

(12) 发明专利

(10) 授权公告号 CN 1864390 B

(45) 授权公告日 2010.10.27

(21) 申请号 200480029319.1

行至第 8 栏第 25 行，第 9 栏第 55 行至第 10 栏第 34 行。

(22) 申请日 2004.10.28

EP 1067745 A2, 2001.01.10, 摘要、说明书第 15-17 段，第 19-26 段，第 28-30 段。

(30) 优先权数据

10/696,629 2003.10.29 US

US 6304973 B1, 2001.10.16, 说明书第 12 栏第 41 行至第 13 栏第 63 行，第 14 栏第 66 行至第 15 栏第 16 行、图 4, 7.

(85) PCT 申请进入国家阶段日

2006.04.06

EP 0465016 A2, 说明书第 1 栏第 35-51 行，第 2 样第 56 行至第 3 样第 10 行，第 4 样第 13 行至第 5 样第 9 样，第 9 样第 19 行至第 10 样第 19 行。

(86) PCT 申请的申请数据

PCT/US2004/035853 2004.10.28

CN 1228174 A, 1999.09.08, 全文。

(87) PCT 申请的公布数据

W02005/046178 EN 2005.05.19

审查员 易水英

(73) 专利权人 思科技术公司

地址 美国加利福尼亚州

(72) 发明人 迈克尔·R·史密斯

(74) 专利代理机构 北京东方亿思知识产权代理

有限责任公司 11258

代理人 王怡

(51) Int. Cl.

H04L 29/06 (2006.01)

(56) 对比文件

EP 0849680 A2, 1998.06.24, 摘要、说明书第 4 样第 20-48 行，第 6 样第 1-57 行，第 7 样第 46

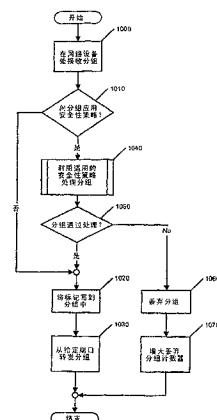
权利要求书 4 页 说明书 15 页 附图 14 页

(54) 发明名称

用于利用安全性标记提供网络安全性的方法和装置

(57) 摘要

公开了一种利用安全性标记来提供网络安全性的方法和设备。该方法包括比较第一安全性级别信息和第二安全性级别信息(1010)，并且基于该比较步骤指示要对分组执行的处理(1040)。第一安全性级别信息被存储在网络节点处接收到的分组(200)的安全性标记(220)中，而第二安全性级别信息被存储在该网络节点处。



1. 一种用于利用安全性标记来提供网络安全性的方法,包括 :

比较第一安全性级别信息和第二安全性级别信息,其中

所述第一安全性级别信息被存储在网络设备处接收到的分组的安全性标记中,

所述第二安全性级别信息被存储在所述网络设备处,

所述第二安全性级别信息被利用联接请求来注册在场境中,并且

所述场境是通用属性注册协议信息传播场境;以及

基于所述比较来指示要对所述分组执行的处理,其中

所述第一安全性级别信息代表第一安全性级别,并且

所述第二安全性级别信息代表第二安全性级别。

2. 如权利要求 1 所述的方法,其中

所述第一安全性级别和所述第二安全性级别实现多级安全性范例和多边安全性范例之一。

3. 如权利要求 1 所述的方法,其中

所述安全性标记是枚举型安全性标记和位图安全性标记之一。

4. 如权利要求 1 所述的方法,其中

所述第二安全性级别是所述网络设备的端口的安全性级别。

5. 如权利要求 4 所述的方法,还包括 :

设置所述端口的安全性级别。

6. 如权利要求 5 所述的方法,其中所述设置所述端口的安全性级别的步骤包括 :

将所述第二安全性级别存储在访问控制列表条目的安全性标记信息字段中。

7. 如权利要求 5 所述的方法,其中所述设置所述端口的安全性级别的步骤包括 :

将所述第二安全性级别存储在转发表条目的标记范围信息字段中。

8. 如权利要求 1 所述的方法,其中所述处理步骤包括 :

如果所述比较指示所述第一安全性级别小于所述第二安全性级别,则丢弃所述分组。

9. 如权利要求 1 所述的方法,其中

所述处理步骤包括至少以下之一:丢弃所述分组、重定向所述分组以及改写所述安全性标记。

10. 如权利要求 1 所述的方法,其中

所述第二安全性级别包括多个安全性级别。

11. 如权利要求 10 所述的方法,其中

所述多个安全性级别是安全性级别范围,并且

所述处理步骤包括如果所述比较指示所述第一安全性级别不在所述安全性级别范围之内,则丢弃所述分组。

12. 如权利要求 1 所述的方法,还包括 :

在所述网络设备处存储所述第二安全性级别信息。

13. 如权利要求 12 所述的方法,其中所述在所述网络设备处存储所述第二安全性级别信息的步骤包括 :

将所述第二安全性级别存储在访问控制列表条目的安全性标记信息字段中。

14. 如权利要求 12 所述的方法,其中所述在所述网络设备处存储所述第二安全性级别

信息的步骤包括：

将所述第二安全性级别存储在转发表条目的标记范围信息字段中。

15. 如权利要求 12 所述的方法,其中所述在所述网络设备处存储所述第二安全性级别的信息的步骤包括：

通过在所述场境中注册所述第二安全性级别的信息而传播所述第二安全性级别的信息。

16. 如权利要求 15 所述的方法,其中所述注册步骤包括：

通过对第三安全性级别的信息和所述第二安全性级别的信息执行逻辑或操作来更新所述第二安全性级别的信息。

17. 如权利要求 15 所述的方法,其中

所述注册是通过发出所述联接请求来完成的。

18. 如权利要求 12 所述的方法,其中所述在所述网络设备处存储所述第二安全性级别的信息的步骤包括：

将所述第二安全性级别的信息存储在所述网络设备的端口中。

19. 如权利要求 1 所述的方法,还包括：

确定所述第一安全性级别。

20. 如权利要求 19 所述的方法,其中所述确定步骤包括：

确定入口端口是否被标记为访问端口;以及

如果所述入口端口被标记为访问端口,则将所述入口端口的安全性级别设置成所述第一安全性级别。

21. 如权利要求 19 所述的方法,还包括：

认证具有所述第一安全性级别的用户,其中

仅当所述用户被认证时所述确定步骤才被执行。

22. 如权利要求 1 所述的方法,还包括：

基于所述比较来对所述分组执行所述处理。

23. 如权利要求 22 所述的方法,其中所述执行所述处理的步骤包括：

如果所述指示步骤指示所述分组被允许转发,则转发所述分组;以及

否则丢弃所述分组。

24. 如权利要求 22 所述的方法,其中所述执行所述处理的步骤包括：

如果所述指示步骤指示所述分组应当被转发到防火墙,则将所述分组转发到所述防火墙。

25. 如权利要求 1 所述的方法,还包括：

从所述分组上剥除网络安全信息;以及

将子网安全性信息添加到所述分组。

26. 如权利要求 25 所述的方法,其中

所述网络安全信息包括所述第一安全性级别的信息。

27. 一种用于利用安全性标记来提供网络安全性的设备,包括：

用于比较第一安全性级别的信息和第二安全性级别的信息的装置,其中

所述第一安全性级别的信息被存储在网络设备处接收到的分组的安全性标记中,

所述第二安全性级别的信息被存储在所述网络设备处,

所述第二安全性级别信息被利用联接请求来注册在场境中，并且
所述场境是通用属性注册协议信息传播场境；以及
用于基于所述比较来指示要对所述分组执行的处理的装置，其中
所述第一安全性级别信息代表第一安全性级别，并且
所述第二安全性级别信息代表第二安全性级别。

28. 如权利要求 27 所述的设备，还包括：

用于设置端口的所述安全性级别的装置，其中
所述第二安全性级别是所述网络设备的所述端口的安全性级别。

29. 如权利要求 28 所述的设备，其中所述用于设置所述端口的所述安全性级别的装置包括：

用于将所述第二安全性级别存储在访问控制列表条目的安全性标记信息字段中的装置。

30. 如权利要求 28 所述的设备，其中所述用于设置所述端口的所述安全性级别的装置包括：

用于将所述第二安全性级别存储在转发表条目的标记范围信息字段中的装置。

31. 如权利要求 27 所述的设备，还包括：

用于在所述网络设备处存储所述第二安全性级别信息的装置。

32. 如权利要求 31 所述的设备，其中所述用于存储的装置包括：

用于将所述第二安全性级别存储在访问控制列表条目的安全性标记信息字段中的装置。

33. 如权利要求 31 所述的设备，其中所述用于存储的装置包括：

用于将所述第二安全性级别存储在转发表条目的标记范围信息字段中的装置。

34. 如权利要求 31 所述的设备，其中所述用于存储的装置包括：

用于传播所述第二安全性级别信息的装置，该用于传播所述第二安全性级别信息的装置包括用于在所述场境中注册所述第二安全性级别的装置。

35. 如权利要求 27 所述的设备，还包括：

用于确定所述第一安全性级别的装置。

36. 如权利要求 35 所述的设备，还包括：

用于认证具有所述第一安全性级别的用户的装置，其中
仅当所述用户被认证时所述用于确定的装置才被执行。

37. 如权利要求 35 所述的设备，其中所述用于确定的装置包括：

用于确定入口端口是否被标记为访问端口的装置；以及

用于在所述入口端口被标记为访问端口的情况下将所述入口端口的安全性级别设置成所述第一安全性级别的装置。

38. 如权利要求 27 所述的设备，还包括：

用于对所述分组执行所述处理的装置，其中所述用于执行所述处理的装置利用由所述用于比较的装置生成的结果。

39. 如权利要求 38 所述的设备，其中所述用于执行所述处理的装置包括：

用于在所述用于指示的装置指示所述分组被允许转发的情况下转发所述分组的装置；

以及

用于在其他情况下丢弃所述分组的装置。

40. 如权利要求 27 所述的设备,还包括 :

用于从所述分组上剥除网络安全性信息的装置;以及

用于将子网安全性信息添加到所述分组的装置。

41. 一种网络设备,包括 :

网络接口,其中

所述网络接口被配置为接收分组,

所述网络设备被配置为存储第一安全性级别信息,

第二安全性级别信息是根据接收到的分组的安全性标记来确定的,

所述第一安全性级别信息被利用联接请求来注册在场境中,

所述场境是通用属性注册协议信息传播场境,

所述网络接口包括端口,

所述端口被配置为存储所述第一安全性级别信息,

所述网络设备还被配置为

比较所述第一安全性级别信息和第二安全性级别信息,并且

基于所述比较来指示要对所述分组执行的处理,

所述第一安全性级别信息代表第一安全性级别,并且

所述第二安全性级别信息代表第二安全性级别。

42. 如权利要求 41 所述的网络设备,其中

所述网络设备还被配置为从所述分组上剥除网络安全性信息并向所述分组添加子网
安全性信息。

43. 如权利要求 41 所述的网络设备,其中

所述第一安全性级别包括多个安全性级别。

用于利用安全性标记提供网络安全性的方法和装置

技术领域

[0001] 本发明涉及信息网络安全领域，尤其涉及用于通过使用安全性标记来保护网络通信的方法和装置。

背景技术

[0002] 当今的网络是用于在大量计算设备之间提供通信的高效且有效的平台。网络上的每个设备易于访问其他联网设备提供的信息和服务。但是，访问的便利性却大大增加了一个或多个这种网络设备上的外部攻击的危险。因此网络安全性越发重要。

[0003] 使问题变得复杂的是诸如无线、动态主机配置协议 (DHCP)、虚拟专用网 (VPN) 网关之类的网络访问技术所提供的灵活性，这些技术允许用户从各种访问点或进入点访问给定的受保护网络。这对于各种网络都是成立的，包括企业网络、服务提供商网络等等。因此在提供这种访问的同时提供安全性越来越受到关注。基于远程认证拨入用户服务 (RADIUS)、终端访问控制器访问控制系统 (TACACS)、DIAMETER 协议和其他协议的技术允许了用户在进入网络时被认证。

[0004] 正如已知的，这种网络上的通信路径从概念上来说是分离的（例如可被视为分离的虚拟路径），虽然它们可能穿越某些或所有相同的网络设备（例如物理网段），并且因此被用例如访问控制列表 (ACL) 单独控制。传统上，网络用户所享有的访问制约是由 ACL 来实施的，这些 ACL 被用于处理分组，从而控制这种用户的网络流量。为了可缩放性和可管理性，传统 ACL 要求用户主机地址（作为给定分组的源；例如互联网协议 (IP) 地址）映射相对静态，或者安全性策略充分宽松以允许用户的所有可能的地址。

[0005] 当今的安全性 ACL 有着许多弱点。这些 ACL 传统上被应用到给定接口并且包含将安全性策略直接联系到网络拓扑的 IP 地址。结果，诸如重新划分子网这样的网络变化会导致安全性策略被再次访问。此外，可能会出现这种情况：每当有用户被认证到网络时，网络的各种部分中的 ACL 将会需要被更新，以便添加与指派给该用户的主机的源 IP 地址相关联的规则，这对于该用户可能是特定的。这将会导致独特的 ACL 的数目的剧增，并且会使这种规则需要被更新的速率剧增。

[0006] 在给定 ACL 内，也存在由于个体 IP 地址的表达而产生的规模剧增问题，其中条目数目通常是源地址数目乘以目的地地址数目再乘以许可数目。从而，添加单个 IP 地址就可能对大量 ACL 的规模有巨大影响。

