



[12] 发明专利申请公开说明书

[21] 申请号 03805843.X

[43] 公开日 2005 年 7 月 20 日

[11] 公开号 CN 1643947A

[22] 申请日 2003.3.19 [21] 申请号 03805843.X

[30] 优先权

[32] 2002.3.20 [33] US [31] 10/101,641

[86] 国际申请 PCT/US2003/008800 2003.3.19

[87] 国际公布 WO2003/090041 英 2003.10.30

[85] 进入国家阶段日期 2004.9.13

[71] 申请人 UT 斯达康有限公司

地址 美国加利福尼亚州

[72] 发明人 萨蒂什·阿玛拉 默德维·维尔马

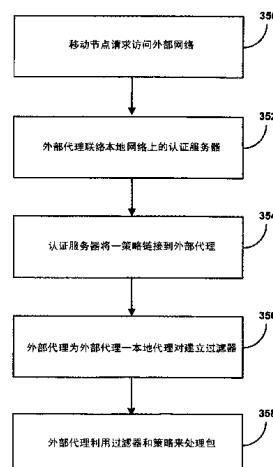
[74] 专利代理机构 隆天国际知识产权代理有限公司
代理人 郑特强 经志强

权利要求书 4 页 说明书 18 页 附图 7 页

[54] 发明名称 用于提供动态互联网协议安全策略服务的方法

[57] 摘要

移动节点可从它的本地网络漫游到外部网络。移动节点可利用移动互联网协议进行通信，并且可利用互联网协议安全以与它的本地网络通信。外部网络上的外部代理和本地网络上的本地代理可动态地链接在外部代理与本地代理之间的互联网协议安全会话所用的策略。外部代理和本地代理可动态地建立互联网协议安全会话所用的过滤器。



1. 一种用于动态提供互联网协议安全策略服务的方法，包括步骤：
接收从一移动节点发送到一外部代理的一连接请求，其中该移动节点使
5 用移动互联网协议；
获取至少一个用于该移动节点的策略模板，其中该至少一个策略模板包括处理信息，用于在该外部代理与该移动节点的一本地代理之间发送的互联网协议安全包；
与该本地代理协商互联网协议安全参数；以及
10 建立至少一个过滤器，其中该至少一个过滤器识别在该本地代理与该外部代理之间传送的数据包，以接收互联网协议安全处理，并且其中该至少一个过滤器识别该至少一个策略模板，以应用于接收互联网协议安全处理的所述数据包。
2. 如权利要求 1 所述的方法，还包括一计算机可读介质，在该介质中
15 存储有用于使得一处理器执行该方法的所述步骤的指令。
3. 如权利要求 1 所述的方法，还包括步骤：将该至少一个过滤器存储于一过滤器列表中，其中该外部代理维护该过滤器列表。
4. 如权利要求 3 所述的方法，还包括步骤：
终止与该移动节点的连接；以及
20 从该外部代理过滤器列表中去除该至少一个过滤器。
5. 如权利要求 1 所述的方法，其中，利用互联网密钥交换，协商所述安全参数。
6. 如权利要求 1 所述的方法，其中，利用互联网安全关联和密钥管理协议，协商所述安全参数。
- 25 7. 如权利要求 1 所述的方法，其中，该至少一个策略模板指明加密的类型。
8. 如权利要求 1 所述的方法，其中，该至少一个策略模板指明一密钥的使用期限。
9. 如权利要求 1 所述的方法，其中，该至少一个策略模板指明用于协
30 商互联网协议安全服务类型的至少一个规则。

10. 如权利要求 1 所述的方法，其中该至少一个过滤器包括一第一过滤器和一第二过滤器；以及

其中该第一过滤器包括用于指明互联网安全关联与密钥管理协议包的端点的参数，并且其中该第二过滤器包括指明需要互联网协议安全服务的包的参数。

11. 如权利要求 1 所述的方法，其中该至少一个策略模板包括用于网络地址转换/端口地址转换应用的信息。

12. 如权利要求 1 所述的方法，其中该至少一个策略包括用于一防火墙应用的信息。

10 13. 如权利要求 1 所述的方法，其中该至少一个策略包括多个策略。

14. 如权利要求 1 所述的方法，其中该至少一个过滤器包括多个过滤器。

15. 一种用于向一移动节点动态提供策略服务的方法，包括步骤：

接收从一外部网络上的一外部代理发送到一本地网络上的一本地代理的一认证请求，其中该认证请求指示从该本地网络漫游到该外部网络的一移动节点，并且其中该移动节点使用移动互联网协议；

判定该移动节点是否需要互联网协议安全，该互联网协议安全用于在该外部代理与该本地代理之间发送的包；

向该外部代理告知该移动节点需要互联网协议安全，用于在该本地代理与该外部代理之间发送的数据包；以及

20 将用于该移动节点的至少一个安全策略模板链接到该本地代理，其中该安全策略模板指明在该外部代理与该本地代理之间的互联网协议安全通信中所用的参数。

16. 如权利要求 15 所述的方法，还包括一计算机可读介质，在该介质中存储有用于使得一处理器执行该方法的所述步骤的指令。

25 17. 如权利要求 15 所述的方法，还包括步骤：

建立一过滤器，其中该过滤器识别在该本地代理和该外部代理之间传送的包，以接收互联网协议安全处理，并且其中该过滤器识别该策略模板，以应用于接收互联网协议安全处理的所述包；以及

将该过滤器存储于一本地代理过滤器列表中。

30 18. 如权利要求 15 所述的方法，还包括步骤：

与该外部代理协商互联网协议安全参数。

19. 如权利要求 18 所述的方法，其中，利用互联网密钥交换，协商所述互联网协议安全参数。

5 20. 如权利要求 18 所述的方法，其中，利用互联网安全关联和密钥管
理协议，协商所述互联网协议安全参数。

21. 如权利要求 18 所述的方法，其中利用 OAKLEY 协议，协商所述互
联网协议安全参数。

22. 如权利要求 17 所述的方法，还包括步骤：

确定该移动节点已漫游离开该外部网络；以及

10 将该过滤器从该本地代理过滤器列表中去除。

23. 如权利要求 17 所述的方法，其中判定该移动节点是否需要互联网
协议安全的步骤还包括访问一认证、授权与记帐服务器。

24. 一种用于在一互联网协议安全应用中提供策略服务的方法，包括步
骤：

15 从漫游到一外部网络的一移动节点接收一请求，以建立到达一本地网络
的安全连接，其中该移动节点使用移动互联网协议；

向该本地网络认证该移动节点；

接收一指示，以将互联网协议安全用于在该本地网络上的一本地代理与
该外部网络上的一外部代理之间发送的包；

20 将用于该移动节点的一策略链接到该外部代理，其中该策略标识在该外
部代理与该本地代理之间发送的互联网协议安全包所用的处理信息；

与一本地代理协商互联网协议安全参数，以在该外部代理与该本地代理
之间建立一虚拟隧道；

建立一用于该移动节点的过滤器，其中该过滤器能够用于识别利用互联
网协议安全的、在该外部代理与该本地代理之间传送的包；以及

25 将该过滤器存储于一过滤器列表中。

26. 如权利要求 24 所述的方法，还包括一计算机可读介质，在该介质
中存储有用于使得一处理器执行该方法的所述步骤的指令。

26. 如权利要求 24 所述的方法，还包括步骤：

30 接收一包；

搜索该过滤器列表，以判定是否将互联网协议安全处理应用于该包；以及

至少部分地基于该策略中含有的信息，处理该包。

27. 如权利要求 24 所述的方法，还包括步骤：

5 确定该移动节点已漫游离开该外部网络；以及
将该过滤器从该过滤器列表中去除。

28. 如权利要求 24 所述的方法，其中该策略标识在经过该虚拟隧道发送包中所用的互联网协议安全加密的类型。

10 29. 如权利要求 24 所述的方法，其中该策略指明在经过该虚拟隧道发送包中所用密钥的使用期限。

30. 如权利要求 24 所述的方法，其中该策略指明解释规则的域，该解释规则用于协商经该虚拟隧道发送包所用的服务类型。

31. 如权利要求 24 所述的方法，其中该移动节点是一无线计算机、一个个人数字助理或一移动电话。

用于提供动态互联网协议安全策略服务的方法

5 技术领域

本发明通常涉及网络通信。更具体地，本发明涉及一种用于提供动态互联网协议策略服务的方法。

背景技术

10 移动节点可利用移动互联网协议（“移动 IP”）从它的本地网络（home network）漫游离开，并且移动节点可建立与外部网络（foreign network）的连接。移动节点可利用协议比如互联网协议安全性（“IPsec”）与它的本地网络安全地通信。IPsec 可用于在外部代理（“FA”）与本地代理（“HA”）之间通信。FA 能够从移动节点接收包(packet)。然后 FA 能够利用 IPsec，例如加密来自移动节点的包，并且通过虚拟隧道（virtual tunnel）将它们转发到 HA。然后 HA 接收这些包，并且对它们解密以找回原始消息。类似的处理可用于将包从 HA 发送到 FA，它们能够最终发送到移动节点。

在 IPsec 中，可定义策略(policy)用于对应于特定 FA-HA 对的移动节点。该策略一般地指明用于在移动节点漫游到 FA 的网络时在 FA 与 HA 之间 20 IPsec 通信的参数。该策略可由 HA 定义和存储，并且对应的策略可由 FA 定义和存储。当包穿过虚拟隧道时，FA 与 HA 能够利用它们各自的策略，以在处理该包时应用适当的 IPsec 参数。

