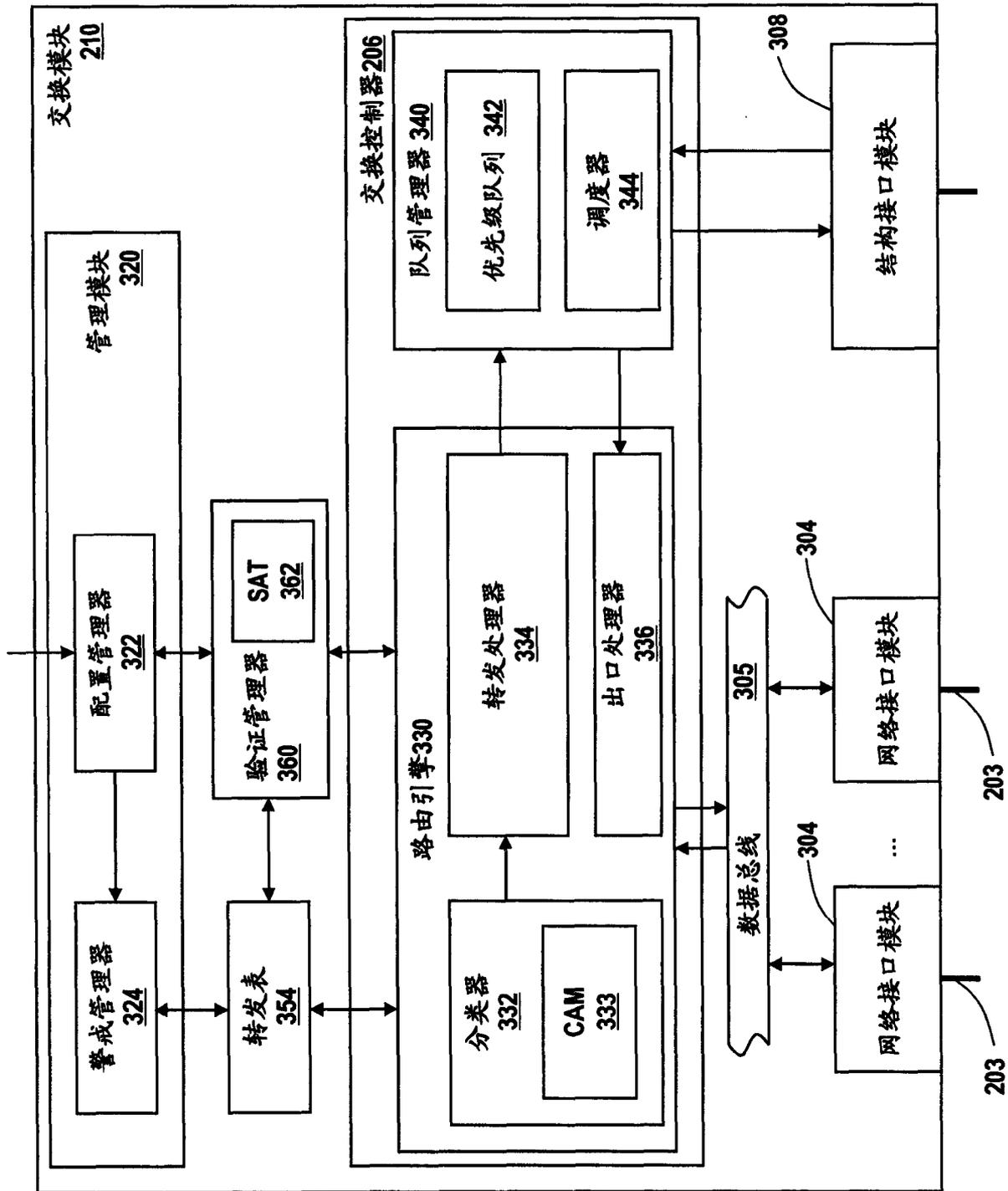


图3

362

| 共享许可表 | |
|--------|---------|
| SA 401 | VID 402 |
| SA-1 | VID-1 |
| SA-2 | VID-2 |
| SA-3 | VID-3 |
| ⋮ | ⋮ |