[0007] 当顾客改变网络拓扑时，ACL 必须被重新检查。由于这种 ACL 的长度相当容易达到数百行或甚至数千行，退一步说，这种重新检查将可能不是无关紧要的。由于这种 ACL 的复杂性，对所做出的改变的置信度一般并不很高，并且 ACL 在被置于生产环境之前常需要用户进行广泛的测试。此外，由于利用内容可寻址存储器 (CAM) 来实现 ACL 的平台在做出改变时需要重新编译某些或所有 ACL，因此处理成本的增大可能会相当严重，接近用户数目的平方。这些复杂性增大增加了网络停机、安全性漏洞或两者的机率。单个 ACL 将用户能力扩展到管理其安全性策略。因此将这种 ACL 置于整个企业网络中影响了当今网络的可管

理性。考虑到上述内容,尤其是根据目前所要求的以及将来将会要求的越来越灵活的访问,依赖于现有的基于 ACL 的解决方案是困难的。

[0008] 因此所需要的是高效识别网络流量的机制。优选地,这种方法应当针对解决使用现有 ACL 技术时遇到的局限性。还优选地,这种方法应当允许网络易于重新配置和发展,而不会招致不成比例的管理负担或消耗过于大量的网络资源。

发明内容

[0009] 在一个实施例中,公开了一种用于利用安全性标记来提供网络安全性的方法。该方法包括比较第一安全性级别信息和第二安全性级别信息,并且基于该比较指示应当对分组执行的处理。第一安全性级别信息被存储在网络节点处接收到的分组的安全性标记中,而第二安全性级别信息被存储在网络节点处。

[0010] 在另一个实施例中,公开了一种网络设备。该网络设备包括网络接口。网络接口被配置为接收分组。网络设备被配置为存储第一安全性级别信息并且利用第一安全性级别信息处理分组。

[0011] 在一个实施例中,公开了一种用于利用安全性标记来提供网络安全性的方法,包括:比较第一安全性级别信息和第二安全性级别信息,其中所述第一安全性级别信息被存储在网络设备处接收到的分组的安全性标记中,所述第二安全性级别信息被存储在所述网络设备处,所述第二安全性级别信息被利用联接请求来注册在场境中,并且所述场境是通用属性注册协议信息传播场境;以及基于所述比较来指示要对所述分组执行的处理,其中所述第一安全性级别信息代表第一安全性级别,并且所述第二安全性级别信息代表第二安全性级别。

[0012] 在另一个实施例中,公开了一种用于利用安全性标记来提供网络安全性的设备,包括:用于比较第一安全性级别信息和第二安全性级别信息的装置,其中所述第一安全性级别信息被存储在网络设备处接收到的分组的安全性标记中,所述第二安全性级别信息被存储在所述网络设备处,所述第二安全性级别信息被利用联接请求来注册在场境中,并且所述场境是通用属性注册协议信息传播场境;以及用于基于所述比较来指示要对所述分组执行的处理的装置,其中所述第一安全性级别信息代表第一安全性级别,并且所述第二安全性级别信息代表第二安全性级别。

[0013] 在另一个实施例中,公开了一种网络设备,包括:网络接口,其中所述网络接口被配置为接收分组,所述网络设备被配置为存储第一安全性级别信息,第二安全性级别信息是根据接收到的分组的安全性标记来确定的,所述第一安全性级别信息被利用联接请求来注册在场境中,所述场境是通用属性注册协议信息传播场境,所述网络接口包括端口,所述端口被配置为存储所述第一安全性级别信息,所述网络设备还被配置为比较所述第一安全性级别信息和第二安全性级别信息,并且基于所述比较来指示要对所述分组执行的处理,所述第一安全性级别信息代表第一安全性级别,并且所述第二安全性级别信息代表第二安全性级别。

[0014] 前述内容是概要性的,因此必然包含对细节的简化、概括和省略;因此,本领域的技术人员将会意识到发明内容只是说明性的,而绝不想要是限制性的。本发明的其他方面、创造性特征和优点仅由权利要求限定,并且将会在以下阐述的非限制性具体实施方式中显

现出来。

附图说明

- [0015] 本领域的技术人员通过参考附图可以更好地理解本发明，并且可以更清楚看到许多目的、特征和优点。
- [0016] 图 1 是示出本发明可在其中实现的包括主机和服务器的网络体系结构的示例的图。
- [0017] 图 2 是示出根据本发明实施例的分组的框图。
- [0018] 图 3 是示出根据本发明实施例的场境 (context) 的框图。
- [0019] 图 4 是示出根据本发明实施例的网络的图。
- [0020] 图 5 是示出根据本发明实施例用于图 4 所示的网络的生成树 (spanning tree) 的框图。
- [0021] 图 6 是示出根据本发明实施例的转发表的示例的框图。
- [0022] 图 7 是示出根据本发明实施例的访问控制列表 (ACL) 的示例的框图。
- [0023] 图 8 是示出本发明可在其中实现的网络体系结构的另一个示例的图。
- [0024] 图 9 是示出根据本发明实施例的网络中的用户认证的示例的流程图。
- [0025] 图 10 是示出根据本发明实施例的网络中的分组标记的示例的流程图。
- [0026] 图 11 是示出根据本发明实施例的网络中的分组处理的示例的流程图。
- [0027] 图 12A 是示出根据本发明实施例的网络中的交换机处的分组接收、标记和转发的示例的流程图。
- [0028] 图 12B 是示出根据本发明实施例的网络中的入口路由器处的分组接收、标记和转发的示例的流程图。
- [0029] 图 13 是示出根据本发明实施例的网络中的出口路由器处的分组接收、标记和转发的示例的流程图。
- [0030] 图 14 是示出根据本发明实施例的网络中的分组认证的示例的流程图。
- [0031] 不同附图中使用相同的标号指示类似或相同的项目。

具体实施方式

[0032] 以下内容想要提供对本发明的示例的详细描述，而不应当被理解为限制本发明本身。更确切地说，任何数目的变化都可能落在说明书之后的权利要求书中所限定的本发明的范围内。

引言

[0034] 本发明提供了一种方法和装置，该方法和装置通过向利用该方法输送的分组添加安全性标记形式的安全性信息来保护网络通信。在通过认证协议（例如电气电子工程学会 (IEEE) 标准 802.1X-2001）认证给定网络访问端口上的用户之后，认证服务器可向网络设备（例如第 2 层交换机）提供针对该访问端口的安全性标记形式的安全性信息。该安全性标记随后被用于利用安全性标记字段（例如利用 IEEE 标准 802.10-1998 可以支持的封装）来标记来自主机的分组。在出口网络访问端口处，分组的安全性信息（即安全性标记）被与出口端口的安全性信息（出口端口的安全性标记）相比较。此时，可基于该比较做出关

于分组处理的决定。例如,可以决定许可或拒绝对分组的访问。从而,如果分组的安全性级别高于接收分组的端口,则分级例如可被丢弃。或者,如果端口支持某个安全性级别范围,则如果分组的安全性级别不在该安全性级别范围内,则分组可被丢弃。

[0035] 这里所描述的是用于采用安全性分组标记的安全性标记删改 (pruning) 协议。在一个实施例中,根据本发明的安全性标记删改协议被实现为通用属性注册协议 (GARP) 安全性标记注册协议 (GSRP)。顾名思义,这种协议实现采用了通用属性注册协议 (GARP) 的特征,如在 ANSI/IEEE 标准 802.1D 1998 年版第 12 节 (通用属性注册协议 (GARP)) 和第 13 节 (GARP 的示例性“C”代码实现) 中所描述的那样,在这里通过引用将其完全结合进来用于所有目的。

[0036] GSRP 独立于其他协议 (包括其他基于 GARP 的协议) 地运行,并且在运行时使与其他采用 GARP 协议的干扰达到最小限度。此外,根据本发明标记的分组能够无缝地经过非 GSRP 感知网络设备 (例如交换机)。在一个实施例中,GSRP 对于每个生成树使用单个 GARP 信息传播 (GIP) 场境 (例如 IEEE 802.1D-1998 所定义)。在典型场景中,访问链路携带未被标记的分组,交换机间 (主干) 链路携带被标记的分组。存在于访问链路上的被标记的分组被丢弃、重定向,或者在服从管理控制的情况下使其安全性标记被改写。

[0037] 在一个实施例中,安全性标记中包含的信息是根据联邦信息处理标准出版物 188 (FIPS PUB 188,标题为“Standard Security Label for Information Transfer (用于信息传送的标准安全性标记)”,1994 年 9 月 6 日,在这里通过引用将其完全结合进来用于所有目的) 来格式化的。利用这种标记格式,GSRP 可被配置为利用 FIPS PUB 188 中定义的若干种标记格式 (其中包括限制性位图型、枚举型、范围型、非约束性位图型和“自由形式”型 (允许用户定义的数据)) 中的一种。这里所描述的两种格式对应于安全性标记的两种不同类型:枚举型安全性标记 (涉及多级安全性范例,例如军方所使用的那种) 和位图安全性标记 (涉及多边安全性范例,例如受信计算中所使用的那种)。

[0038] 当利用枚举型安全性标记时,每个链路具有与其相关联的最小和最大安全性标记。最小安全性标记是被认证的实体希望接收到的分组的最小安全性级别。最大安全性标记是被认证的实体被允许接收的分组的最大安全性级别。每个 GSRP 客户端针对该客户端的最小和最大安全性标记发出联接 (join) 请求 (例如按照 GARP 协议)。最小和最大安全性标记被编码为两种不同的属性类型 (同样是按照 GARP 协议)。联接请求是在特定主机所在的每个 GIP 场境上发出的。由于 GIP 场境与生成树相关联,因此主机可能不知道 VLAN 到生成树绑定。在这种情况下,主机可在主机所属的每个 VLAN 上发送联接请求。在生成树感知网络设备 (例如交换机) 上,这将会导致针对该属性的单个 GID 注册。

[0039] 在网络边缘处,这个生成树感知网络设备或者是运行受信操作系统的启用了 GSRP 的主机,或者是在利用诸如 802.1X 之类的认证协议进行本地认证之后代表主机的安全网络设备 (例如安全网络交换机)。以下论述是就子网级别 (例如第 2 层) 上的交换而言的,但是将会意识到,所论述的技术适用于更多种场景。

[0040] 虽然给定的交换机间链路包含针对各种安全性标记的多个 GID 注册,但是向附接的网段应用最小和最大安全性标记是 GSRP 应用的责任。启用 GSRP 的交换机上的每个端口的最小安全性标记是 GID 注册器在该特定端口上接收到的最低安全性标记注册。启用 GSRP 的交换机上的每个端口的最大安全性标记是 GID 注册器在该特定端口上接收到的最高安

全性标记注册。当在交换机间链路（802.1Q 干线）上使用 802.1Q VLAN 标记时，最小和最大安全性标记被指派给 { 端口, VLAN} 对。当共享网段存在于 GIP 场境中时，仅当网段上联接的最小安全性标记高于 GID 申请者希望申请的最小安全性标记时 GID 申请者才发送联接请求。类似地，仅当网段上联接的最大安全性标记低于 GID 申请者希望申请的最大安全性标记时，GID 申请者才发送联接请求。

[0041] 在两种格式的第二种中（例如当使用位图安全性标记时），每个链路具有相关联的安全性标记位图。每个 GSRP 客户端针对所需要的安全性标记位图发出联接请求（同样是按照 GARP 协议）。传播发生的方式与枚举型安全性标记相同。主要差异是交换机间链路上的行为。给定的交换机间链路将会包含针对各种安全性标记位图的多个 GID 注册。GSRP 应用负责对 GID 注册器在该特定端口上接收到的所有安全性标记位图进行或 (OR) 操作。

[0042] 将会意识到，可采用其他方法来实现利用本发明控制分组安全性。例如，认证也可被应用到利用 IEEE 802.10 封装的 GSRP PDU。在该实施例中，网桥可充当 IEEE 802.10 多播群组，以及用于认证的单个共享关键字。

[0043] 本发明提供了多个优点。根据本发明的协议将基于安全性标记分组的安全性从网络的出口边缘移动到较深处的核心和更接近流量源头。这提高了网络的整体安全性，减少了来自所需路径的分类流量的潜在泄漏，提供了针对分布式拒绝服务攻击的保护，还提高了可用的网络带宽。此外，虽然这里提供的示例是针对 IEEE 802.10 安全性标记分组的，但是应当意识到，本发明的协议可用于删改任何形式的安全性标记分组。

实现安全性标记的网络的示例

[0045] 图 1 是示出网络体系结构 100 的示例的框图，该网络体系结构 100 包括主机 110 和 111 以及服务器 120 和 121，本发明可在其中实现。主机 110 和服务器 120 经由企业核心网络 140 彼此通信。企业核心网络 140 包括多个网络设备，但是为了简单起见，被示为包括彼此互连的多个路由器（在图 1 中示为路由器 150(1)-(N)）。为了允许企业核心网络 140 的用户访问企业外部的计算机，企业核心网络 140 经由防火墙 170 与互联网 160 通信。对防火墙 170 的访问（因而对互联网 160 的访问）是在路由器 150(1)-(N) 之一（例如路由器 150(5)）处提供的。

[0046] 将会注意到，可通过使用根据本发明实施例的技术来使路由器 150(1)-(N) 中的多个路由器之间的链路（示为链路 180(1)-(N)）安全。但是，正如将会意识到的，从分组安全性观点来看，企业核心网络 140 外部的链路（例如链路 190(1)-(4)）却不一定安全的。还将会意识到，在某些实施例中可通过根据本发明在给定服务器（例如服务器 121）上运行受信操作系统并且标记分组（在这种场景中服务器 121 被称为“受信服务器”），来使通信（例如服务器 121 和路由器 150(6) 之间的通信）安全。在这种情况下，耦合路由器和服务器的链路（例如链路 190(5)）被视为安全性干线端口。