为了允许移动节点漫游到不同的外部网络，并且利用 IPsec 继续与它的 HA 通信，能够一设置策略用于移动节点能利用的每个可能的 FA-HA 对。为 25 FA-HA 对所建立的策略应当由 HA 与对应的 FA 存储。添加移动节点能够访问的附加 FA 会增大需要建立的 FA-HA 对的数量。此外，当建立策略时，需要知道 FA 与 HA 的 IP 地址或其他标识符。用于定义 FA-HA 对的该方法不容易升级（scalable），并且需要大量时间以建立和存储所有可能的 HA-FA 对。

30 除为每个 FA-HA 对存储一策略之外，FA 与 HA 均存储对应于每个可能

FA-HA 对的过滤器。这些过滤器能够存储在过滤器列表中，并且它们能够用以确定包是否应当接收 IPsec 处理。例如，当 FA 或 HA 收到包时，FA 或 HA 能够搜索它的过滤器列表，以确定是否存在对应于该包的过滤器。如果存在过滤器，则 FA 或 HA 例如通过利用为该 FA-HA 对和该移动节点所定义的策略，能够将 IPsec 处理应用于该包。

FA 或 HA 均存储对应于许多 FA-HA 对的大量过滤器，因此它的过滤器列表也会很大。当包到达 FA 或 HA 时，FA 或 HA 搜索它的过滤器列表，以确定是否将策略服务应用于该包。搜索过滤器列表是耗时和计算密集的处理，并且会降低 FA 或 HA 处理该包的速度。

因此，存在着对在 IPsec 环境中提供策略服务的新的改进方法的需要。

发明内容

按照本发明的优选实施例，能够克服与互联网协议安全通信相关联的某些问题。提供一种用于提供动态互联网协议安全策略服务的方法。

本发明的一方案包括一种方法，用于动态地链接一策略以应用于外部代理与本地代理之间的互联网协议安全会话。该策略能够应用于外部代理与本地代理之间发送的包。外部代理在与本地代理建立互联网协议安全会话时可动态地链接到一策略，并且本地代理在与外部代理建立互联网协议安全会话时可动态地链接一策略。

本发明的另一方案包括一种方法，用于动态地创建一过滤器，以应用于外部代理与本地代理之间的互联网协议安全会话。外部代理可动态地建立一过滤器，该过滤器能够用于识别接收互联网协议安全处理的包。本地代理也能够创建一过滤器，该过滤器识别接收互联网协议安全处理的包。当外部代理与本地代理之间的 IPsec 会话结束时，该过滤器可从现行过滤器列表中去除。

适当参照附图，阅读如下的具体描述，本发明的这些以及其他方案和优点将变得更明显。

附图说明

这里参照附图，描述本发明的示范性实施例，在附图中：

- 图 1 是说明 IP 包报头的框图；
图 2 是说明示范性移动互联网协议系统的框图；
图 3 是说明图 2 的移动互联网协议系统中的示范性移动互联网协议通信的框图；
5 图 4 是说明互联网协议安全认证报头的框图；
图 5 是说明封装安全有效载荷(payload)包格式的框图；
图 6 是说明在经过互联网协议网络的两个端点 (endpoint) 之间的各种端对端安全配置的框图；以及
图 7 是用于动态链接一策略和建立一过滤器的处理的流程图。

10

具体实施方式

许多不同的设备能够连接于网络和交换数据，并且各种类型的网络可用于连接设备。例如，一个或多个计算机可连接于局域网（“LAN”）。然后，连接于 LAN 的计算机能够经过网络交换数据。在另一实例中，无线设备可
15 连接于蜂窝无线网络。然后无线设备可与连接于无线网络的其他设备通信。

一个或多个网络也可链接在一起，并且连接于某一网络的设备能够与连接于另一网络的设备通信。例如，LAN 可通过互联网服务供应商（“ISP”）提供与互联网的连通性。类似地，蜂窝无线网络可提供与公共交换电话网（“PSTN”）或与分组数据服务节点（“PDSN”）比如互联网的连通性。
20 一旦这些网络连接于互联网或另一网络，某一网络上的设备设备能够与另一连接网络上的设备交换数据。例如，蜂窝网络上的无线设备能够连接于 PSTN 上的设备或互联网上的设备。

一网络一般地支持一个或多个通信协议。通信协议通常提供用于在网络上的设备之间交换数据的格式，并且多个协议可在通信会话期间使用。除提供用于在同一网络上的设备之间交换数据的格式之外，通信协议可提供用于在连接于不同网络的设备之间交换数据的格式。
25

例如，传输控制协议（“TCP”）和互联网协议（“IP”）可用于在同一或不同网络上的设备之间发送数据。TCP 是用于在网络比如互联网上发送数据的面向连接协议。TCP 通常结合 IP 一起利用，并且它们提供这样的格式，用于将数据消息分成包、在一个或多个网络上将这些包传输给接收端、
30

以及在接收端重组这些包以形成原始数据消息。

IP 能够用于在同一网络上的设备之间和在不同网络上的设备之间发送数据。对于 IP 通信，一设备通常分配有 32 位的 IP 地址。IP 地址在连接的网络上通常是全球唯一的，并且这允许目标设备通过它的 IP 地址被唯一识别。
5 数据以 IP 包的形式传输。IP 包包括报头（header）部分和数据部分。

图 1 是说明 IP 包报头 50 的框图。IP 包报头包括许多不同字段。版本字段 52 表示 IP 版本，比如 IPv4 或 IPv6。互联网报头长度（“IHL”）字段 54 表示报头的长度。服务类型（“ToS”）字段 56 表示所请求的服务类型。总长度字段 58 表示包括 IP 报头 50 在内的 IP 包中所有内容的长度。标识字段 10 60 可用于包分段（fragmentation）。分段偏移字段 62 也用于包分段。保存时间（“TTL”）字段 64 可以是跳跃计数，用于限制 IP 包的使用期(lifetime)。协议字段 66 表示与 IP 包一起利用的协议。例如，TCP、用户数据包协议（“UDP”）、封装安全有效载荷（“ESP”）和认证报头（“AH”）是可结合 IP 一起利用的通用协议。也可利用其他协议。报头校验和字段 68 能够 15 用于校验 IP 包报头 50 的内容。源地址字段 70 可包括用于发送端点的源 IP 地址，目标地址字段 72 可包括用于接收端点的 IP 地址。选项字段 74 能够用于安全、源发送、错误报告、调试、时间标记（stamping）或其他信息。IP 15 数据可承载于选项字段 74 之下的 IP 包数据部分中。

IP 包在网络上发送，并且利用报头中所含的目标设备的 IP 地址，适当 20 地发送到目标设备。IP 包在到达目标设备之前可穿过不同设备和经由不同网络。IP 地址用于准确地经过网络发送该包，并且发送到正确的目标设备。

尽管 IP 提供用于唯一地识别经过多个网络的设备的方法，但是它并不提供用于确保从源设备发送的包将在目标设备成功接收的机制。由于不同因素 25 比如数据破坏、缓冲溢出、设备故障或其他错误，包在经过网络的传输期间可能丢失。TCP 能够结合 IP 一起利用，以确保包的可靠的端对端传输。在其他功能中，TCP 处理丢失或破坏的包，并且重组次序混乱地到达其目的地的包。TCP/IP 是一种在手机(handset)与媒体服务器之间建立连接的方法，并且还存在许多其他互联网或网络协议。

另一可用于发送数据的协议是移动 IP，其为 IP 的扩展。虽然 IP 能够用 30 于连接在分离网络上的设备，但是 IP 地址通常仅关联于一个特定网络。无线

设备可分配有与该无线设备的本地网络相关联的 IP 地址。然而在通信会话期间，无线设备可能漫游到另一网络。

移动 IP 是 IP 协议的扩展，其允许“移动”节点在不同的 IP 子网络（“子网”）之间透明地移动，并且仍接收寻址于与移动节点本地网络相关联的 IP 地址的数据。虽然移动节点动态地改变它的网络连通性，但是这对于 IP 以上的协议层（例如 TCP 或 UDP）是透明的。移动 IP 在 1996 年 10 月，C.Perkins 的 Internet Engineering Task Force Request for Comment 2002 中有具体描述，这里整体并入作为参考，并且在 ISBN-0-13-856246-6, 1998, Prentice-Hall, J.D.Solomon 的“Mobile IP: The Internet Unplugged”中有具体描述，这里整体并入作为参考。
10

图 2 是说明示范性移动 IP 系统 124 的框图。移动 IP 系统 126 包括连接于本地网络 100 的两个非移动网络设备 102、104 和移动网络设备（“移动节点”）106。然而本地网络 100 可包括更多或更少的非移动网络设备。它也可包括多个移动网络设备。移动节点 106 可优选为任一无线设备，比如便携电话、个人数字助理（PDA）、无线装备的计算机或其他设备；然而，移动节点也可能是非无线设备。非移动网络设备 102、104 例如也可以是包括网络接口卡（“NIC”）的计算机或其他设备。NIC 通过接口与本地网络 100 连接并且提供与本地网络 100 的连通性。
15