图 4

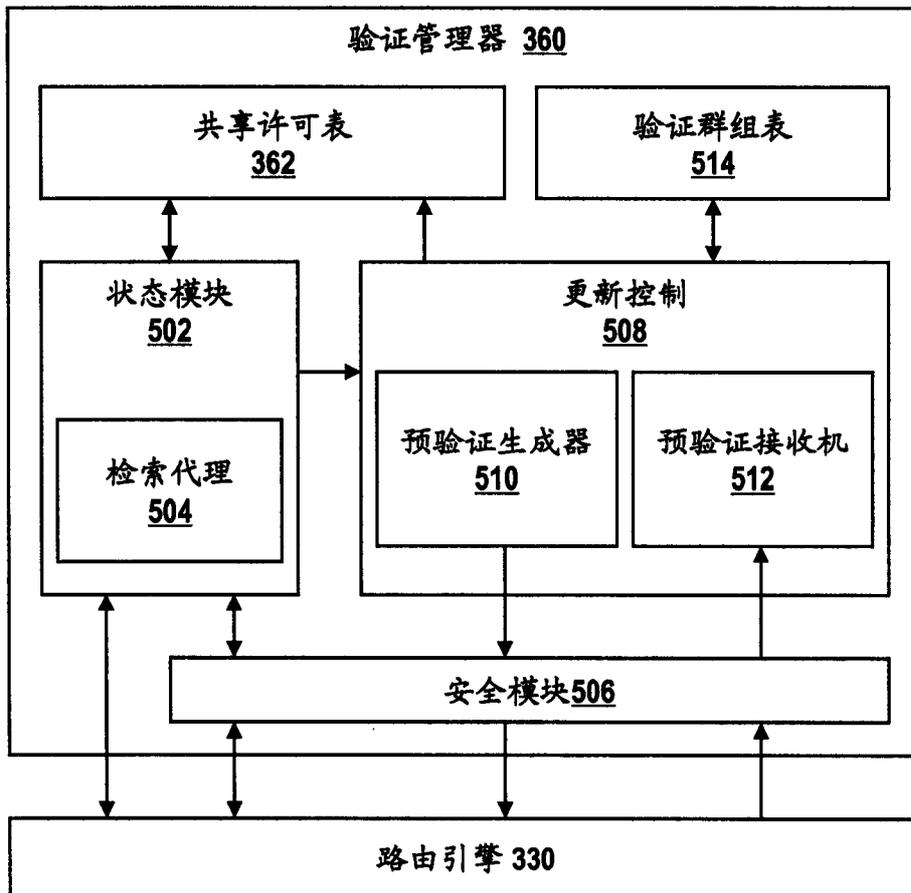


图 5

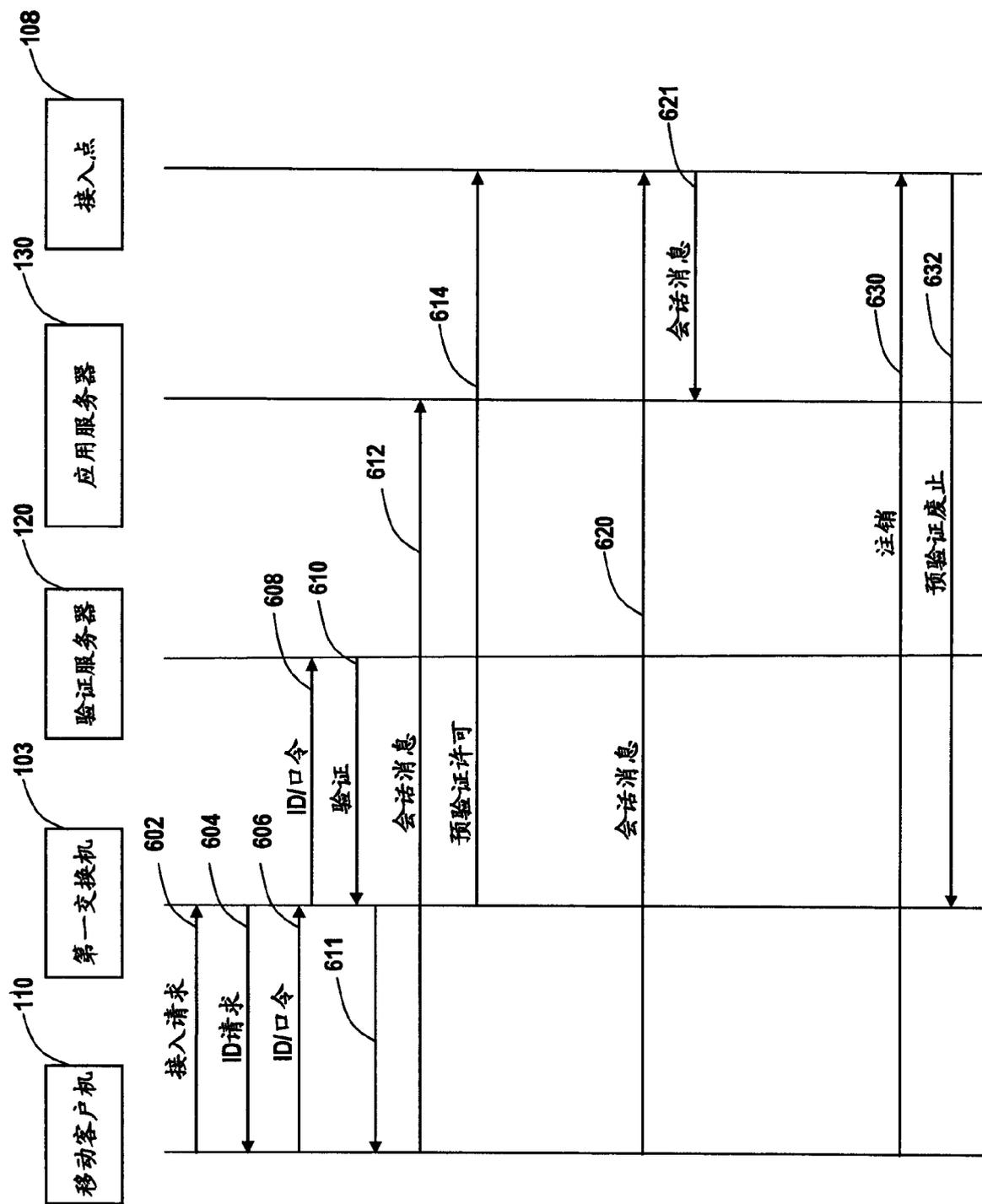


图6