[0047] 将会注意到变量标识符“N”被用于这里所描述的附图中的若干个实例中，以便更简单地标明一系列相关或类似的元件（例如路由器 150(1)-(N) 和链路 180(1)-(N)）中的最终元件。重复使用这种变量标识符不是想要必然地暗示这种元件系列的规模之间的相关性，虽然这种相关性是可能存在的。使用这种变量标识符不要求每个元件系列与由相同变量标识符定界的另一系列具有相同数目的元件（例如路由器和链路）。更确切地说，在每个使用实例中，由“N”（或任何其他这种标识符）所标识的变量可以保存与相同变量标识符的

其他实例相同或不同的值。

[0048] 图 2 是示出根据本发明实施例的带安全性标记的分组 200 的框图。带安全性标记的分组 200 包括控制信息 210、安全性标记 220 和原始分组信息 230。原始分组信息 230 包括最初作为要被递送到目的地的网络分组而被发送的信息。控制信息 210 和安全性标记 220 是由本发明的实施例添加的，以便允许安全地输送包含在原始分组中的信息（例如原始分组信息 230）。

[0049] 安全性标记 220 指示发起分组的用户、主机或其他网络实体 / 设备的安全性级别。控制信息 210 包含关于先前对分组进行的网络操作的信息（例如关于分组曾经过防火墙，分组到 SMTP 端口被应用了防病毒措施等等的指示），以及关于希望对分组执行的动作的信息（例如加速特征交换 (AFS)、安全性服务质量 (QoS) 信息、用于加速安全性设备的分类标签（例如关于源自内部 / 外部的流量的指示）、被分布式安全性设备所使用的信息，等等）。将会意识到，这种信息也可被直接反映在安全性标记 220 中包括的信息中。

[0050] 带安全性标记的分组 200 经由路由器 150(1)-(N) 中的各路由器之间的传输而穿越企业核心网络 140。例如，主机 110 所发送的、目的地为服务器 120 的分组经由链路 190(1) 被路由器 150(1) 接收、经由路由器 150(2)-(N-1)（不一定包括所有）之一被输送，并且经由链路 190(2) 被路由器 150(N) 提供给服务器 120。在这里，链路 180(1)-(N) 被称为安全性干线（因此耦合到这种安全性干线的端口被称为安全性干线端口）。当分组经由安全性干线被输送时，所有这种分组都被加上安全性标记，并且未被标记的分组被重定向或丢弃。以类似的方式，路由器 150(1)-(N) 之一的耦合到不安全的计算机（例如经由链路 180(1)-(3) 之一）的端口在这里被称为安全性访问端口。在安全性访问端口处，没有分组具有安全标记，因此被标记的分组或者被重定向、丢弃，或者它们的标记被删除或改写。安全性访问端口的示例是路由器 150(1) 上的耦合到主机 110 的端口。

[0051] 在这种场景中，利用适当的基于介质的认证协议（例如 IEEE802.1X、IEEE P802.11i/D3.0、点对点协议 (PPP)、生物测定等），用户被认证到直接连接的网络设备（例如交换机或路由器）。在认证过程中，负责的认证服务器将指派给被认证的用户耦合到的端口的适当安全性级别通知给网络设备。将会注意到，在给定网络中，网络的安全性策略将会限定安全性级别，并且还可能限定安全性关联的范围（例如，对于此 [phy port], [MAC, phy port], [IP address, phy port] 等等）。

[0052] 正如将会意识到的，这种认证只能发生在已经被标记为安全性访问端口的端口上。正如先前注意到的，预期安全性访问端口上的分组不会具有安全性标记，这是因为这种分组是从不安全的源接收到的（至少从根据本发明的技术的角度来看是这样），因此不包含适当的安全性标记。正如还注意到的，在安全性访问端口上接收到的包括安全性标记的分组一般由于其被标记而被丢弃。还将会注意到，先前所述的认证一般只在网络边缘处（例如路由器 150(1) 处）执行，而不在网络设备（例如路由器 150(1)-(N)）之间执行。

[0053] 一旦被标记，来自给定安全性干线端口的网络流量被允许流入企业核心网络 140 中。每个来自安全性干线端口的分组被标记以安全性标记，该标记在最小限度上会指示发起该分组的用户的安全性级别。在这种分组穿越企业核心网络 140 时，企业核心网络 140 内的策略（实现在路由器 150(1)-(N) 上）被以类似于访问控制列表的方式基于分组的安全性标记而应用。

[0054] 但是,策略不是基于网络地址实现的,而是基于网络内的各种实体的安全性级别来实现的。将会意识到,虽然这种策略很可能被应用到出口点(例如路由器 150(N)),但这并非强制性的。这种策略可以被推入企业核心网络 140 中,从而被其中的网络设备(路由器 150(1)-(N-1))所应用,或者在入口点(例如路由器 150(1))处被应用。

[0055] 可以想象很多种这样的安全性策略。例如,网络设备可被配置为阻止针对超过原始用户的安全性级别的设备的分组。在另一个示例中,所有安全性级别都可能被允许与给定服务器交谈,但是具有低于给定值的安全性级别的分组被发送经过防火墙。此外,可实现防止主机获得较高的安全性级别的安全性策略。从而,即使诸如主机 110 这样的主机要被征用,其他具有较高安全性级别的系统也将由于无法改变流量的安全性级别而保持安全。正如将会意识到的,当使用受信操作系统的计算机与根据本发明配置的网络被结合使用时,多级安全性能能力被分布到网格上,从而产生了所谓的“受信网络”。

[0056] 图 3 是示出通用属性注册协议 (GARP) 信息传播 (GIP) 场境 300 的框图。在 GIP 场境 300 内,包括了多个 GARP 信息声明 (被示为 GARP 信息声明 (GID) 310(1)-(N)), 并且分别与多个申请者 (被示为申请者 320(1)-(N)) 相关联。GID 310(2) 将经历联接操作 (被示为联接请求 330)。

[0057] 根据本发明的一个实施例,诸如 GIP 场境 300 这样的 GIP 场境是在每生成树基础上使用的(联系图 4 和 5 论述的一个方面)。在图 3 的设置中,只有当主机 / 服务器联接的最小安全性级别低于与申请者相关的注册器已经记录的安全性级别时,或者当最大安全性级别高于先前联接的安全性级别时,才发送联接(例如联接 330)。从而,对于每个端口,存在两种不同的属性类型:最小安全性标记和最大安全性标记。给定端口的最大安全性级别是 GID 注册器(未示出)所接收到的最高安全性级别。该端口的最小安全性级别是 GID 注册器接收到的最低安全性级别。从而端口的位图是该端口上接收到的安全性位图的逻辑或。一旦限定此最低限度信息(或采用缺省),则该端口就能够正确地处理 GSMP 分组。

[0058] 在基于 IEEE 标准的网络中,GSMP 分组(在这里也被称为协议数据单元 (PDU))例如可经由 IEEE 802.10 封装被认证。正如所注意到的,在这种场景中,网桥可被配置为以与 IEEE 802.10 多播群组类似的方式动作。还将会意识到,如果安全性干线端口也是 VLAN(即 IEEE 802.1Q-1998) 干线端口,则最小 / 最大标记是在每 { 端口, VLAN} 基础上指派的。

[0059] 图 4 是示出根据本发明实施例的网络 400 的框图。网络 400 包括多个网络设备(被示为网络设备 410(1)-(12))。正如本领域的技术人员将会理解的,网络设备 410(1)-(12) 只是可用于形成网络 400 的网络设备的示例。正如将会意识到的,这种网络设备的一个示例是路由器。正如可看出的,网络设备 410(1)-(12) 中的每一个包括多个端口(在图 4 中示为端口 420(1,1)-(12,5))。虽然网络设备 410(1)-(12) 中的每一个被示为包括五个端口,但是将会意识到网络设备 410(1)-(12) 也可以具有更多端口或更少端口。还将会意识到,图 4 所示的端口 420(1,1)-(12,5) 之间的连接只是这种耦合可能采取的多种可能部署的示例。

[0060] 在枚举型安全性标记被用于实现多级安全性范例的情况下,安全性标记信息被用于提供数据 / 用户分类级别。在这种场景中,认证服务器指派包括最小和最大安全性级别的安全性标记。所指派的最小安全性级别是该实体(用户、主机等等)将会接受的分组的最小安全性级别,因此限定了被允许与给定网络设备通信的实体。类似地,所指派的最大安

全性级别是该实体（用户、主机等等）将会接受的分组的最大安全性级别，因此限定了该给定网络设备被允许与之通信的实体（以及该网络设备被允许访问的信息）。将会意识到，在这种场景中，要使标记被正确地处理，分组只需要被标记以单个安全性级别。

[0061] 在位图安全性标记被用于实现多边安全性范例的情况下，安全性标记信息被用于在分类级别不适当的情况下（例如通过功能（例如市场、工程等等）更好地定界的公司环境）提供数据访问群组或用户群组。在这种场景中，认证服务器指派安全性位图，该安全性位图例如包括具有一个或多个位集合的位图，从而指示在一个或多个安全性群组（例如数据访问或用户群组）中的成员资格。就像先前一样，数据分组只需要被标记以单个安全性级别。但是，在使用位图安全性标记时，在位图中可设置多位，从而允许用户、主机或网络实体享有多个安全性群组中的成员资格。

[0062] 对于这里所描述的信号，本领域的技术人员将会认识到可以直接将信号从第一块传输到第二块，或者可以在块之间修改（例如放大、衰减、延迟、锁存、缓冲、反相、过滤或其他方式修改）信号。虽然上述实施例的信号被表征为被从一个块传输到下一个块，但是本发明的其他实施例可以包括取代这种直接传输的信号的经修改的信号，只要信号的信息和/或功能方面被在块间传输即可。在某种程度上，在第二块处输入的信号可以被概念化为由于所涉及的电路的物理局限性（例如不可避免地会有一些衰减和延迟）而从输出自第一块的第一信号得出的第二信号。因此，这里所使用的从第一信号得出的第二信号包括第一信号或对第一信号的任何修改，不论该修改是由电路局限性引起的还是由于经过其他不改变第一信号的信息和/或最终功能方面的电路元件所引起的。

[0063] 以上描述了不同组件被包含在不同其他组件内的实施例（例如被示为网络设备410(1)-(N)的组件的各种元件）。应当理解，所示出的这种体系结构只是示例性的，实际上可以实现许多其他的实现相同功能的体系结构。从抽象但仍明确的意义上来说，任何用于实现同一功能的组件部署被有效地“关联”以便实现所需功能。从而，在这里被组合以实现特定功能的任何两个组件可被看作彼此“关联”以便实现所需功能，而不论体系结构或中间组件如何。类似地，任何两个如此关联的组件也可以被视为是被“可操作地连接”或者“可操作地耦合”到彼此以便实现所需功能的。

[0064] 图5是示出与图4（即网络400）的网络设备410(1)-(12)之间的耦合相对应的生成树的框图。如图5所示，生成树500（例如IEEE 802.1D生成树）被用于表示网络400内的通信路径。以网络设备410(1)内的模块开始，申请者502向注册器506发出联接请求504（以图3的联接330的方式）。注册器506与申请者508相关联。申请者508又向多个注册器（注册器510、512和514）提出申请。注册器510与申请者516相关联，该申请者516经由端口420(1,1)访问网络400。类似地，注册器512与申请者518相关联，该申请者518经由端口420(1,3)访问网络400。以类似的方式，注册器514与申请者520相关联，该申请者520经由端口420(1,5)访问网络400。

[0065] 申请者516、518和520又向多个注册器提出申请。经由端口420(1,1)和420(2,1)之间的连接，申请者516向注册器522提出申请，该注册器522与申请者524相关联。申请者524经由端口420(2,2)和420(5,2)向注册器526（其与申请者528相关联）提出申请。申请者524还经由端口420(2,3)和420(6,5)向注册器530（其与申请者532相关联）提出申请。最后，申请者524经由端口420(2,4)和420(7,2)向注册器534（其与申请者536

相关联)提出申请。

[0066] 以类似的方式,申请者 518 经由端口 420(1,3) 和 420(3,2) 向注册器 538 提出申请。注册器 538 与申请者 540 相关联。申请者 540 经由端口 420(3,3) 和 420(8,1) 向注册器 542(其与申请者 544 相关联)提出申请。申请者 540 还经由端口 420(3,4) 和 420(9,3) 向注册器 546(其与申请者 548 相关联)提出申请。最后,申请者 540 经由端口 420(3,5) 和 420(10,1) 向注册器 550(其与申请者 552 相关联)提出申请。

[0067] 耦合到网络设备 410(1) 的端口之一的最后一个申请者,即申请者 520,经由端口 420(1,5) 和 420(4,3) 向注册器 554 提出申请。与注册器 554 相关联的是申请者 556。申请者 556 经由端口 420(4,4) 和 420(11,3) 向注册器 558(其与申请者 560 相关联)提出申请。申请者 556 还经由端口 420(4,5) 和 420(12,4) 向注册器 562(其与申请者 564 相关联)提出申请。