在一实施例中，本地网络 100 是 LAN，并且连接于本地网络 100 的网络设备 102、104、106 利用 IEEE803.2 以太网协议进行通信。在该协议中，本地网络 100 上的每个网络设备 102、104、106 分配有子网网络地址，该地址是 IEEE803.2 协议所支持类型的以太网地址。该子网网络地址提供用于识别每个网络设备 102、104、106 的机制，并且用于在本地网络 100 上的网络设备 102、104、106 之间交换数据。本地网络 100 并不限于利用 IEEE803.2 协议的 LAN。存在许多不同的网络类型，并且许多不同的协议和寻址方案可用于在网络上的设备之间交换数据。也可以利用这些不同的网络类型和协议。
25

本地网络 100 经由本地代理（“HA”）108 连接于外部网络 110，比如互联网或内联网。本地代理 108 是用于本地网络 100 的“网关路由器”。正如现有技术中所公知的，网关利用不同的连网协议或以不同的传输性能进行操作来连接网络。同时，正如现有技术中所公知的，路由器解释网络协议之
30

间的差异，并且将数据包发送到适当的网络节点或网络设备。通过连接于本地网络 100，本地网络 100 上的网络设备 102、104、106 能够与连接于外部网络 110 的设备交换数据。

分配给本地网络 100 上每个网络设备 102、104、106 的子网网络地址，
5 比如以太网地址，通常并非是全球可发送的地址。因此，它可能不支持本地
网络 100 上的设备与连接于外部网络 110 的设备之间的通信。为了与连接于
外部网络 110 的设备通信，本地网络 100 上的一个或多个设备也可分配有一
10 全球地址。当该设备与外部网络上的设备通信时，该全球地址可用于识别该
设备。例如，连接于本地网络 100 的一个或多个设备可均分配有一 IP 地址，
该 IP 地址是用于与连接于外部网络 110 的设备交换数据的全球可发送的地
址。

尽管除其子网网络地址之外，本地网络 100 上的网络设备 102、104、106
可能分配有全球可发送的地址，但是本地网络 100 上的网络设备 102、104、
106 也可能利用一寻址方案来交换数据，该寻址方案支持与连接于外部网络
15 110 的设备的通信。在这种情况下，子网网络地址可全球发送，并且与全球
地址相同。例如，本地网络设备 102、104、106 可利用 IP 或另一相似的协议
彼此通信。由于 IP 能够是全球可发送的地址，所以不必给网络 102、104、
106 分配除其子网地址之外的全球地址。

移动节点 106 表示为连接于本地网络 100 的虚线方框 106，因为移动节
点 106 会从它的本地网络 100 “漫游”离开并且连接于外部网络 120。当移
动节点 106 从它的本地网络 100 漫游离开时，它周期性地将移动 IP “代理请
求”消息传输到外部代理，比如外部代理（“FA”）112。外部代理 112 相
对于移动节点的本地网络 100 是外部的。

图 2 还表示出外部网络 120。外部网络 120 包括两个非移动节点 114、
25 116。然而该外部网络可能包括更多或更少数量的非移动节点。外部网络 120
还可包括一个或多个移动节点，对于这些移动节点，外部网络 120 用作本地
网络，但这样的移动节点在图 2 中未示出。外部代理 112 存在于外部网络 120
上。类似于本地代理 108，外部代理 120 是用于外部网络 120 的网关路由器。

外部网络设备 114、116 分配有外部网络 120 上的子网网络地址。子网
30 网络地址可用于连接于外部网络 120 的设备之间的通信。如前文所述，子网

网络地址可能并非是全球可发送的，并且外部网络 120 上的网络设备 114、116 还可能分配有全球可发送的地址。例如，外部网络上的一个或多个设备 114、116 还可分配有一 IP 地址。然而，子网网络设备（例如 IP 地址）可能是全球可发送的，并且能够用于与连接于外部网络 110 的设备通信。

5 当移动节点 106 从它的本地网络 100 离开时，它可连接于外部网络 120。漫游的移动节点 106 从外部代理（即外部网关路由器，比如外部代理 112）收听移动 IP “代理广告” 消息。该代理广告消息表示漫游的移动节点 106 现在位于外部网络 120 上。当漫游的移动节点 106 从一外部代理比如外部代理 112 接收到代理广告消息时，移动节点 106 向外部代理（例如外部代理 112）
10 以及它的本地代理（例如本地代理 108）注册。该注册表示移动节点 106 已经从它的本地网络 100 漫游到外部网络 120。

移动节点 106 利用它在本地网络 100 上的家庭全球(home global)地址以向外部代理 112 和本地代理 108 注册。在移动节点 106 注册之后，除用于外部网络 120 上网络设备 114、116 的数据包之外，外部代理 112 可在用于移
15 动节点 106 的特定家庭全球地址接受移动节点 106 的数据包。外部代理 112 还可将外部网络 120 上的临时子网网络地址分配给移动节点 106。

图 3 是说明示范性移动 IP 系统 128 中的示范性移动 IP 通信的框图。一旦移动节点 106 漫游到外部网络 112 并且注册它的当前位置（例如在外部网络 112 上和在本地网络 100 上），本地代理 108 可经由外部网络 110 建立去
20 往外部代理 112 的“虚拟隧道” 126。虚拟隧道 126 并非是外部代理 112 与本地代理 108 之间建立的附加物理连接，而是虚拟隧道 126 代表一概念上的数据路径，用于在本地代理 108 与外部代理 120 之间传输数据。虚拟隧道 126 能够通过将数据包装入另一数据包内并且通过添加附加的隧道包报头来建立。

25 在本发明的一个优选实施例中，利用 IP-in-IP 隧道传输。IP-in-IP 隧道传输在 1995 年 10 月，W.Simpson 的 Internet Engineering Task Force Request for Comment 1853 中有更具体地描述，这里整体并入作为参考。隧道传输和数据封装还在 1996 年 10 月，C.Perkins 的 Internet Engineering Task Force Request for Comment 2003 中有所讨论，这里整体并入作为参考，并且在 1996 年 10
30 月，C.Perkins 的 Internet Engineering Task Force Request for Comment 2004 中

有所讨论，这里整体并入作为参考。也能够建立并且也可利用其他类型的虚拟隧道，比如 UDP 隧道传输或双重的 IP-in-IP 隧道传输。

连接于外部网络 110 的网络设备 130 可能需要发送数据到移动节点 106。尽管网络设备 130 通常表示为连接于外部网络 110，但是它实际上可以是连接于网络比如 LAN 的计算机或另一类型的设备。然后该网络向网络设备 130 提供与外部网络 110 的连通性。

网络设备 130 发送一寻址于移动节点 106 的数据消息。这例如可通过向移动节点 106 发送一寻址于其全球可发送 IP 地址的包来完成。该包穿过外部网络 110，并且发送到本地代理 108。本地代理 108 接受寻址于其子网中设备的 IP 地址的包。如果移动节点 106 连接于本地网络 100，则本地代理 108 转发该包到移动节点 106。然而，移动节点 106 并未连接于本地网络 100。移动节点 106 连接于外部网络 120，该包必须从本地代理 108 转发到外部网络 120。

移动节点 106 向本地代理 108 和外部代理 112 预先注册它的新子网位置。本地代理 108 将寻址于移动节点 106 的包封装为隧道包，其经过虚拟隧道 126 发送到外部代理 112。当外部代理 112 接收到该隧道包时，它去除隧道包报头，并且发送该包到移动节点 106。

移动节点 106 利用 ICMP 消息，周期性地传输“继续有效（keep-alive）”消息。这些消息可包括专用于移动 IP 的标准 ICMP 消息和其他 ICMP 消息。移动节点 106 能够漫游到除图 3 所示外部网络 120 之外的外部网络，并且移动节点 106 能够利用移动 IP 向其他外部代理注册。这允许移动节点 106 移动到多个外部网络。

互联网协议安全

尽管 IP 提供寻址方案，用于在源设备与目标设备之间发送包，但是它不能确保源设备和目标设备是访问和读取 IP 包的数据部分的仅有设备。其他设备可截取 IP 包及读取它的数据部分。为了阻止其他设备截取 IP 包和读取它们的数据部分，在 IP 通信期间采用附加的安全协议以提供 IP 包的安全。

互联网协议安全性（“IPsec”）是一种用于提供 IP 包安全的方法。IPsec 在 1998 年 11 月，Kent et al. 的 Internet Engineering Task Force Request for Comment 2401 的“Security Architecture for the Internet Protocol”中有更具体

地描述，这里将其整体并入作为参考，并且在 2001 年 7 月，A. Krywaniuk 的 Internet Engineering Task Force IP Security Working Group Draft 的“Security Properties of the IPsec Protocol Suite”<draft-krywaniuk-ipsec-properties-00.txt> 中有更具体地描述，这里将其整体并入作为参考。IPsec 通常对在源端点与 5 目标端点之间移动的 IP 包改善消息认证、消息完整性和消息机密性。从两个端点之间不存在连接的状态开始，安全关联（“SA”）能够基于 IP 而建立，从而使每个端点信任该连接的安全，并且每个端点的身份可认证至另一端点。

IPsec 通常定义两个安全服务，并且每个安全服务具有相关联的报头，利用该服务将该报头添加到 IP 包。这两个安全服务是认证报头（“AH”）和封装安全有效载荷（“ESP”）报头。尽管 IPsec 定义这两个安全服务，但是更少或更多数量的安全服务也能够与 IPsec 一起利用。
10

AH 对 IP 包提供认证和完整性保护。认证报头在 1998 年 11 月，Kent et al. 的 Internet Engineering Task Force Request for Comment 2402 的“IP 15 Authentication Header”中有更具体地描述，这里将其整体并入作为参考。

图 4 是说明互联网协议安全认证报头 200 的框图。下一报头字段 202 是标识在 AH 之后下一有效载荷的类型的 8 位域。有效载荷长度字段 202 以 32 位的字（即 4 个字节）指明 AH 的值。保留字段 206 是保留的 16 位字段以备用。安全参数索引（“SPI”）字段 208 是任意 32 位的值，该值与目标 IP 20 地址和安全协议（例如 AH 或 ESP）相结合，唯一地标识用于数据包的 SA。序列号字段 210 是无符号（unsigned）的 32 位字段，该字段包括单调递增的计数值作为序列号。认证数据字段 212 是包括用于包的完整性校验值（“ICV”）的可变长度字段。

ESP 提供机密性以及认证和完整性保护。封装安全有效载荷在 1998 年 25 11 月，Kent et al. 的 Internet Engineering Task Force Request for Comment 2046 的“IP Encapsulating Security Payload (ESP)”中有更具体地描述，这里将其整体并入作为参考。

图 5 是说明 ESP 包格式 250 的框图。SPI 字段 252 是任意 32 位的值，该值与目标 IP 地址和安全协议（例如 AH 或 ESP）相结合，唯一地标识用于 30 该包的 SA。序列号字段 254 是 32 位的字段，该字段包括单调递增的计数值

作为序列号。有效载荷数据字段 256 是可变长度字段，该字段包括下一报头字段 262 所描述的数据。填充字段 258 与有效载荷数据字段 266 一起用于加密。填充长度字段 260 表示紧接在其之前的许多填充字节。下一报头字段 262 是 8 位字段，该字段包括有效载荷数据字段 256 中所含数据的类型。认证数据字段 264 是可变长度字段，该字段包括通过整个 ESP 报头 250 减去认证数据字段 264 而计算的完整性校验值（“ICV”）。

IPsec 协议报头在 IP 包报头 50 的协议字段 66 中被标识。IPsec 协议报头指明协议类型（即 AH 或 ESP），并且包括被称为安全参数索引（“SPI”）的数值。SPI 是通过接收端点关联于 SA 的专用标识符。标识信息由接收端利用，以有助于它将 IP 包正确地与 SA 相关联。IP 包与 SA 的关联允许恰当的 IPsec 处理。

IPsec 服务能够应用于两种模式之一，即“传送模式”或“隧道模式”。在传送模式中，通常仅加密 IP 包的数据。利用目标地址（例如 IP 目标地址 72）将 IP 包发送到目标设备。在传送模式中，目标 IP 地址和源 IP 地址对于网络上的其他设备都是“可见的”（即未加密）。结果，另一设备能够监控在源设备与目标设备之间发送的包的数量。然而，由于数据被加密，该设备一般不能够确定 IP 包中的数据内容。一旦传送模式包到达它的最终目标，目标设备进行 IPsec 处理。例如，目标设备可按照协定的加密方法对 IP 包中所承载的数据解密。

在隧道模式中，通常加密整个 IP 包，并且沿着虚拟隧道将该包发送到目标设备。虚拟隧道能够利用作为源设备和目标设备的 IPsec 代理的路由器或其他网络设备来形成。源设备发送 IP 包到源设备端点。源设备端点加密 IP 包，并且将加密后的包替换成新的 IP 包。然后，新的 IP 包经过网络发送到目标设备端点。目标设备端点解密原始 IP 包，并且将该包转发到目标设备。利用该模式，黑客仅能确定隧道的端点。黑客无法确定隧道传送的包的实际源地址和目标地址，因而黑客无法准确地确定在两个设备之间正在发送多少包。

图 6 是说明在传送和隧道模式中利用 AH、ESP 及其组合在 IP 网络 318（例如互联网或内联网）上的两个端点之间的各种端对端安全结构 300 的框图。第一端点 302 具有至第二端点 306 的安全连接 304。第一示范性数据包

308 包括第一 IP 报头中的第一 IP 地址（“IP1”）、AH 报头和上级协议数据。第二示范性数据包 310 包括第一 IP 地址、ESP 报头和上级协议数据。第三示范性数据包 312 包括第一 IP 地址、AH 报头、ESP 报头和上级协议数据。示范性数据包 308、310 和 312 用于传送模式中。取决于期望的安全类型，
5 一般为传送模式选定一种类型的数据包设计（308，310 或 312）。

在隧道模式中，第四示范性数据包 314 包括带有隧道 IP 地址（TIP）的
10 隧道 IP 报头、AH 报头、带有第一 IP 地址（“IP1”）的原始 IP 报头和上级协议数据。第五示范性数据包 316 包括带有隧道 IP 地址的隧道 IP 报头、AH 报头、带有第一 IP 地址的原始 IP 报头和上级协议数据。取决于期望的安全性，一般为隧道模式选定一种类型的示范性数据包 314 或 316。
10

IPsec 协议建立和利用安全关联（“SA”）以识别两个端点之间的安全虚拟连接。SA 是两个端点之间的单向连接，其代表单个 IPsec 协议模式组合。单个 SA 的两个终端端点（即用于传送模式的网络设备或用于隧道模式的中间设备）定义一 IPsec 服务所保护的安全虚拟连接。这两个端点之一发送 IP
15 包，另一端点接收 IP 包。由于 SA 是单向的，最少需要两个 SA 用于安全的双向通信。也能够通过组合多个 SA 在两个端点之间构造多层的 IPsec 协议。
15

除定义安全服务（即 AH、ESP）和模式（即隧道或传送）之外，IPsec 允许利用许多不同方法，用于执行加密、认证和其他功能。这些各种参数还能够在 SA 中定义。例如，SA 可表示哪个加密方法和哪些密钥将用于 IPsec
20 通信会话中。在成功的通信能够出现在 IPsec 通信会话中的两个设备之间以前，应当确定用于该会话的特定 SA。
20

建立 IPsec SA 的处理包括协商和认证。在协商中，两个端点协定利用哪个安全协议和模式。它们还对建立的每个 SA，协定要利用的其他算法，比如具体的加密技术、关联参数值和 SPI 分配。该认证确保每个端点在协商期间以及在建立 SA 之后能够信任其他端点的身份。
25

已提出许多标准用于建立 SA 的协议，包括：互联网安全关联和密钥交换协议（“ISAKMP”）、Oakley 协议（“Oakley”）、以及合并 ISAKMP 和 Oakley 的互联网密钥交换（“IKE”）协议。ISAKMP 在 1998 年 11 月，
30 Maughan et al. 的 Internet Engineering Task Force Request for Comment 2408 的
“Internet Security Association and Key Management Protocol（“ISAKMP”）”

中有更具体地描述，这里将其整体并入作为参考。Oakley 在 1998 年 11 月，H.K. Orman 的 Internet Engineering Task Force Request for Comment 2412 的“*The OAKLEY Key Determination Protocol*”中有更具体地描述，这里将其整体并入作为参考。IKE 在 1998 年 11 月，Harkins et al. 的 Internet Engineering
5 Task Force Request for Comment 2409 的“*The Internet Key Exchange (IKE)*”中有更具体地描述，这里将其整体并入作为参考。

例如，利用 IKE，SA 协商可作为两个端点之间信令交换的序列来进行。第一端点提出安全协议和加密算法，并且第二端点接受或反对提议。一旦信令完成并且两个端点已协定所协商的细节，则交换有关的安全参数信息，并且端点准备在单个单向 SA 上发送或接收。部分信令包括利用认证授权（“CA”）的认证信息的交换。
10

认证是基于被称为认证授权的受托第三方。参与 IPsec 的每个端点产生公开/私用加密密钥对，并且具有 CA 所“确认”的它的公开密钥。CA 将端点的 IP 地址绑定到它的公开密钥，产生证书 (certificate) 并且将其返还给密
15 钥所有人。因此，IP 地址是用于将公开密钥绑定到其所有人的一个“安全名义空间”。

在 SA 协商期间，某一端点向另一端点提供它的证书以及已利用它的私用密钥加密过的签名。证书和签名通过公开密钥来校验。接受者（在每个端点的一方）利用来自其证书的发送者的公开密钥，以使签名和发送者权力有效，以利用它的 IP 地址。由于仅发送者能够访问私用密钥，所以一旦接受者
20 验证过签名，接受者就确信发起人的“身份”。该身份可通过发起人的 IP 地址来确定，因为 IP 地址形成用于将公开密钥绑定到其所有人的安全名义空间。然而，除利用用于发起人身份的 IP 地址之外，还能够利用其他安全名义空间。证书签发有“保存时间”值，它们在该值之后过期并且变为无效。协商和认证的结果是用于某个单向 SA 的安全连接。用于双向通信的第二 SA
25 可以相似的方式注册。

策略服务

IPsec 能够应用于各种不同的通信会话，并且能够用于各种不同设备之间的通信会话中。为了恰当地建立 IPsec 会话，参与 IPsec 会话的设备一般应当
30 协定 IPsec 会话期间要利用的参数。这些参数例如能够在将应用于 IPsec 会话