[0068] 因此将会意识到,生成树 500 内的申请者与 GIP 场境 300 内的申请者类似。从而,申请者发出联接请求(例如联接请求 504(与联接请求 330 类似)),以便在整个生成树 500 内公布其安全性级别。这使得能够基于连接到给定端口的网络设备的安全性级别在整个网络内设置正确的安全性级别。从而安全性措施可从出口接口被推到核心网络中的网络设备,从而提供了许多优点。一个这种优点是保护较高安全性的网络实体不受到具有较低分类的网络实体的定向拒绝服务攻击。由于先前丢弃的踪迹路线(traceroute)、扫描(sweep)等,提高了对剽窃的抵抗性。这些优点部分是源于可在每个网跳(network hop)处加强安全性这一事实。此外,这种解决方案提供了与可在受信操作系统中获得的多实例化(polyinstantiation)类似的保护。

[0069] 在这种场景中,每个边缘端口具有经由用户认证提供的来自策略服务器的安全性信息。例如,可以实现多级安全性模型(例如最小、最大安全性级别对)或者多边安全性模型(例如包含一个或多个位集合的位图)。从而每个核心端口经由适当的协议接收安全性信息。在多级安全性模型的情况下,维护关于经由端口可到达的网络/主机的最低最小和最高最大安全性级别的信息。在多边安全性模型的情况下,维护包含经由端口可到达的网络/主机中的所有位集合的超集。将会意识到,端口还可具有静态配置的多级范围和/或多边位图。

[0070] 图 6 是示出根据本发明实施例的转发表 600 的示例的框图。转发表 600 包括多个转发表条目(示为转发表条目 610(1)-(N))。转发表条目 610(1)-(N) 中每一个包括媒体访问控制(MAC)地址字段(示为 MAC 地址字段 620(1)-(N))、虚拟局域网(VLAN)标识符字段(示为 VLAN 标识符字段 630(1)-(N))、端口标识符字段(示为端口标识符字段 640(1)-(N))以及安全性标记范围信息字段(或者更简单地说是标记范围字段;示为安全性标记范围信息字段 650(1)-(N))。

[0071] 如前所述,转发表 600 中包含的各种字段之间的映射使端口、VLAN、地址和标记(或标记范围)信息相互联系。从而,MAC 地址和 VLAN 标识符可以与物理端口(由端口的端口标识符所指示)以及端口的安全性级别(由端口的安全性标记(范围)所指示)相联系。端口被申请者联接端口的相关注册器所属的 GIP 场境的过程指派安全性级别(或安全性级别范围),其被存储在转发表中端口的条目的各自的标记范围信息字段中。分组的 MAC 地址、分组的 VLAN 标识符和/或者在其上接收到分组的端口的端口标识符随后可被用于确

定适用的（一个或多个）安全性级别。例如，可基于在其上接收到分组的端口以及分组的 VLAN 来识别分组的安全性级别。这允许了网络内的网络设备基于分组的安全性标记决定如何处理分组。此外，这种技术可以用按端口索引的单独的表来实现，从而允许了集中式方法，以便转发表不需要包含范围。在这种情况下，范围被存储在另一个按端口标识符索引的表中。

[0072] 将会意识到，将这种信息存储在转发表中的一种可能的备选方案是将标记范围存储在端口本身中（例如在硬件寄存器、存储器等中）。在这种情况下，给定分组是在分组的出口端口处被检查的。这样一来，每个端口（例如出口端口）可以以图 5 所示的方式在给定分组的源和计划目的地之间的中间网络设备处执行分组的过滤。在使用根据本发明的协议（例如 GSRP）时，如前所述，协议分组被安全性干线端口所接受，并且被安全性访问端口所丢弃。正如先前联系图 3、4 和 5 所描述的，这种协议对于每个生成树使用单个 GIP 场境。在一个实施例中，存在两种不同的属性类型：最小安全性标记（MaxSL；指示最大安全性级别）和最大安全性标记（MinSL；指示最小安全性级别）。端口的最大安全性级别是该端口的 GID 注册器接收到的最高安全性级别，端口最小安全性级别是该端口的 GID 注册器接收到的最低安全性级别。这可以以多种方式来实现。例如，端口的安全性位图可以是在该端口上接收到的所有安全性位图的逻辑或，在实现多边安全性范例时通常就是这种情况。或者，关于最大和最小安全性级别的信息可以被维护（例如利用上述 MaxSL 和 MinSL 属性），在实现多级安全性范例时通常就是这种情况。为了简化过程并且使对网络资源的影响达到最低限度，仅当申请者的最小安全性级别低于该子网的最小安全性级别或者申请者的最大安全性级别高于该子网的最大安全性级别时，才应当从给定申请者向给定端口的 GID 注册器发送联接请求。

[0073] 图 7 是示出根据本发明的访问控制列表（ACL）700 的示例的框图。访问控制列表 700 包括多个条目（被称为访问控制列表条目或 ACE），这些条目在图 7 中被示为访问控制列表条目 710(1)–(N)。访问控制列表条目 710(1)–(N) 中的每一个包括流标记字段（示为流标记字段 720(1)–(N)）、安全性标记信息字段（示为安全性标记信息字段 730(1)–(N)）以及其他流规格字段（示为其他流规格字段 740(1)–(N)）。诸如被示为 ACL 700 的 ACL 那样的 ACL 可以用内容可寻址存储器（CAM）来实现，更具体地说，可以用三元 cam（TCAM）来实现，从而基于存储在安全性标记信息字段 730(1)–(N) 中的信息提供对安全性信息的快速高效查找。

[0074] 在根据本发明配置的网络设备中，诸如 ACL 700 这样的 ACL 被用于部分地基于分组的安全性级别以及在其上接收到分组的端口的安全性级别（或安全性级别范围）来识别要对给定分组执行的处理。端口的安全性级别被反映在访问控制列表条目 710(1)–(N) 中适用的那个条目中存储的安全性标记中，更具体而言，反映在在安全性标记信息字段 730(1)–(N) 中相应的那个字段中。ACE 应当适用的端口是通过识别适用的（一个或多个）ACE 的过程来识别的。

[0075] 将会意识到，可以采用流标记字段 740(1)–(N) 来将访问控制列表条目 710(1)–(N) 中的给定条目识别为支持根据本发明的安全性标记的 ACE（例如在并非所有 ACE 都支持这种确定的情况下）。或者，流标记字段可以被（至少部分地）用于帮助识别（一个或多个）端口，从而帮助识别 ACE 应当适用的流量。

[0076] 图 8 是示出本发明可在其中实现的网络体系结构 800 的示例的框图。在呈现为网络体系结构 800 的示例中, 网络 810 是互联网协议 (IP) 网络 (即, 例如, 其中设备利用第 3 层地址来转发分组的网络)。网络 810 耦合子网 820 和 830, 所述子网 820 和 830 分别经由路由器 840 和 850 访问网络 810。子网 820 和 830 是 IP 子网 (即, 例如, 其中设备利用第 2 层地址来转发分组的网络)。耦合到子网 820 的是交换机 850 和 855。交换机 850 将主机 860 和 861 耦合到子网 820, 并且还提供对认证服务器 865 的访问, 以便主机 860 和 861 的用户被认证。认证服务器 865 认证登录到主机 860 中 (或者更概括地说, 登录到网络体系结构 800 中) 的用户。以类似的方式, 交换机 855 向服务器 870 提供对子网 820 (以及网络体系结构 800 的其余部分) 的访问。以类似的方式, 交换机 880 和 885 提供对子网 830 的访问。主机 890 和 891 经由交换机 880 访问子网 830; 主机 890 和 891 的用户被认证服务器 892 所认证。正如之前那样, 认证服务器 892 帮助认证登录到主机 890 中的用户。同样正如之前那样, 交换机 885 还向服务器 895 提供对子网 830 的访问。

[0077] 在诸如网络体系结构 800 这样的网络中本发明的操作可以支持多种部署。例如, 主机 860、861、890 和 891 中每一个, 以及服务器 870 和 895, 都可以被设计为支持单个安全性级别 (对于该安全性级别可使用从 1 (最低安全性级别) 到 7 (最高安全性级别) 的范围)。在这种情况下, 主机 860、主机 861 和服务器 870 可能各自具有为 3 的安全性级别。给定这种部署, 主机 860 和 861 将会能够访问服务器 870 (即它们的分组不会被交换机 850 或 855 中的任何一个所丢弃)。从而路由器 840 和 845 以及交换机 850、855、880 和 885 根据本发明被配置为根据分组的安全性级别阻止或者允许分组通过。

[0078] 以类似的方式, 主机 890、主机 891 和服务器 895 可能各自具有为 5 的安全性级别。给定这种部署, 主机 890 和 891 将会能够访问服务器 895 (即它们的分组将不会被交换机 880 或 885 中的任何一个所丢弃)。此外, 主机 890 和 891 将会能够访问服务器 870 (给定它们各自的安全性级别), 因为由主机 890 和 891 所发起的分组不会被路由器 840 或 845 中任何一个 (或任何中间路由器) 或交换机 880 或 855 所丢弃。但是, 主机 860 和 861 将不能够访问服务器 895。主机 860 所发起的分组将会被交换机 885 (或者路由器 845, 这取决于实现方式) 阻止, 如前所述, 所述交换机 885 (路由器 845) 只允许交换机 885 (路由器 845) 所允许的最低安全性级别或以上的分组。

[0079] 或者, 在网络体系结构 800 中可以实现安全性标记范围。在这种情况下, 利用相同的安全性级别方案 (1-7) 和客户端安全性级别设置 (主机 860 的安全性级别为 2, 主机 861 的安全性级别为 3, 主机 890 的安全性级别为 4, 主机 891 的安全性级别为 5), 可以提出以下示例。在该示例中, 服务器 870 将会具有 1-3 的安全性级别范围, 而服务器 895 将会具有 3-5 的安全性级别范围。在这种情况下, 路由器 840 将会只允许具有 1-3 的安全性级别的分组进入子网 820, 而路由器 845 将只会允许具有 3-5 的安全性级别的分组进入子网 830。

[0080] 与之前一样, 主机 860 和 861 能够访问服务器 870, 因为它们的分组的安全性标记将不会导致其分组被交换机 855 所阻止。类似地, 主机 890 和 891 能够访问服务器 895, 因为它们的分组的安全性标记将不会导致其分组被交换机 885 所阻止。此外, 由主机 861 所发起的具有反映安全性级别 3 的安全性标记的分组能够访问服务器 895, 因为这些分组不会被路由器 845 丢弃。但是, 由主机 860 所发起的具有反映安全性级别 2 的安全性标记的分组不能够访问服务器 895, 因为这些分组将会因为具有对于给定子网 (即子网 830) 来说

不充分的安全性级别而被路由器 845 丢弃。

[0081] 用于安全性标记及其使用的示例性过程

[0082] 图 9 是示出认证操作的示例的流程图，在该认证操作中用户在主机（例如主机 110 或 111）上登录到网络中。该过程开始于主机发起认证过程（步骤 900）。接下来，从适当的认证服务器发出询问，以询问用户的用户名和口令（步骤 910）。响应于该询问，用户提供其用户名和口令（步骤 920）。然后确定认证服务器是否能够认证用户（步骤 930）。如果用户不能被认证，则确定是否允许用户重新输入其用户名和密码（步骤 940）。如果重新输入此信息是可接受的，则过程循环回认证服务器询问用户的点（步骤 910）。否则（例如，如果已经最大次数地允许了重新输入，或者不允许重新输入），则过程结束。

[0083] 或者，如果用户被认证（步骤 930），则用户被允许登录，这是通过认证服务器向交换机转发访问接受而完成的（步骤 950）。典型情况下，随后通过从交换机向主机发送通知来向用户发送通知，这主要是为了向用户指示接受。然后确定该用户将会使用的端口（例如主机被附接到的端口）是否被指定为安全性访问端口（步骤 960）。如果该端口未被指定为安全性访问端口，则用户登录过程完成。但是，如果该端口被指定为安全性访问端口，则认证服务器将指派给端口的适当安全性级别通知给网络设备（例如主机耦合到的交换机或路由器）。然后在给定访问该端口的其他用户和现有安全性信息的情况下，网络设备适当地指派该安全性级别，正如联系图 4 和 5 和这里的其他地方所描述的那样。这完成了用户登录过程。

[0084] 如前所述，图 9 示出了图示根据本发明实施例的过程的流程图。意识到这里所论述的操作可以包括由计算机系统用户或由专用硬件模块执行的步骤直接输入的命令，但是优选实施例包括由软件模块执行的步骤。这里所提到的步骤的功能可以对应于模块或模块的某些部分的功能。

[0085] 这里所提到的操作可以是模块或模块的某些部分（例如软件、固件或硬件模块）。例如，虽然所描述的实施例包括软件模块和 / 或包括手动输入的用户命令，但是各种示例性模块也可以是专用硬件模块。这里所论述的软件模块可以包括脚本、批处理或其他可执行文件，或者这种文件的组合和 / 或某些部分。软件模块可以包括编码在计算机可读介质上的计算机程序或其子例程。

[0086] 此外，本领域的技术人员将会认识到，模块之间的界线只是说明性的，其他实施例可以合并模块或对模块的功能施加其他分解。例如，这里所论述的模块可以被分解成将会作为多个计算机进程并且（可选地）在多个计算机上执行的子模块。此外，其他实施例可以组合特定模块或子模块的多个实例。此外，本领域的技术人员将会认识到，示例性实施例中所描述的操作只是用于说明。根据本发明，操作可以被组合，或者操作的功能可以被分布在另外的操作中。

[0087] 或者，这种动作可以体现在实现这种功能的电路结构中，例如复杂指令集计算机（CISC）的微代码、编程到可编程或可擦除 / 可编程设备中的固件、现场可编程门阵列（FPGA）的配置、门阵列或完全定制的专用集成电路（ASIC）的设计，等等。