的策略中被指定。然后，这些设备能够将这些参数应用于 IPsec 会话期间的通信。

例如，隧道端点比如 FA 或 HA 可从多种不同源接收包，并且这些包需要不同地进行处理。例如，隧道端点可接收作为 IPsec 通信会话的一部分的

5 某些包，并且可接收并非 IPsec 通信会话的一部分的其他包。对于并非 IPsec 通信会话的一部分的包，隧道端点可按照它的 IP 目标地址，简单地发送该包；然而，对于作为 IPsec 通信会话的一部分的包，隧道端点可执行各种 IPsec 处理功能。

在 IPsec 处理功能的实例中，隧道端点可从源设备接收 IP 包。然后，该

10 隧道端点加密该包，并且将它放置于发送给另一隧道端点的新 IP 包的数据部分中。然后，另一隧道端点接收该 IP 包，解密新包的数据部分，以找回原始包并且将原始包转发到目标设备。

隧道端点可附加地支持多个 IPsec 通信会话。每个 IPsec 会话可利用不同的安全协议、不同的加密密钥或其他不同的参数。因此，隧道端点不得不在

15 不同的 IPsec 通信会话中将不同的处理功能应用于包。例如，某一 IPsec 会话利用 ESP，而另一 IPsec 会话利用 ESP 和 AH 的组合。这两个会话可利用不同的加密算法；它们可利用不同的密钥；或者它们可具有其他不同的参数。为了恰当地服务 IPsec 包，隧道端点应当应用正确的处理功能用于 IPsec 包。

对于 IPsec 通信会话，每个隧道端点通常存储一策略和一过滤器用于该

20 IPsec 会话。该策略一般包括关于如何处理该 IPsec 会话的 IPsec 包的信息。

例如，该策略可包括信息比如要利用的服务类型（例如 AH、ESP 或二者兼有）、要利用的加密类型、密钥的使用期限、解释域（“DOI”）。用以协商服务类型的规则或其他信息。策略文件还可定义 IPsec 会话的其他属性。

25 比如通过识别需要 IPsec 处理的包，过滤器能够用于从较大的包集合中识别包的子集。例如，通过维护对应于 IPsec 会话的 FA-HA 对的列表，过滤器一般能够指明需要 IPsec 服务的包。过滤器还可为对应于 FA-HA 会话的 IPsec 包识别要利用的策略，或者可指明其他信息。

当隧道端点接收到一包时，隧道端点确定如何处理该包。隧道端点可维护过滤器列表。该过滤器列表能够覆盖对应于 FA-HA 对的可能的 IPsec 会话。

30 这些对(pairs)可以各种不同方式指明，但它们优选地基于设备的 IP 地址指明。

在隧道端点接收到包之后，它能够参照其过滤器列表中的 FA-HA 对，校验该包的源地址和目标地址。如果过滤器列表包括用于该 IP 包的过滤器，则隧道端点可处理该包。然而，如果过滤器列表不包括用于该包的过滤器，则隧道端点可简单地经过该 IP 包，而不应用策略，也不进行 IPsec 处理功能。

5 在一个示范性操作中，移动节点漫游到外部网络。移动节点将包发送到外部网络的外部代理。FA 读取源 IP 地址、IP 协议类型、源和目标端口以及该包的目标 IP 地址。然后，基于 IP 地址，FA 搜索它的过滤器列表，以确定该 IP 包是否需要 IPsec 处理，以及应用哪个策略。基于过滤器列表，FA 确定该包需要 IPsec 处理。然后，FA 例如按照该过滤器所指示的策略来处理该包。
10 接着，FA 将该包经过该隧道发送到移动节点的 HA。HA 从 FA 接收该包，并且 HA 搜索它的过滤器列表，以确定输入的包是否需要 IPsec 处理。基于过滤器列表，HA 能够确定该包需要 IPsec 处理和应用于该包的策略。然后，HA 能够按照该过滤器所指示的策略来处理该包。

移动节点可漫游到多个不同的外部网络，并且每个外部网络具有它自己的 FA。为了支持 IPsec 通信，应当识别多个 FA-HA 对。用于 FA-HA 对的策略和过滤器应当由 FA 存储，并且用于 FA-HA 对的对应策略和过滤器也应当由 HA 存储。静态定义 FA-HA 对并且存储它们的过滤器和策略可建立由 FA 和 HA 所存储的非常大量的信息。这还会造成处理包的延迟，因为 FA 或 HA 必须搜索大量过滤器以确定是否将 IPsec 处理应用于所接收的包。
15

20 为了提供更大的伸缩性和提高的处理效率，能够动态地链接用于 FA-HA 对的一个或多个策略，并且动态地建立一个或多个过滤器。例如，可为移动节点建立策略模板。策略模板可构造于移动节点的本地网络中，并且可由 HA 存储。可选地，策略模板可存储于能够由 HA 访问的认证、授权和记帐（“AAA”）服务器中，或者策略模板可存储于另一位置中。除存储于本地
25 网络上之外，策略模板还可存储于外部网络中。例如，外部代理也可存储策略模板。

策略模板可存储将用于 FA 与 HA 之间的 IPsec 通信中的参数。当移动节点访问外部网络时，FA 通过 AAA 进行认证程序。然后，AAA 向 FA 指示 IPsec 应当用于与移动节点的通信。然后，策略模板能够动态地链接到 FA，
30 并且策略模板能够用于指明移动节点与 HA 之间通信的参数。例如，FA 可

通过建立策略实例（instance）来建立到策略模板的动态链接。策略实例可以是作用于 PDSN 与 HA 之间的具体关联性的策略模板的实例。尽管策略模板可指明 FA/PDSN 与 HA 之间的各种参数，FA 和 HA 可附加地协商专用于包含该移动节点的会话的其他参数。例如，FA 和 HA 可附加地协商在 IPsec 策略的 IKE 认证中所用的动态预享（pre-shared）密钥。当然也可以协商其他参数。然后，这些附加的参数可成为策略实例的一部分。因此，策略实例能够从策略模板以及协商的参数中推导。

可为对应于具体移动节点的具体 FA-HA 对建立一策略模板。然而，策略模板对应于特定 FA-HA 对也是可能的。另外，策略模板可用于多个移动节点，或者可用于多个 FA-HA 对。

图 7 是说明用于动态链接策略到 FA 和动态建立过滤器的示范性处理的流程图。在步骤 350，移动节点请求访问外部网络。在步骤 352，外部网络上的外部代理联络移动节点本地网络上的认证服务器。如果移动节点被授权连接于本地网络并且需要安全服务，则认证服务器向外部代理传达：该移动节点需要 IPsec 服务，如步骤 354 所示。外部代理动态地链接到策略模板，并且能够与 HA 协商附加的参数。然后在步骤 356，外部代理为 FA-HA 对建立过滤器。类似地，尽管图 7 中未示出，但是本地代理还为 FA-HA 对建立过滤器，并且能够利用移动节点的本地网络中已定义的策略。最后，在步骤 358，外部代理利用动态链接的策略和动态建立的过滤器来处理包。

继续参照图 3，移动节点 106 漫游到外部网络 120，并且需要与它的本地网络 100 通信。例如通过与外部网络的外部代理 112 通信，移动节点 106 首先启动与外部网络 120 的连接。这可利用各种不同的方法完成。例如，移动节点 106 可拨号进入蜂窝网络，并且尝试通过向 FA112（例如 PDSN）发送移动 IP 注册请求来建立移动 IP 会话。移动 IP 注册请求可请求 FA112 建立与 HA108 的隧道。然后，FA112 可连接 AAA 服务器（图中未示出）。AAA 服务器一般属于移动节点 106 的本地网络 100，并且能够用于确定移动节点 106 是否具有连接到本地网络 100 的许可。如果移动节点 106 具有连接到本地网络 100 的许可，则 HA108 会返回一包括移动节点本地 IP 地址的注册响应消息。然后，移动节点 106 无论漫游到哪儿都能够利用该 IP 地址。

除确定移动节点 106 是否具有连接到本地网络 100 的许可之外，AAA

服务器还确定移动节点 106 在与本地网络 100 通信时是否需要安全（例如 IPsec）。用于移动节点与 HA108 通信的安全策略通常定义于 AAA 服务器中，并且移动节点 106 一般利用 AAA 服务器中所定义的安全策略。AAA 服务器通常仅指明移动节点 106 是否需要安全；它一般并不指明要利用的具体参数。

5 例如，AAA 服务器可表示移动节点 106 应当利用 IPsec，但是它一般并不表示用于 IPsec 会话的具体参数。如果 AAA 服务器确定移动节点 106 需要利用 IPsec，则告知 FA112。然后，FA112 启动与 HA108 的连接，并且 HA 能够动态地将安全策略模板链接到 FA112。然后，FA112 和 HA108 按照安全策略中所指明的具体参数，能够为该会话协商其他 IPsec 参数。例如，FA112
10 和 HA108 可进行适当的协商程序比如 IKE，以协商用于 FA112 与 HA108 之间的通信的其他参数。

FA112 还可为 FA-HA 对动态地建立过滤器，然后该过滤器可存储于 FA112 所维护的过滤器列表中。然后，参照 FA112 所维护的过滤器，校验到达 FA112 的输入包。如果该包的过滤器存在，则 FA112 应用适当的处理；
15 然而，如果过滤器不存在，则 FA112 简单地通过该节点经过该包。HA108 还可为 FA-HA 对动态地建立过滤器，并且利用该过滤器准确地处理从 FA112 接收的并对应于移动节点 106 的包。