[0088] 流程图的每个块可以由模块（例如软件模块）或者模块的一部分或者计算机系统用户来执行。从而，上述方法、其操作以及其模块可以在被配置为执行该方法的操作的计算机系统上执行，并且 / 或者可以从计算机可读介质执行。该方法可以被体现在用于配置计

算机系统以执行该方法的机器可读和 / 或计算机可读介质中。从而，软件模块可以被存储在计算机系统存储器内和 / 或被传输到计算机系统存储器，以便配置计算机系统以执行模块的功能。

[0089] 这种计算机系统通常根据程序（内部存储的指令的列表，例如特定应用程序和 / 或操作系统）来处理信息，并且经由 I/O 设备产生所生成的输出信息。计算机进程一般包括执行（运行）程序或程序的一部分，当前程序值和状态信息，以及被操作系统用于管理进程的执行的资源。父进程可以繁殖其他子进程，以帮助执行父进程的整体功能。由于父进程具体地繁殖子进程来执行父进程的整体功能的一部分，因此子进程（以及孙子进程等）所执行的功能有时可被描述为是由父进程执行的。

[0090] 这种计算机系统一般包括“同时”执行的多个计算机进程。通常，计算机系统包括能够交替地支持多个活动进程的单个处理单元。虽然多个进程可能看起来是同时执行的，但是在任何给定时刻实际上只有一个进程被单个处理单元所执行。通过迅速地改变进程执行，计算机系统给出了同时进程执行的外观。计算机系统在各执行阶段在多个进程之间对计算机系统的资源进行多路复用的能力被称为多任务处理 (multitasking)。按照其定义，能够支持真正的同时处理的具有多个处理单元的系统被称为多处理系统。当活动进程被在多任务处理和 / 或多处理环境中执行时，这些进程常被称为是同时执行的。

[0091] 这里所描述的软件模块可以被这种计算机系统例如从计算机可读介质接收。计算机可读介质可以被永久性地、可移除地或远程地耦合到计算机系统。计算机可读介质例如可以不排他地包括以下介质中的任意多个介质：磁存储介质，其中包括磁盘存储介质和磁带存储介质；光存储介质，例如紧致盘介质（例如 CD-ROM、CD-R 等）以及数字视频盘存储介质；非易失性存储器存储存储器，其中包括基于半导体的存储单元，例如 FLASH 存储器、EEPROM、EPROM、ROM 或专用集成电路；易失性存储介质，其中包括寄存器、缓冲器或缓存、主存储器、RAM 等等；以及数据传输介质，其中包括计算机网络、点对点电信和载波传输介质。在基于 UNIX 的实施例中，软件模块可以被体现在一个文件中，该文件可以是设备、终端、本地或远程文件、套接字、网络连接、信号或者通信或状态变化的其他手段。其他新的和各种类型的计算机可读介质可以被用于存储和 / 或传输这里所论述的软件模块。

[0092] 图 10 是示出根据本发明实施例的网络中的分组标记的示例的流程图。给定网络设备处的分组标记过程开始于在网络设备处接收该分组（步骤 1000）。接收到该分组后，网络设备就确定是否向这样接收到的分组应用安全性策略（步骤 1010）。如果该确定指示安全性策略将不被应用到该分组（例如在未被标记的分组在入口路由器处被接收到的情况下），则就只是将适当的标记写到分组中（步骤 1020），并且将分组转发到适当的端口（步骤 1030）。但是，如果要将安全性策略应用到该分组（步骤 1010），则利用适用的策略处理该分组（步骤 1040）。这种安全性策略的应用联系图 11 来更详细描述。

[0093] 接下来，确定分组是否成功通过了所执行的安全性策略处理（步骤 1050）。如果分组未通过此处理，则分组被丢弃（步骤 1060），并且丢弃分组计数器被增大（步骤 1070）。但是，如果分组成功地通过了此安全性处理，则适当的标记被写到分组中（步骤 1020），并且分组被转发到适当的端口（步骤 1030）。正如别处所述，预期安全性访问端口上的带安全标记的分组以及在安全性干线端口上接收到的未被标记的分组被丢弃，因为未预期它们会出现在这种地方。

[0094] 图 11 是示出当以根据本发明实施例的方式应用安全性策略时对分组执行的处理的示例的流程图（例如就图 10 的步骤 1040 所推断的）。过程开始于分组被实现本发明的分组处理单元接收（步骤 1100）。确定负责生成分组的用户的安全性级别（步骤 1110）。接下来，确定该分组（以及该用户）的安全性级别是否在分组在其上被接收到的端口的安全性级别范围之内（步骤 1120）。如果分组的安全性级别不在端口的安全性级别范围内，则分组处理单元指示分组未成功通过安全性策略处理，因此分组应当被丢弃（步骤 1130）。

[0095] 但是，如果分组的安全性级别在端口的安全性级别范围内，则确定分组的安全性级别是否允许在网络设备内将分组直接转发到其指定的外出端口（步骤 1140）。如果分组的安全性级别指示分组应当被直接转发，则分组在网络设备内被转发到其指定的外出端口，以便转发到其计划路径上的下一个网络设备（步骤 1150）。但是，如果分组的安全性级别不允许直接转发，则确定分组的安全性级别是否指示可改为经由防火墙转发分组（步骤 1160）。将会意识到，实际上，可以使分组的转向由于任意多个原因而发生，并且在这种转向时可以采取任意多个动作（或执行处理）。如果分组的安全性级别指示经由防火墙转发是不可接受的，则分组处理单元指示分组应当被丢弃（步骤 1130）。如果分组的安全性级别指示允许经由防火墙转发，则分组处理单元将分组转发到防火墙以便进一步处理（步骤 1170）。

[0096] 图 12A 是示出根据本发明实施例的网络中的交换机处的分组接收、标记和转发的示例的流程图。过程开始于在交换机处接收到分组（步骤 1200）。然后利用第 2 层安全性协议标记分组（步骤 1210）。一旦被标记，分组就被沿其计划路径转发（步骤 1220）。在其中执行这种安全性标记的子网中，安全性干线端口执行前述分析，从而允许利用根据本发明的方法来保护子网。

[0097] 图 12B 是示出根据本发明实施例的网络中的入口路由器处的分组接收、标记和转发的示例的流程图。过程开始于在路由器处接收到分组（步骤 1250）。然后利用第三层安全性协议标记分组（步骤 1260）。一旦被标记，分组就被沿其计划路径转发（步骤 1270）。如前所述，这种标记允许了要在核心（例如 IP）网络内执行的分组分析和控制，从而提供了先前所述的益处。

[0098] 图 13 是示出根据本发明实施例的网络中的出口路由器处的分组接收、标记和转发的示例的流程图。过程开始于在出口路由器处接收到分组（步骤 1300）。然后确定该分组上是否存在网络安全性信息，以及该信息是否需要被从分组上剥除（步骤 1310）。如果分组包括网络 3 安全性信息，则该安全性信息被从分组上剥除（步骤 1320）。

[0099] 否则（或者在已经从分组上剥除网络信息之后），确定网络安全性信息是否指示应当添加子网安全性信息（步骤 1330）。如果网络安全性信息指示应当添加子网安全性信息，则路由器利用适当的子网安全性协议来标记分组（按照该协议向分组添加安全性信息）（步骤 1340）。否则（或者在添加子网安全性信息之后），分组被沿其计划路径转发（步骤 1350）。

[0100] 图 14 是示出根据本发明实施例的网络中的分组认证的示例的流程图。过程开始于在首先接收到分组的网络设备（例如入口路由器）处接收到分组（步骤 1400）。接下来，根据适当的安全性策略标记分组（步骤 1410）。然后被标记的分组被沿其计划路径转发（步骤 1420）。在沿着被标记的分组的计划路径的一个或多个网络设备处，按以下方式认证分

组。首先，在将会认证分组的网络设备处接收到分组（步骤 1430）。接下来，该网络设备认证被标记的分组（步骤 1440）。然后确定是否已在该分组的目的地处接收到了该分组（步骤 1450）。如果当前网络设备是分组的计划目的地，则认证过程完成。但是，如果当前网络设备不是计划目的地，则分组被沿其计划路径转发（步骤 1460）。

[0101] 虽然已经示出和描述了本发明的特定实施例，但是对于本领域的技术人员很明显的是，基于这里的教导，可以在不脱离本发明及其更宽的方面的情况下做出改变和修改，因此所附权利要求将会把所有这种处于本发明的真正精神和范围内的改变和修改包含在其范围内。此外，虽然已参考这些特定实施例具体地示出和描述了本发明，但是本领域的技术人员将会理解，可在其中做出前述和其他形式和细节上的改变，而不会脱离本发明的精神或范围。