由于 IPsec 安全关联是单向的，所以能够建立两个或更多安全关联。例如，FA-HA 对可为从 FA112 发送到 HA108 的包建立一个隧道，并且为从
20 HA108 发送到 FA112 的包建立另一隧道。可将一个或多个策略模板链接到 FA112 用于每个建立的隧道。例如，一个策略模板可为 IPsec 会话指明参数集，而第二策略模板可指明附加参数。此外，还可为每个隧道建立一个或多个过滤器。还能够仅在一个方向上建立隧道。

一旦移动节点 106 从外部网络 120 漫游离开，FA112 与 HA108 之间的
25 隧道会终止。然后，对于移动节点 106 的 FA-HA 对的过滤器从 FA 的过滤器列表中去除。将该过滤器从 FA 的过滤器列表中去除，可改善 FA112 的性能并且加速包的处理。例如，应当参照 FA 的过滤器列表，校验到达 FA112 的输入包，以确定该包是否需要特别处理（例如 IPsec 处理）。如果 FA112 维护庞大的过滤器列表，则参照列表中的每个过滤器校验输入包会是一项费
30 时的处理。通过为 FA-HA 对动态建立过滤器，并且在连接停止有效时去除

该过滤器，FA 的过滤器列表可仅包括用于有效连接的过滤器。这能够减少列表中存储的过滤器的数量，并且提高处理包的效率。

可利用相似的程序用于 HA108 以从它的过滤器列表中去除该过滤器。当移动节点 106 从 FA112 漫游离开时，HA108 可为 FA-HA 对去除该过滤器。

5 例如，当移动节点在移动 IP 会话中注册新的“转交地址（care-of-address）”时，HA108 会去除该过滤器，或者表示它不再利用外部网络的 FA112。通过去除不再有效的过滤器，HA108 能够提高其处理输入包的效率。

在另一实施例中，可为 FA-HA 对定义多个策略或过滤器。在一个实例中，IPsec 会话可具有用于 Phase_1 和 Phase_2 的策略。用于这些阶段（phase）10 的策略可在移动节点连接于 FA 时建立，然后 FA 将移动 IP 注册请求传递到 HA 并且获得作为反馈的响应。用于 Phase_1 的过滤器可包括指明 FA 与 HA 之间的 ISAKMP 包的参数。例如，它可指明用于 FA 的 IP 地址、用于 HA 的 IP 地址、IP 协议以及源和目标端口。用于 Phase_2 的过滤器可包括指明 FA 与 HA 之间的隧道包的参数。例如，它可包括用于 HA 的 IP 地址、用于 FA 15 的 IP 地址和协议类型（例如 IP-in-IP、通用路由封装（“GRE”）或其他类型）。在另一实例中，它可包括用于 HA 的 IP 地址、用于 FA 的 IP 地址、协议类型（例如 UDP、TCP 等）以及源和目标端口。

尽管前面的实例说明了在 IPsec 环境中动态地链接策略和动态地建立过滤器，但是基于策略的服务可用于各种不同系统中。例如，它们可用于网络地址转换（NAT）/端口地址转换（PAT）系统。另外，它们可应用于防火墙环境、服务质量（“QoS”）环境或其他系统中。例如在 QoS 中，策略模板可包括默认优先权和管制信息。AAA 可将 Diffserv 标记和管制信息传递到 PDSN。然后 PDSN 可从该策略模板中建立一策略实例，或者可从移动用户中选择使用该策略模板。

25 应当理解，这里所述的程序、处理、方法和设备并不相关或限定于任何特定类型的计算机或网络设备（硬件或软件），除非另有指明。各种类型的通用或专用计算机设备可按照这里所述的指导来使用或执行操作。尽管优选实施例的各元件已描述为以软件实施，但是在其他实施例中，以硬件或固件实施也是可选择使用的，反之亦然。

30 从本发明的原理能够应用于广泛多样的实施例的观点来看，应当理解所

述实施例仅是示范性的，不应当被视为限制本发明的范围。例如，流程图的步骤可采用所述之外的顺序，并且更多、更少或其他元件可用于框图中。

权利要求不应当被理解为限于所述次序或元件，除非对其效果另有说明。此外，在权利要求中利用术语“设备”旨在调用 35 U.S.C. §112，第 6 段，并且没有“设备”一词的任一权利要求并无此意图。因此，落入所附权利要求及其等效的范围和精神之内的所有实施例均被本发明请求保护。

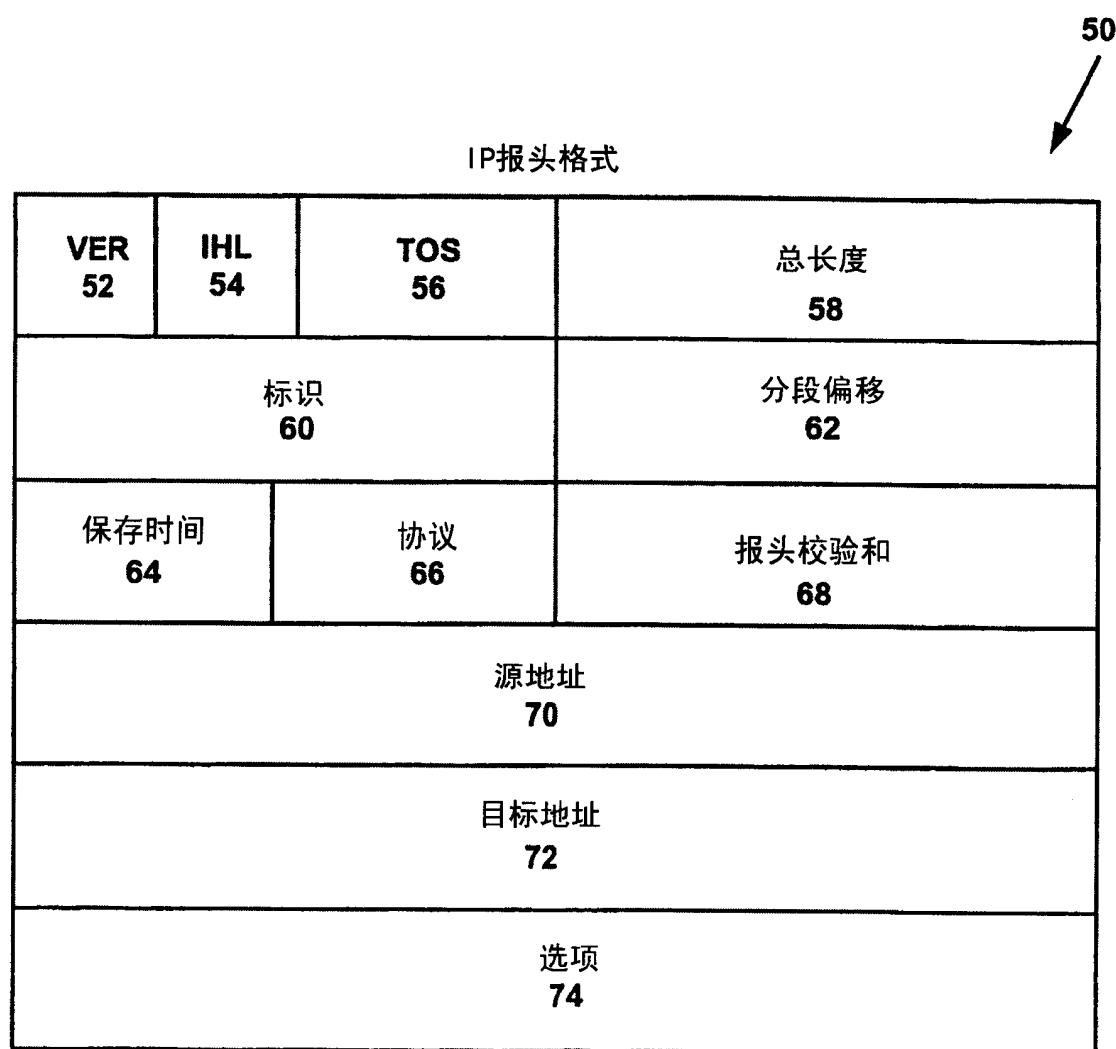
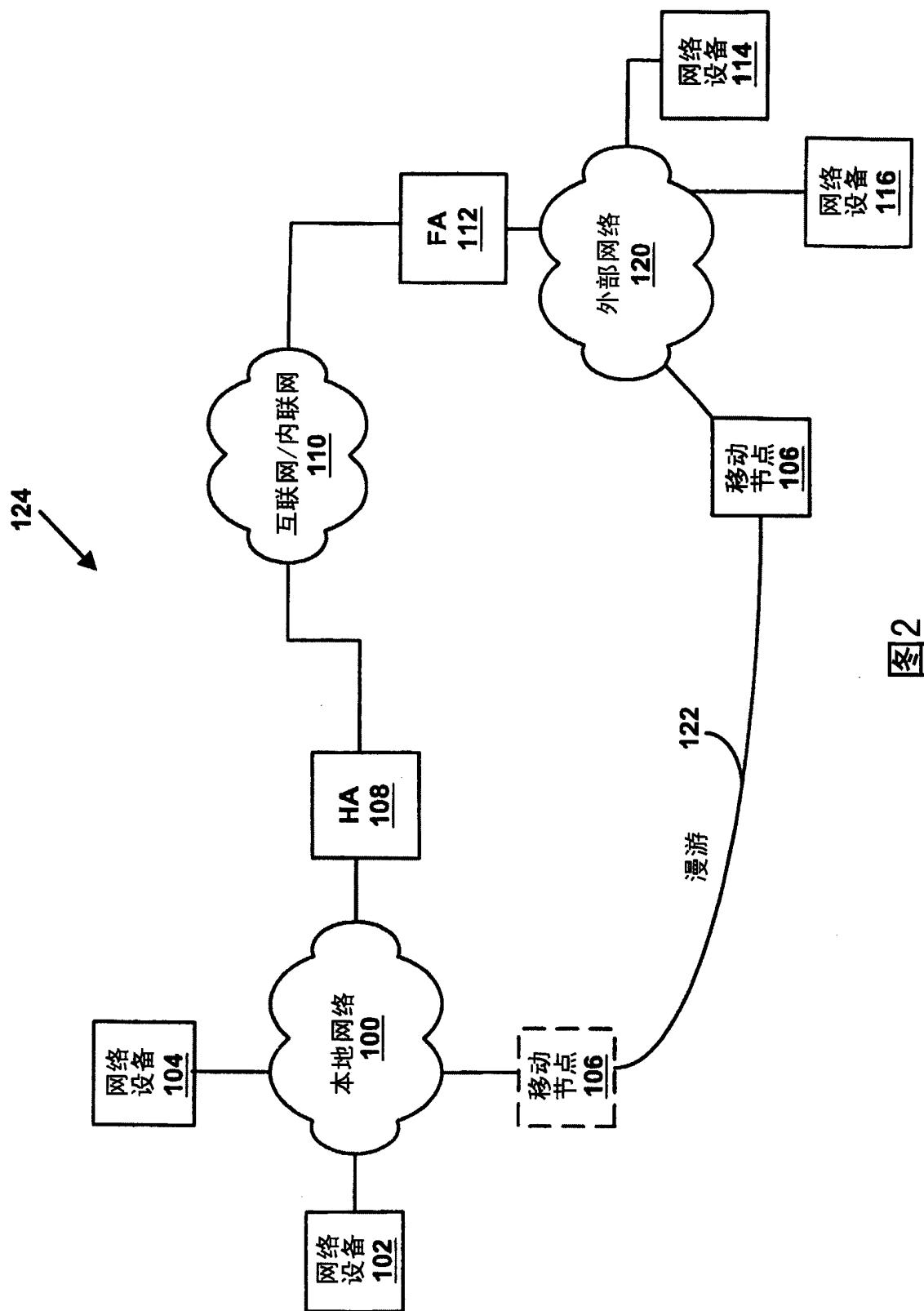


图1



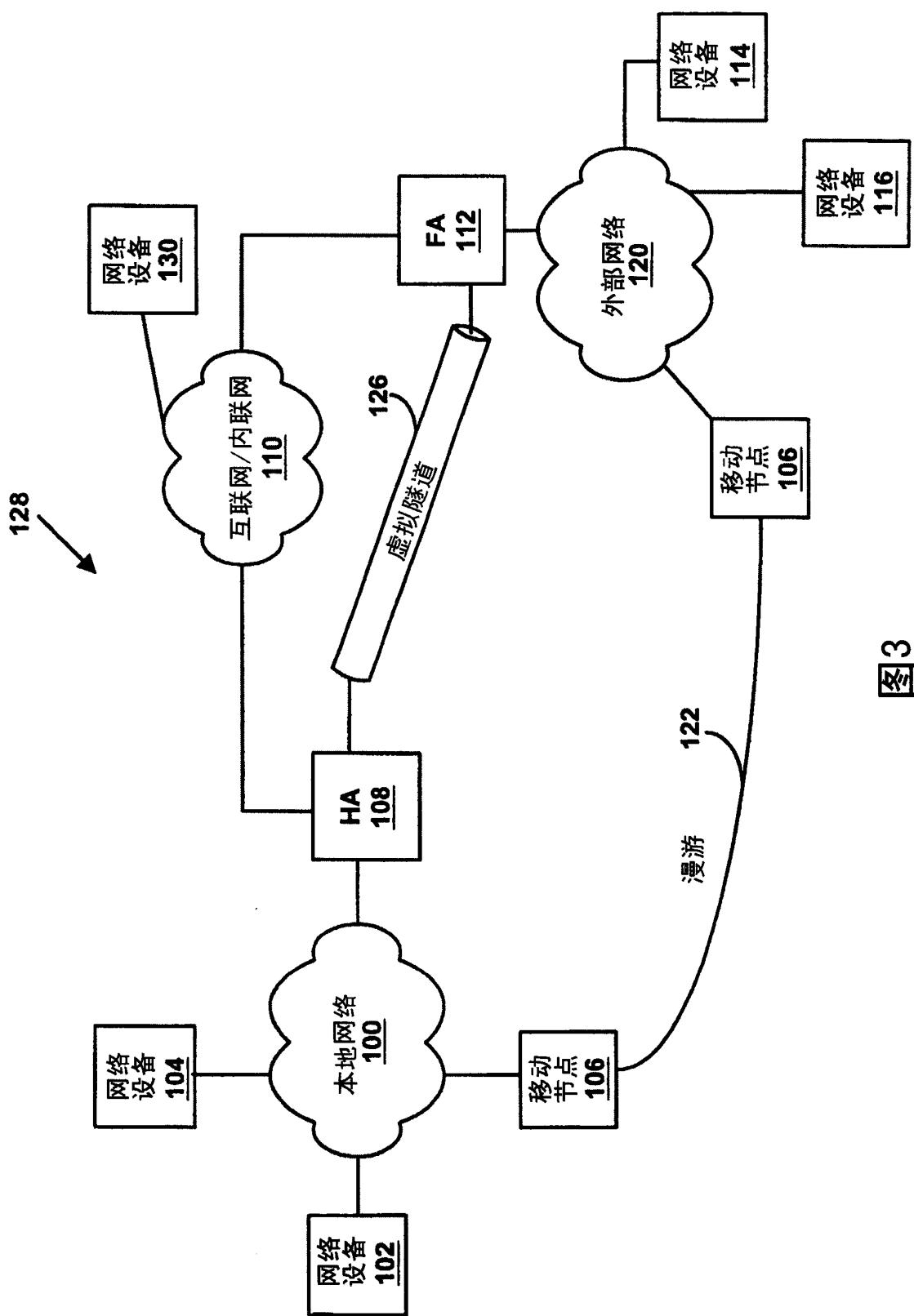


图3

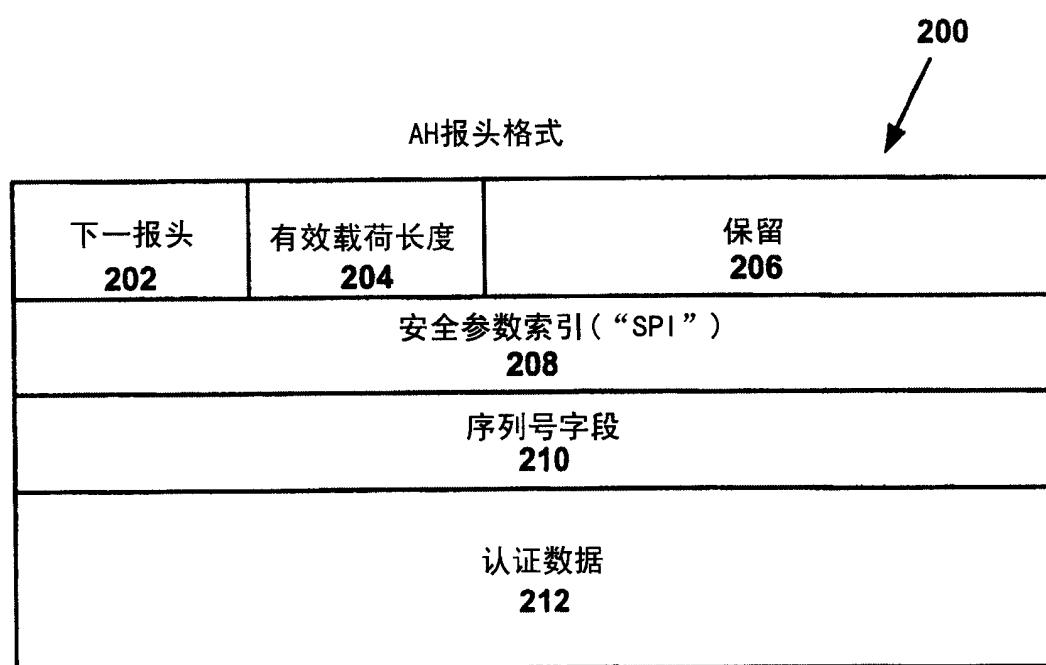


图4