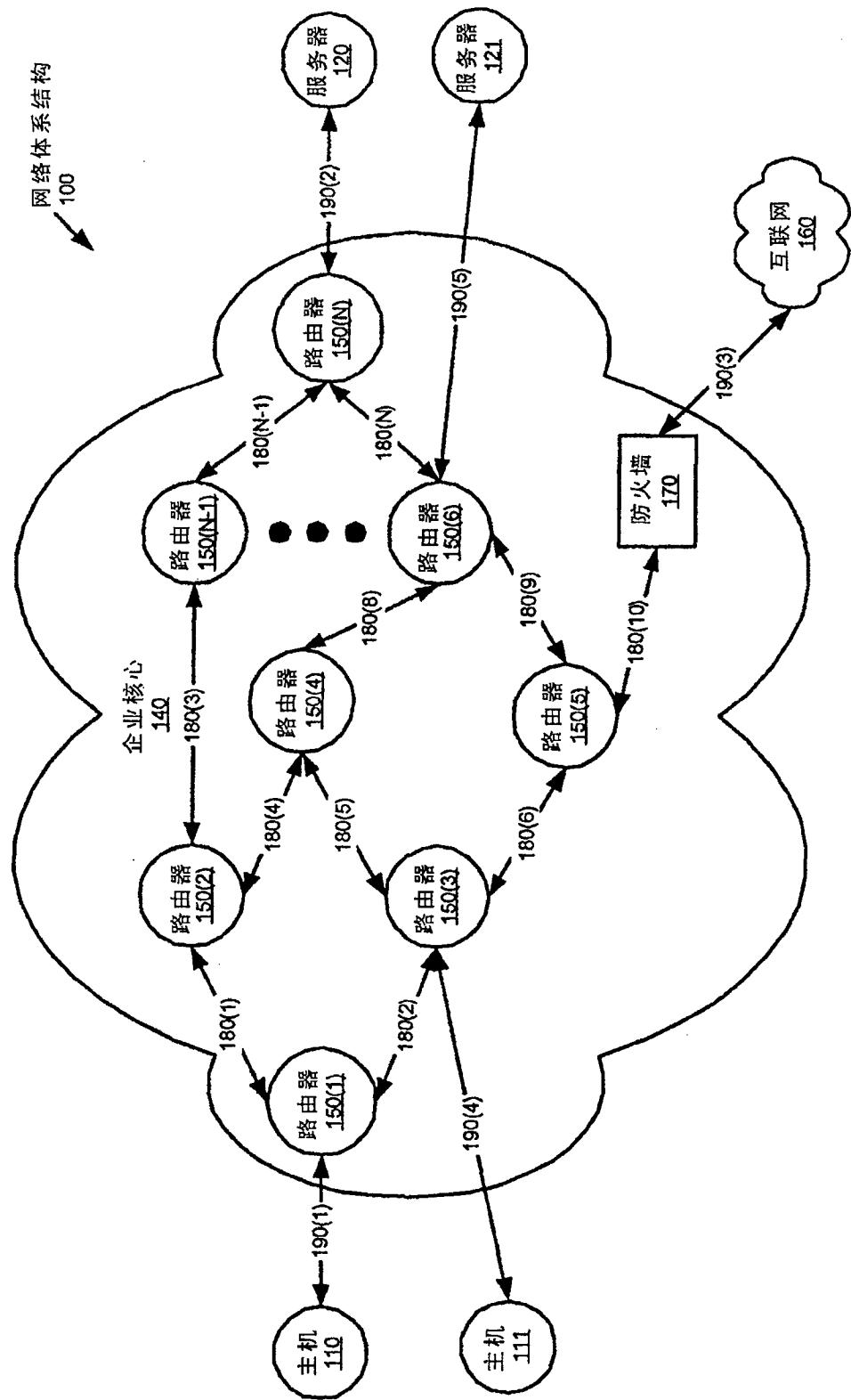


图 1

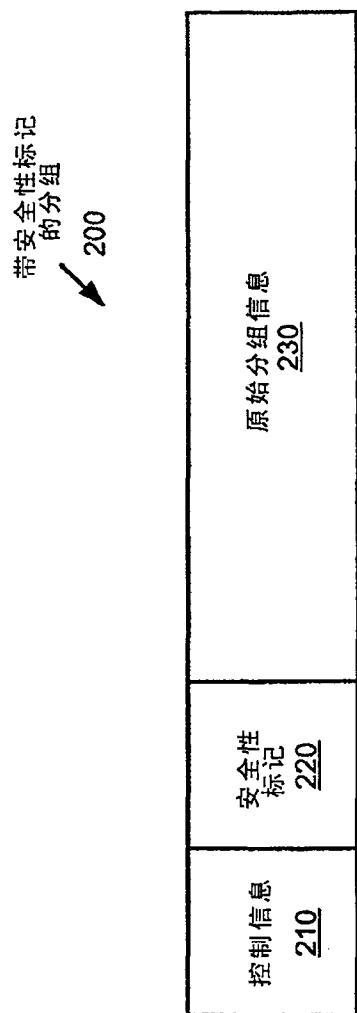


图 2

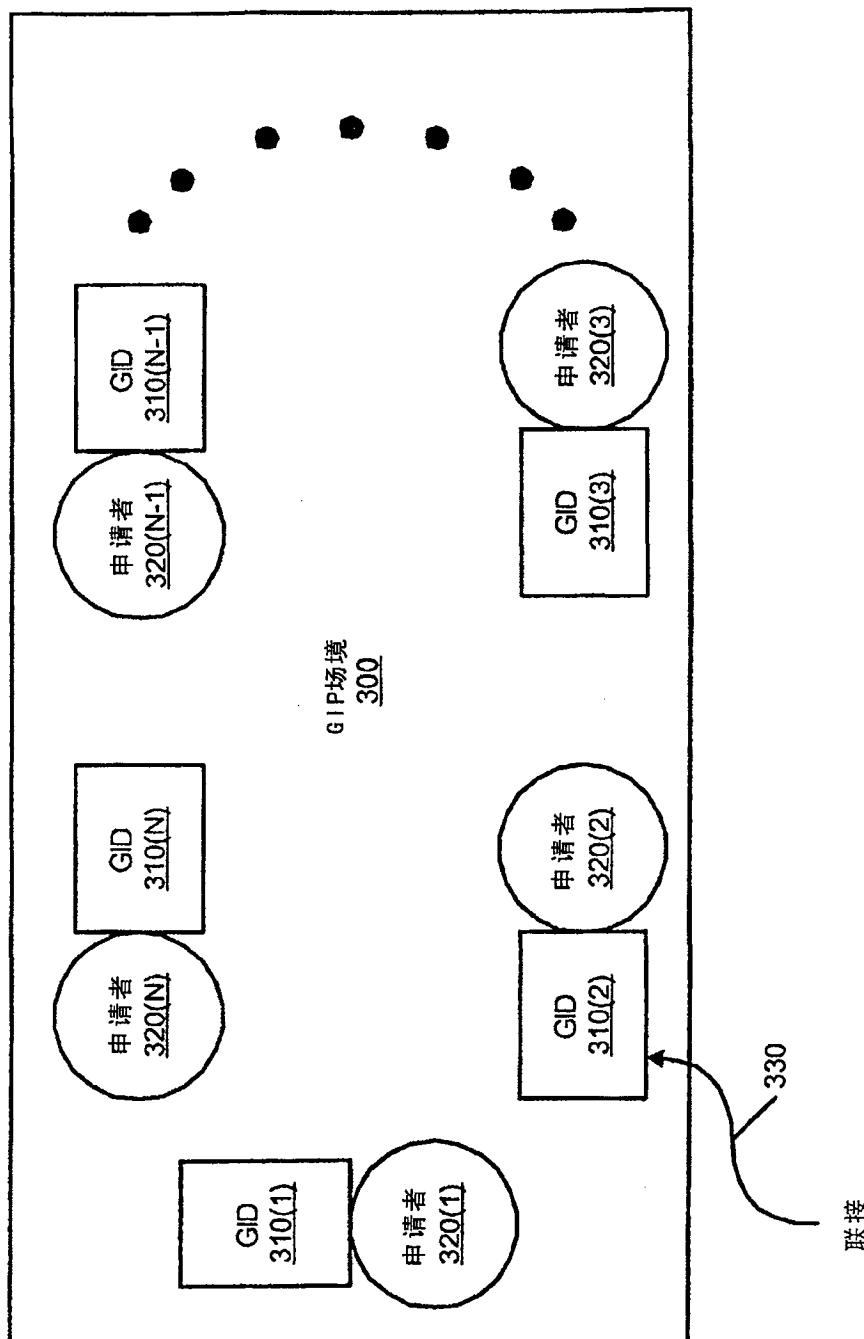


图 3