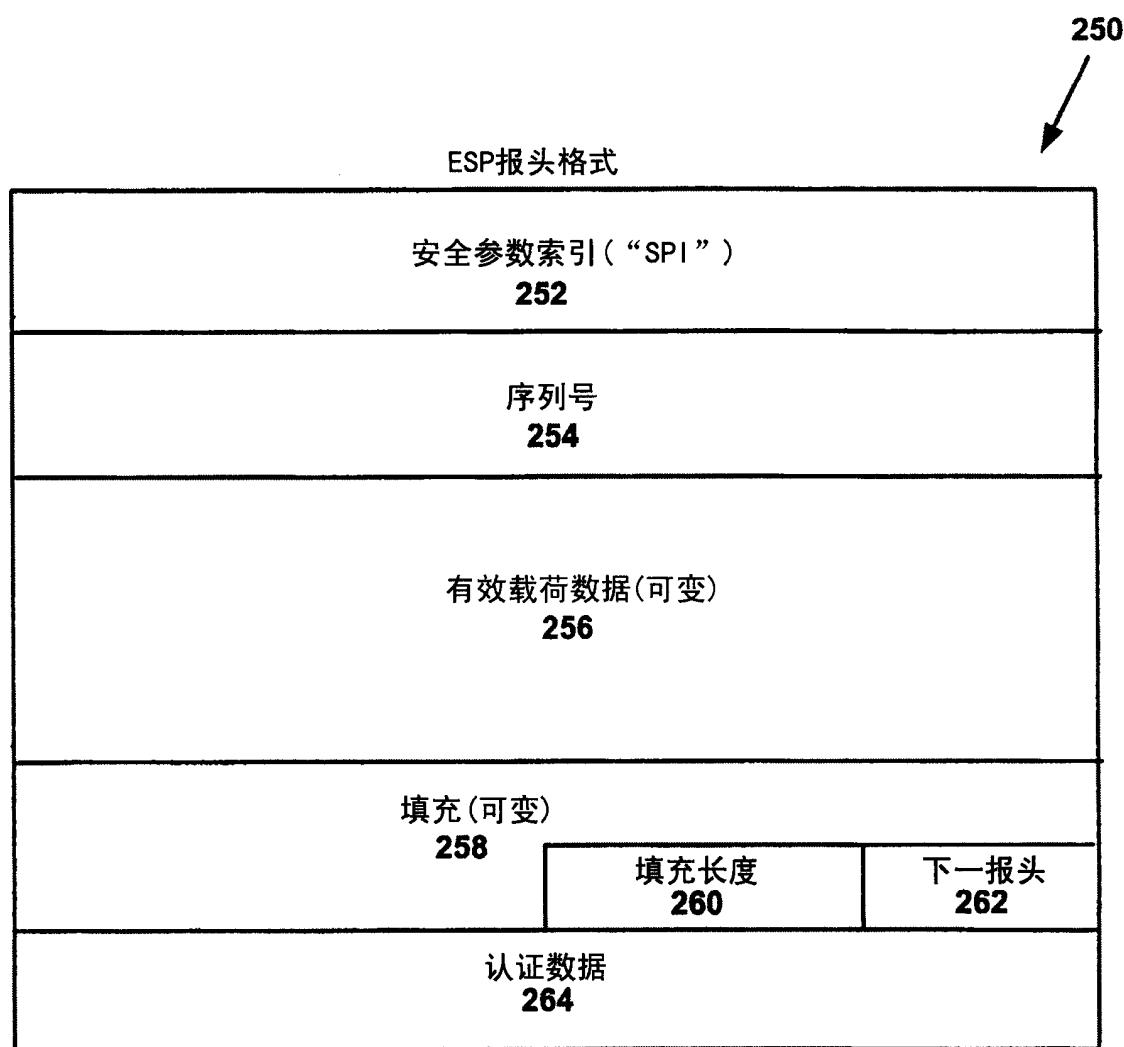


图5

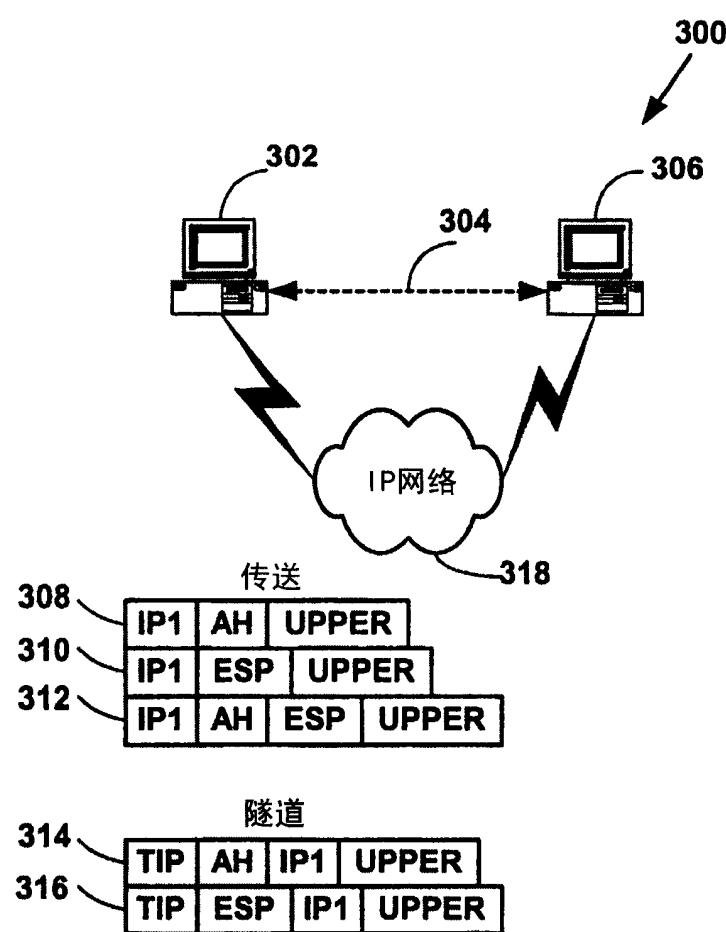


图6

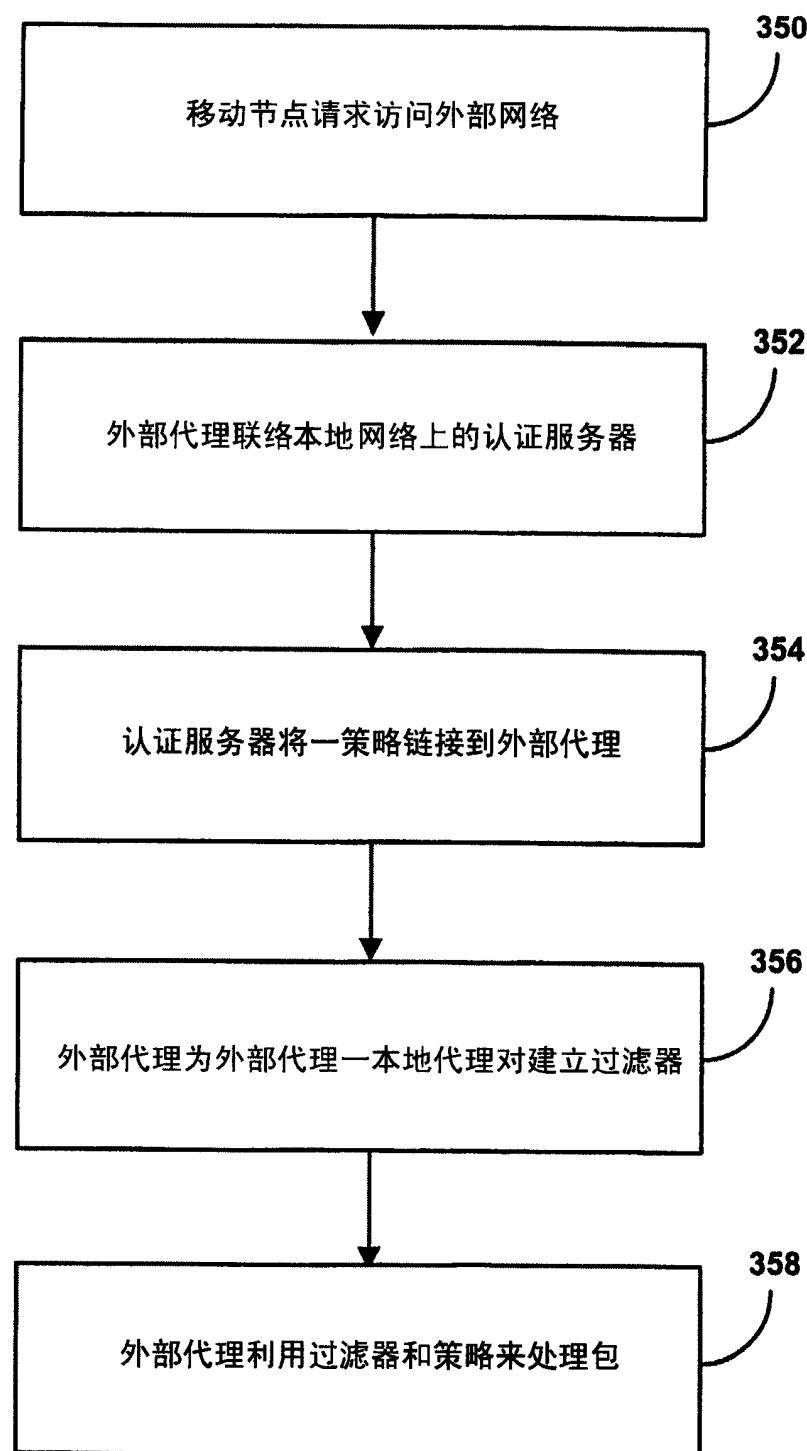


图7