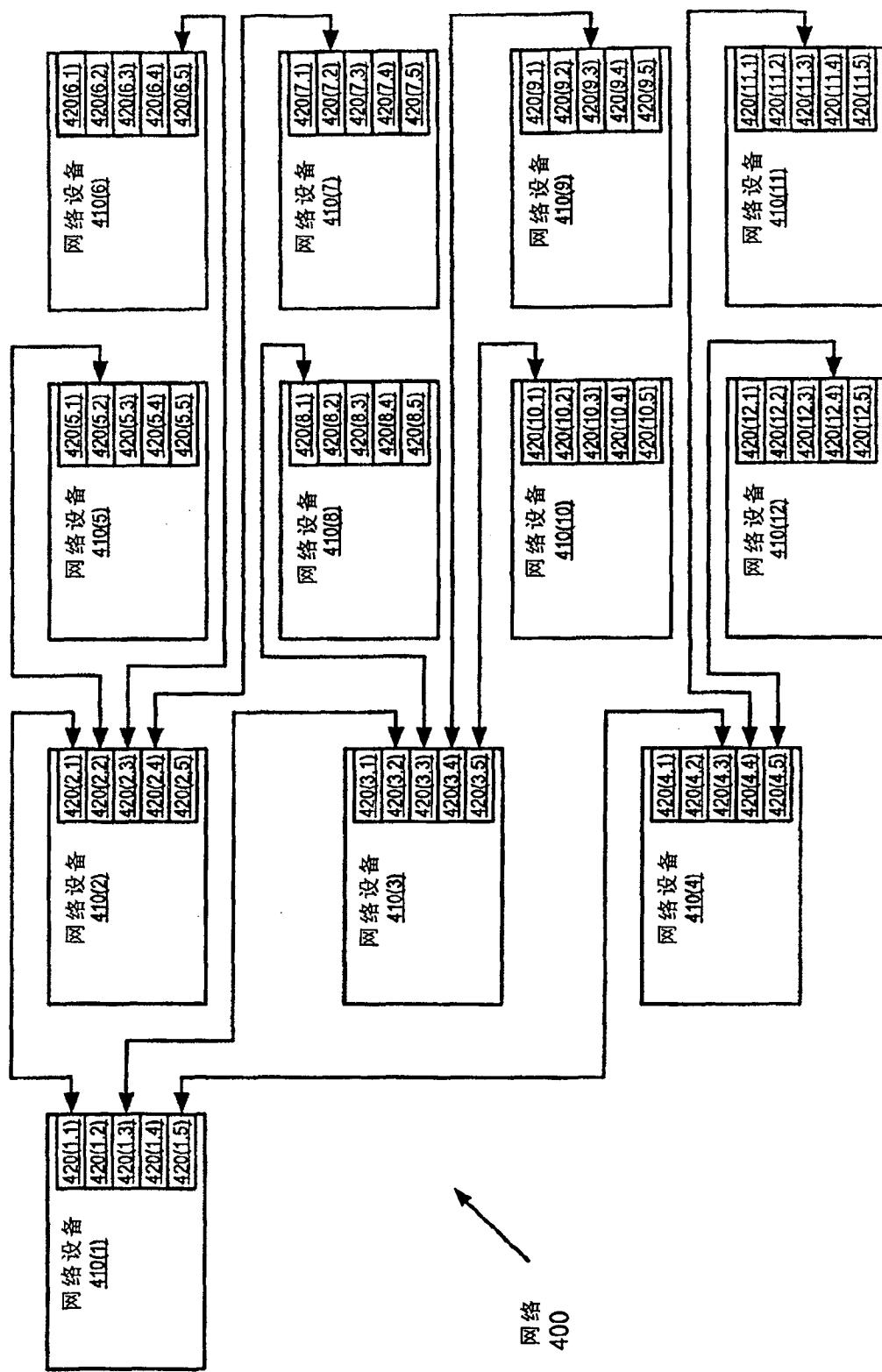


图 4

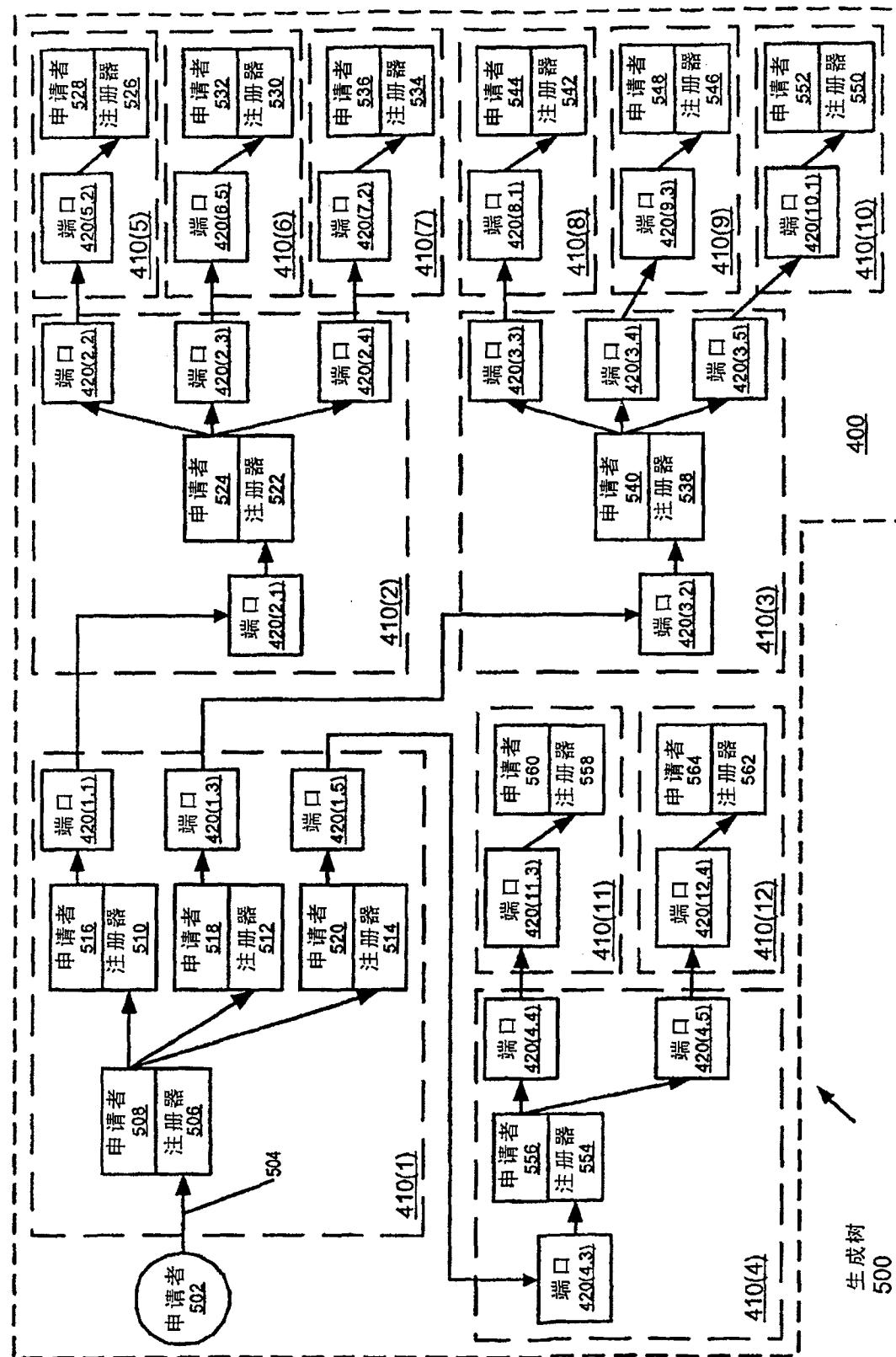


图 5

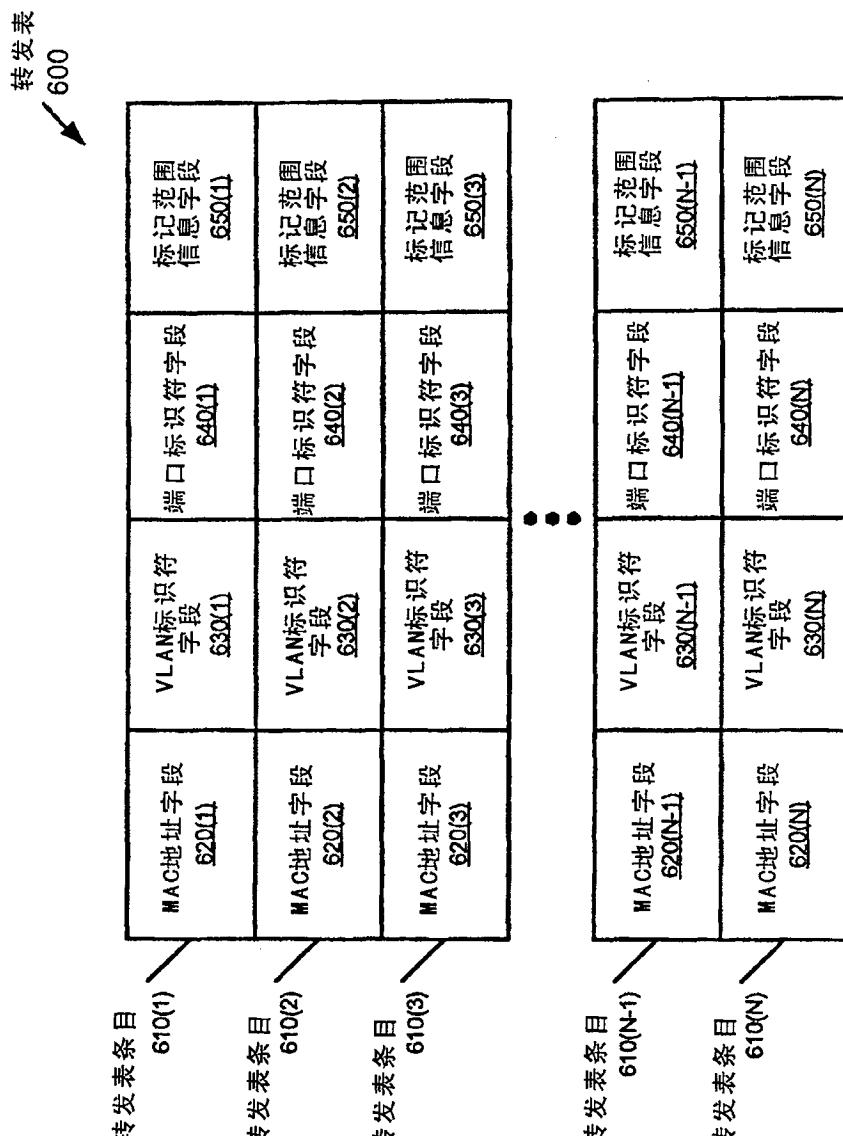
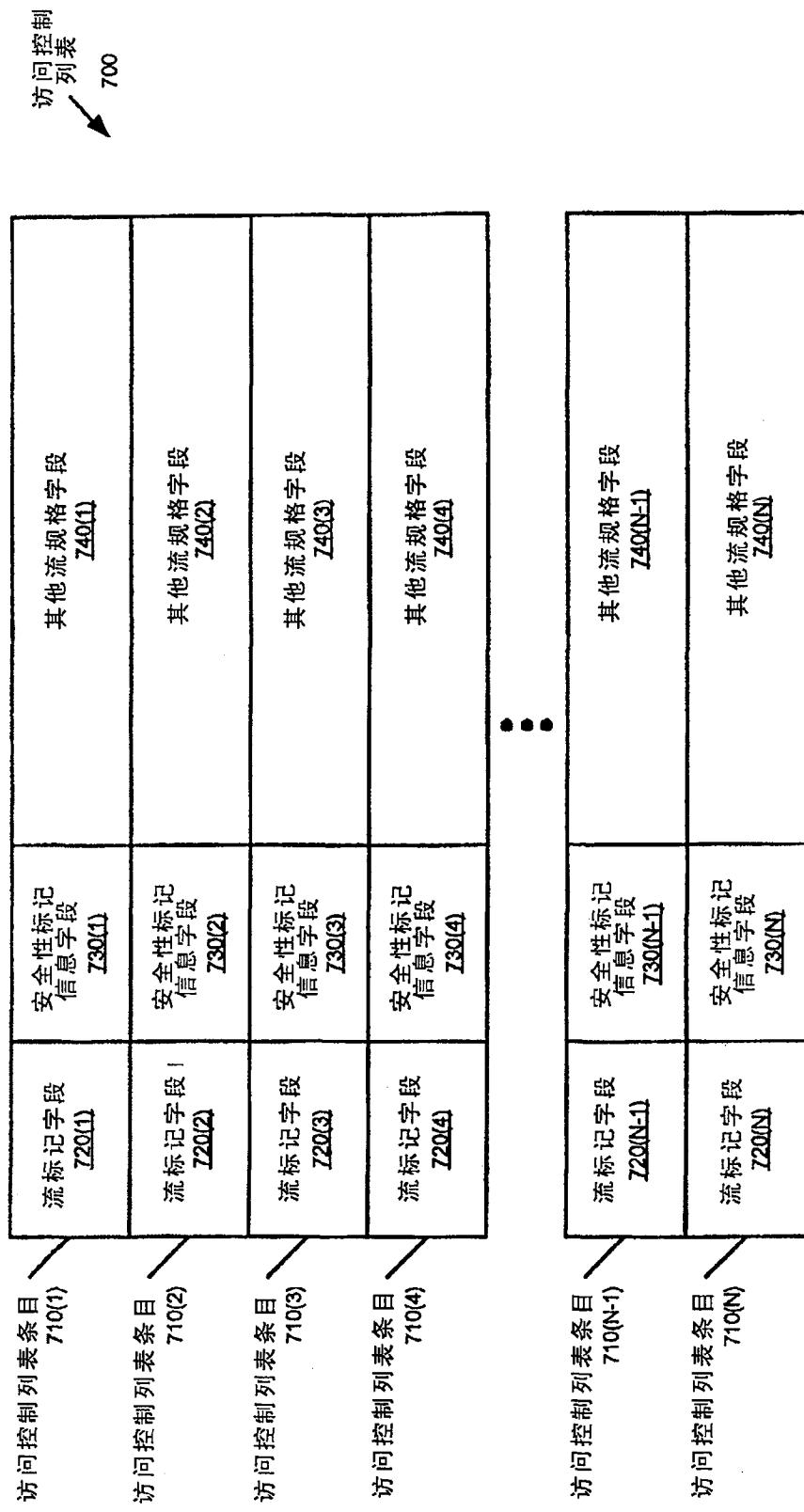


图 6



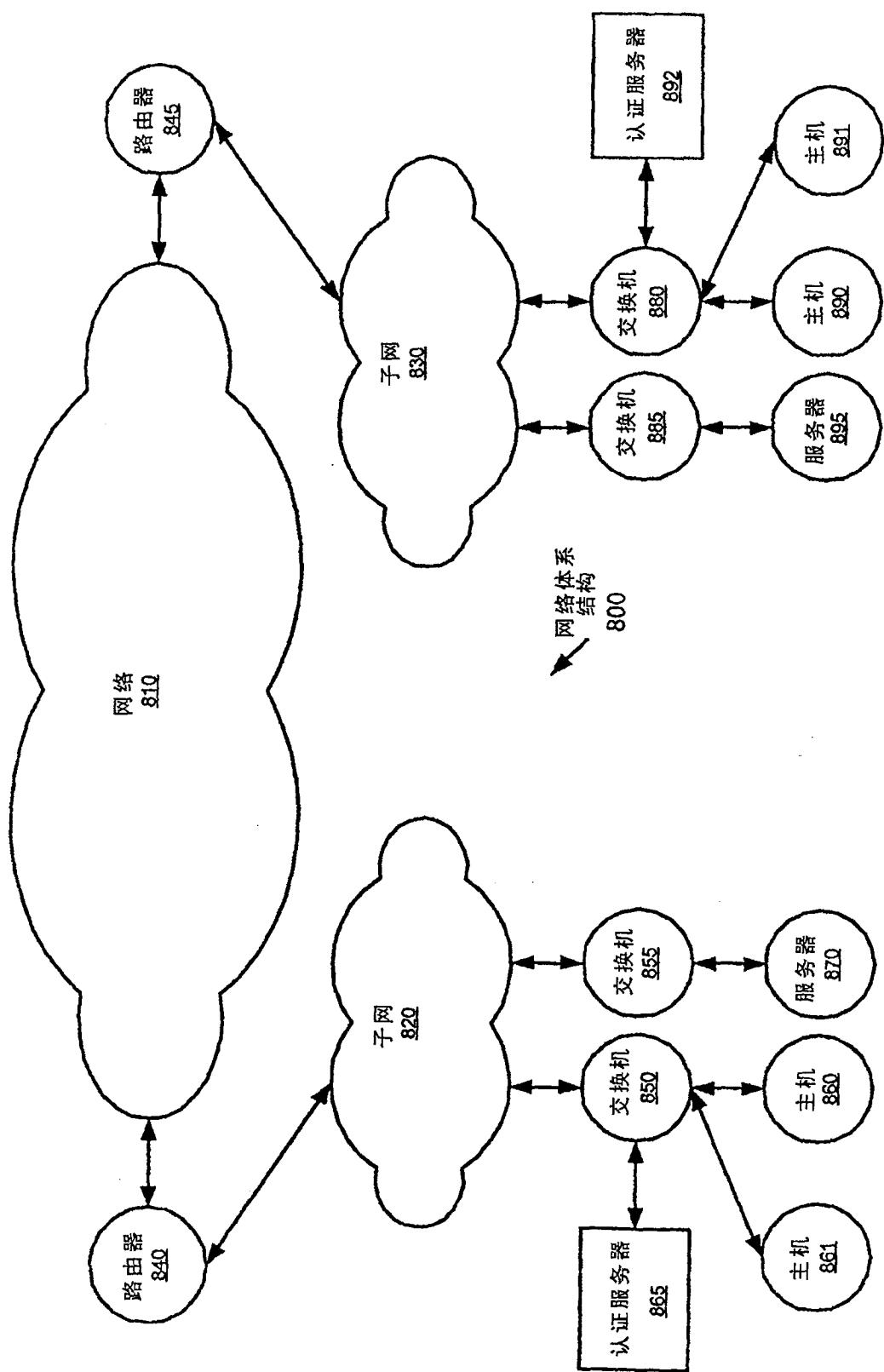


图 8

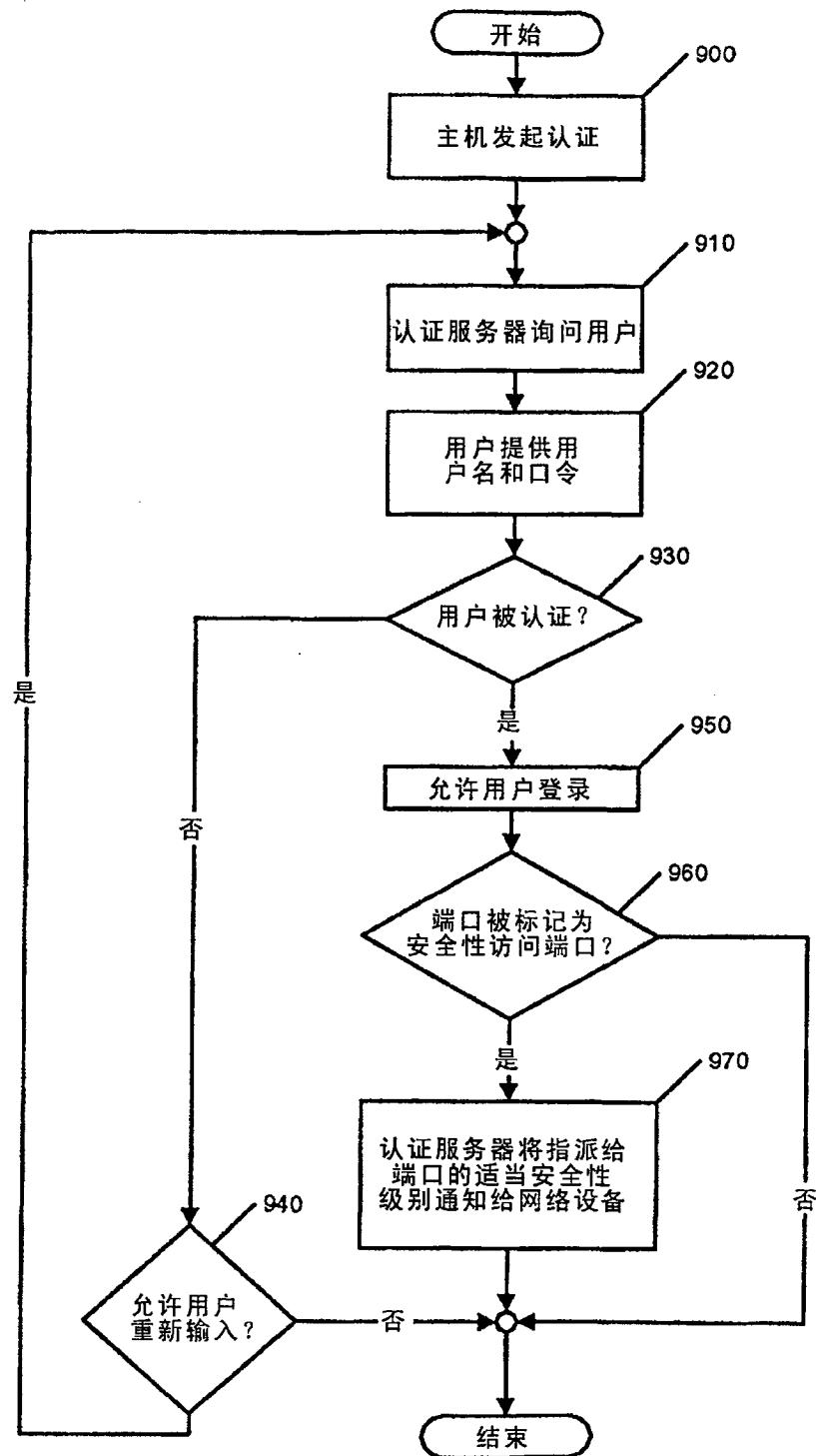


图 9

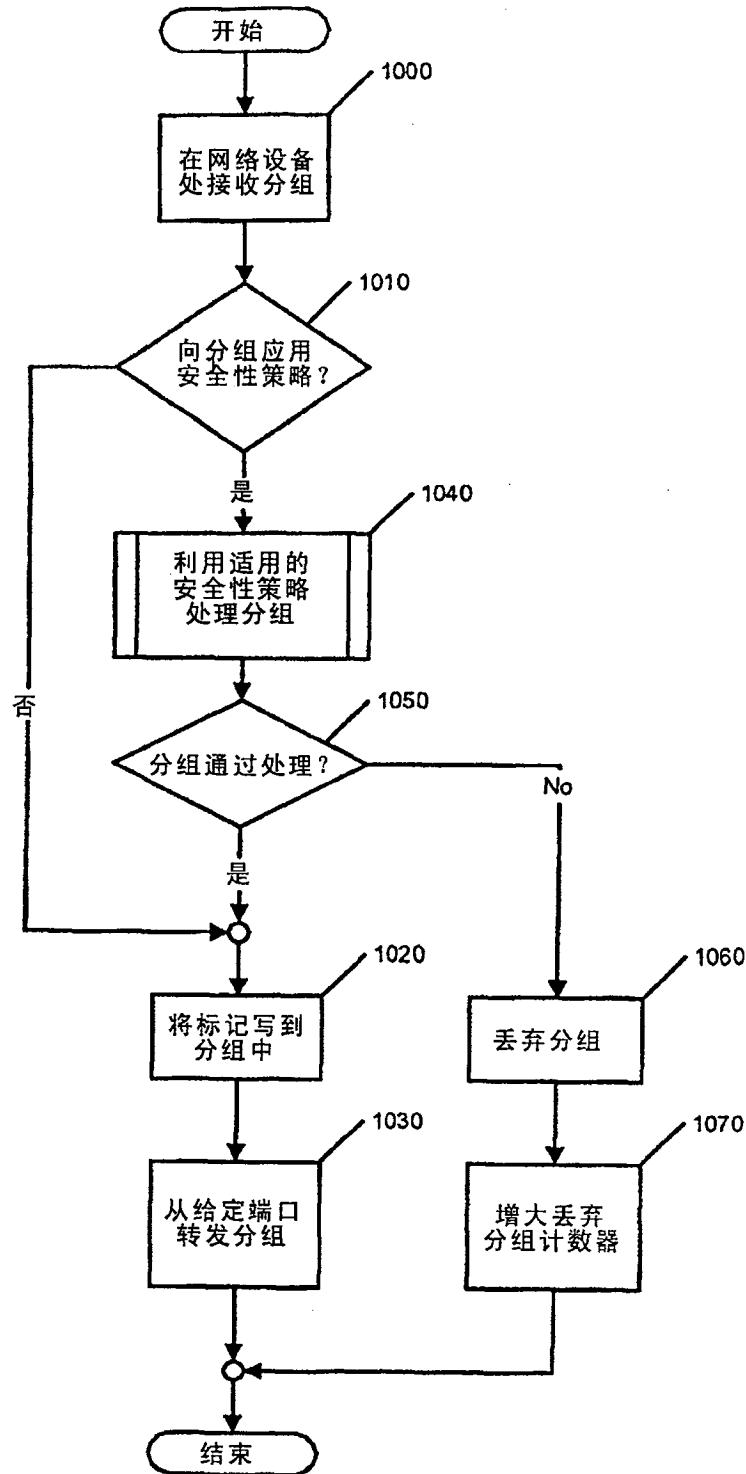


图 10

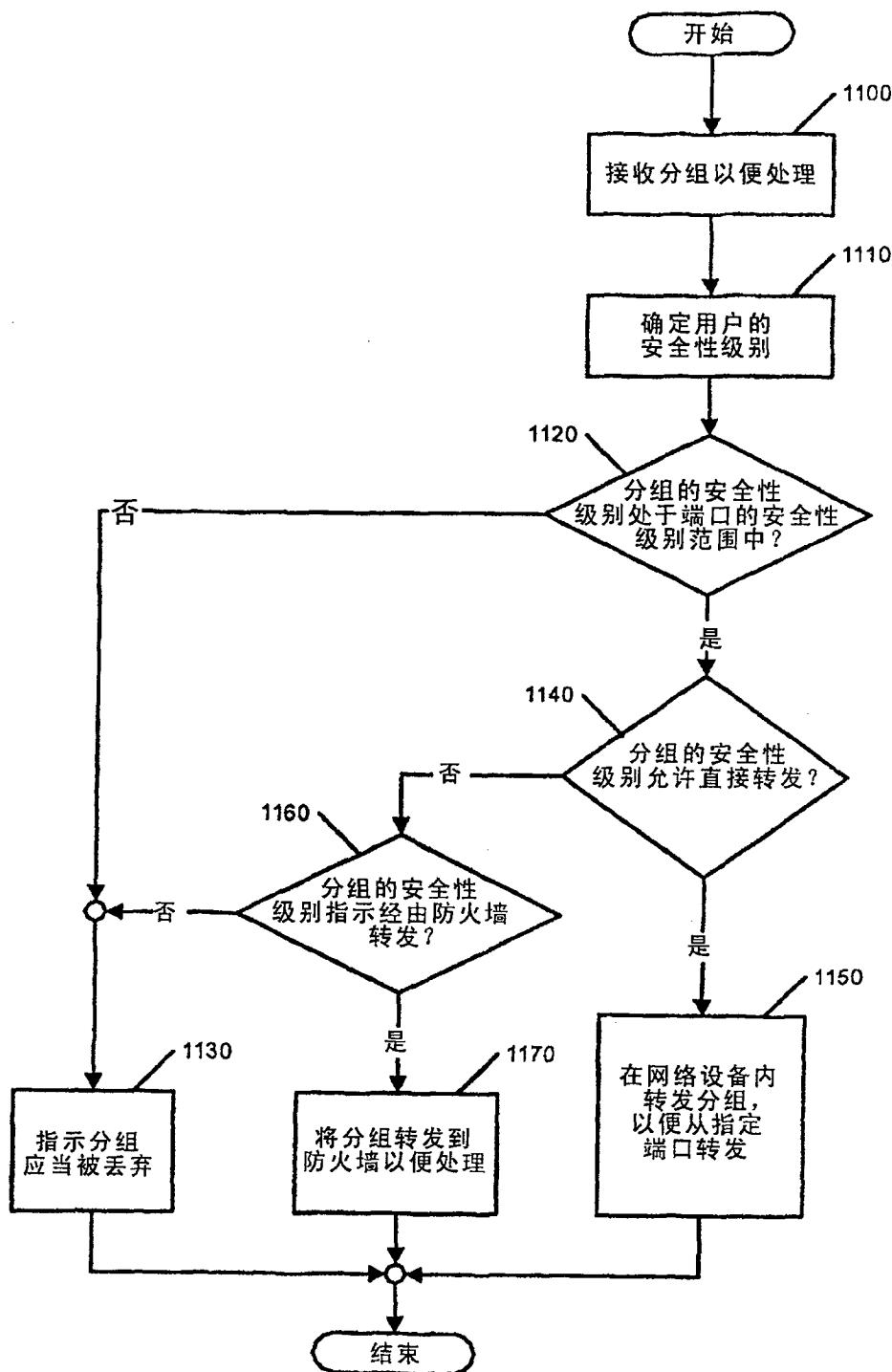


图 11

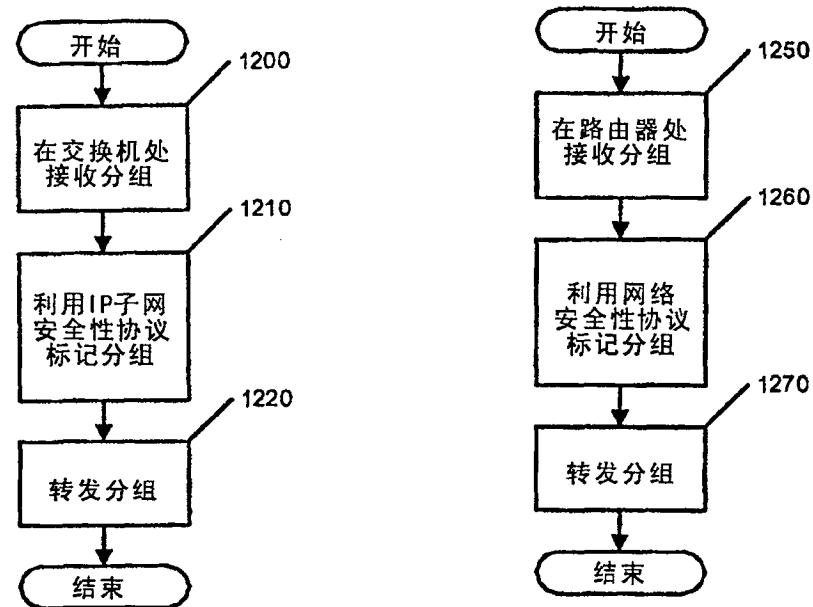


图 12A

图 12B

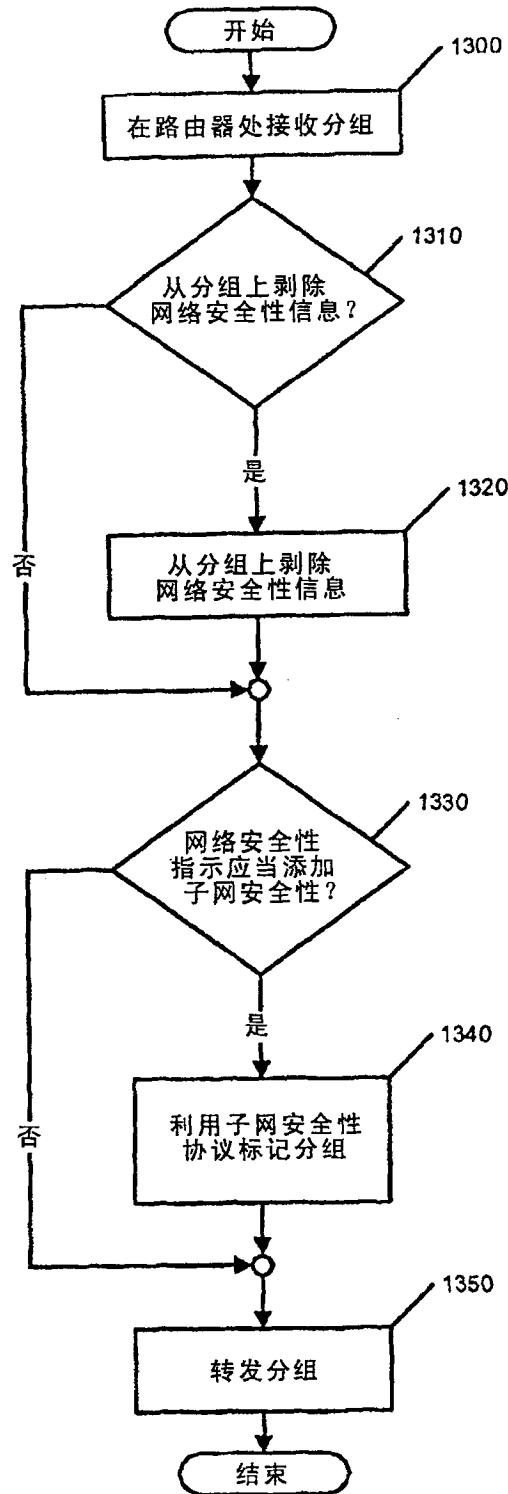


图 13

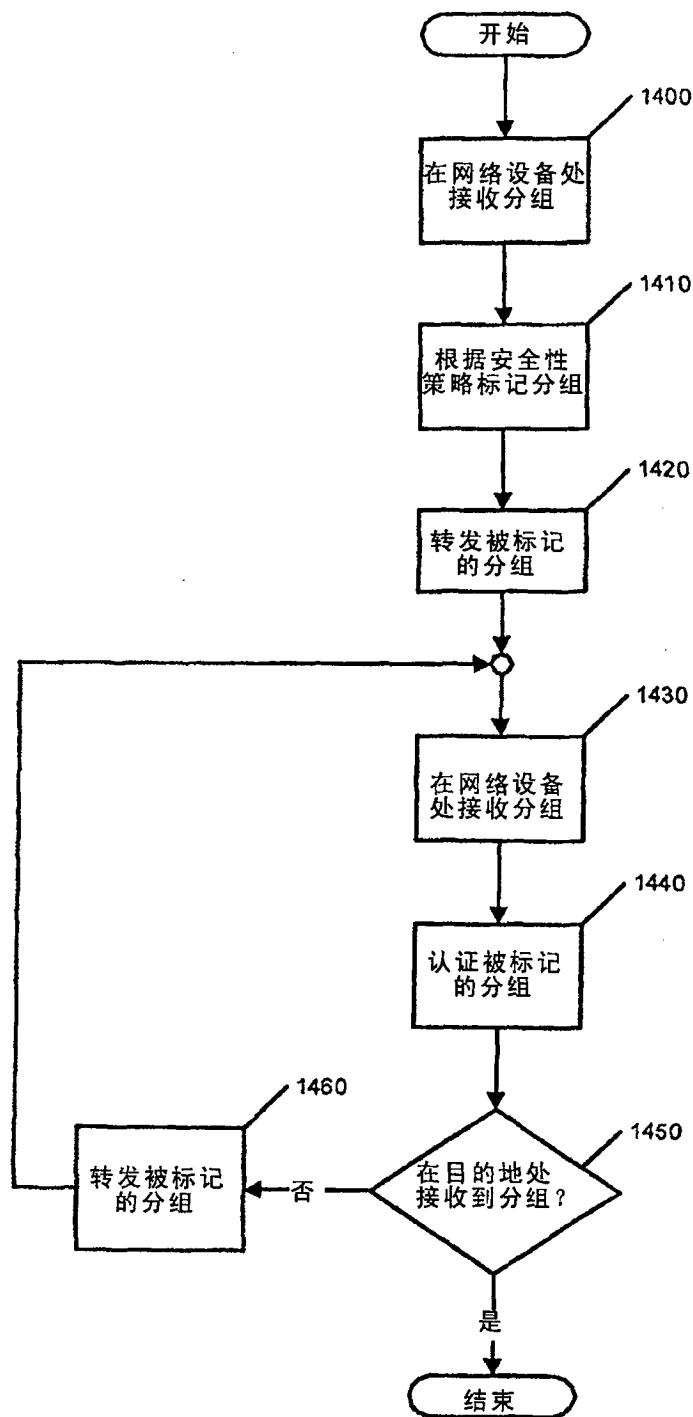


图 14