(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106031096 B
(45)授权公告日 2019.07.09

(21)申请号 201480074945.6

(22)申请日 2014.02.06

(65)同一申请的已公布的文献号
申请公布号 CN 106031096 A

(43)申请公布日 2016.10.12

(85)PCT国际申请进入国家阶段日
2016.08.05

(86)PCT国际申请的申请数据
PCT/US2014/015035 2014.02.06

(87)PCT国际申请的公布数据
WO2015/119606 EN 2015.08.13

(73)专利权人 加速系统有限责任公司
地址 美国肯塔基

(72)发明人 J·D·麦肯尼

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李颖

(51)Int.Cl.
H04L 12/28(2006.01)

(56)对比文件
CN 1977494 A,2007.06.06,
CN 1332552 A,2002.01.23,
US 2004148382 A1,2004.07.29,
CN 101360045 A,2009.02.04,
CN 102333306 A,2012.01.25,
US 2005144282 A1,2005.06.30,
CN 101662479 A,2010.03.03,
CN 101252509 A,2008.08.27,

审查员 牟茜茜

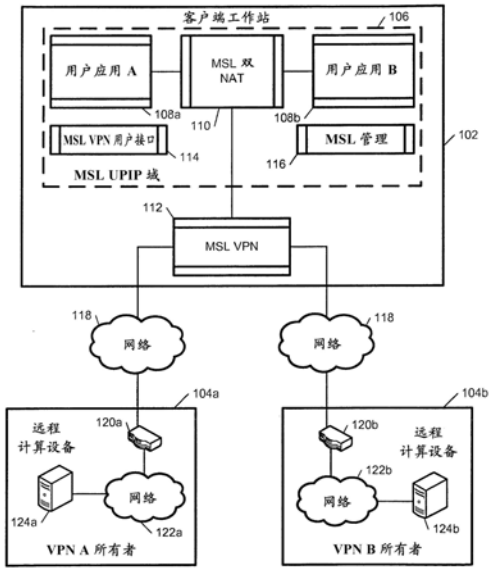
权利要求书3页 说明书9页 附图10页

(54)发明名称

用于提供多安全链路架构的系统和方法

(57)摘要

本文中所公开的一些实施例包括MSL双网络地址转换器(NAT),包括逻辑,该逻辑当由处理器执行时使该MSL双NAT从MSL VPN接收入站数据报并且记录来自入站数据报中的源IP地址的新的VPN所有者私有IP地址。在一些实施例中,该逻辑使该MSL双NAT为入站数据报和客户端工作站指派新的UPIP并且促进向客户端工作站发送入站数据报。



CN 106031096 B

1.一种用于提供多安全链路MSL架构的系统,包括:

MSL虚拟专用网VPN组件,包括第一逻辑,第一逻辑当由处理器执行时使所述系统执行以下各项:

在客户端工作站与第一所有者网关之间创建第一VPN隧道;

从所述客户端工作站向所述第一所有者网关发送出站数据报;

接收从所述第一所有者网关到所述客户端工作站的入站数据报,其中所述入站数据报包括源因特网协议IP地址和被设置为VPN所有者私有IP地址的目的地IP地址;以及

发送具有所述目的地IP地址的所述入站数据报;以及

MSL双网络地址转换器NAT,包括第二逻辑,第二逻辑当由所述处理器执行时使所述系统执行至少以下各项:

从MSL VPN接收所述入站数据报;

记录来自所述入站数据报中的所述源因特网协议IP地址的新的VPN所有者私有IP地址;

为所述入站数据报和所述客户端工作站指派新的独特私有IP(UPIP)地址;以及

向所述客户端工作站发送所述入站数据报,

其中所述系统在所述第一VPN隧道正被利用时在所述客户端工作站与第二所有者网关之间额外地创建第二VPN隧道。

2.如权利要求1所述的系统,其中,所述第一逻辑还使所述系统执行以下各项:

加密所述出站数据报并且将所述出站数据报传递到所述第一所有者网关;以及

从所述第一所有者网关接收加密形式的入站数据报并且解密所述入站数据报。

3.如权利要求1所述的系统,其中,所述第二逻辑还使所述系统将所述出站数据报中的UPIP地址映射到私有IP地址。

4.如权利要求1所述的系统,还包括MSL VPN用户接口组件,所述MSL VPN用户接口组件包括第三逻辑,所述第三逻辑当由所述处理器执行时使所述系统提供用于建立到所述客户端工作站的第一VPN隧道的用户接口。

5.如权利要求1所述的系统,还包括MSL管理组件,所述MSL管理组件包括第四逻辑,所述第四逻辑当由所述处理器执行时使所述系统创建所述第一VPN隧道。

6.如权利要求1所述的系统,其中,所述第二逻辑还使所述系统将所述入站数据报转发到商用货架产品COTS明文处理组件以处理所述入站数据报。

7.如权利要求1所述的系统,其中,所述MSL双网络地址转换器NAT和所述MSL VPN驻留于所述客户端工作站上,并且其中所述客户端工作站还包括MSL VPN用户接口组件和MSL管理组件。

8.如权利要求1所述的系统,还包括MSL服务器,其中所述MSL VPN和所述MSL双网络地址转换器NAT驻留于远离所述客户端工作站的所述MSL服务器上,其中所述系统还包括驻留于所述客户端工作站上的MSL VPN用户接口组件、第一MSL VPN组件和第一MSL管理组件,并且其中所述系统还包括驻留于所述MSL服务器上的商用货架产品COTS明文处理组件、COTS VPN组件和第二MSL管理组件。

9.如权利要求1所述的系统,还包括MSL网关路由器,所述MSL网关路由器包括所述MSL VPN和所述MSL双网络地址转换器NAT,其中所述系统还包括驻留于所述客户端工作站上的

第一COTSVPN组件、MSL管理组件，并且其中所述系统还包括驻留于所述MSL网关路由器上的第二COTS VPN组件和MSL服务器管理组件。

10.如权利要求1所述的系统，还包括MSL装置和MSL服务器，其中所述MSL VPN组件和所述MSL双网络地址转换器NAT驻留于所述MSL服务器上，其中所述系统还包括驻留于所述客户端工作站上的第一COTS VPN组件和MSL VPN用户接口组件，其中所述系统还包括驻留于所述MSL装置上的第一MSL服务器管理组件、第二COTS VPN组件、第三COTS VPN组件和COTS明文处理客户端组件，并且其中所述系统还包括驻留于所述MSL服务器上的第二MSL服务器管理组件、第四COTS VPN组件和第二COTS明文处理客户端。

11.如权利要求1所述的系统，还包括MSL网络操作中心NOC，其中所述MSL双网络地址转换器NAT和所述MSL VPN组件驻留于所述NOC上，其中所述系统还包括驻留于所述客户端工作站上的COTS VPN客户端、MSL VPN用户接口组件和MSL管理组件，并且其中所述系统还包括驻留于所述MSL网络操作中心NOC上的COTS VPN组件、COTS明文处理组件、会话管理器组件和登录管理器组件。

12.一种用于提供多安全链路MSL架构的方法，包括：

在客户端工作站与第一所有者网关之间创建第一VPN隧道；

从所述客户端工作站向所述第一所有者网关发送出站数据报；

接收从所述第一所有者网关到所述客户端工作站的入站数据报，其中所述入站数据报包括源因特网协议IP地址和被设置为VPN所有者私有IP地址的目的地IP地址；

记录来自所述入站数据报中的所述源因特网协议IP地址的新的VPN所有者私有IP地址；

为所述入站数据报和所述客户端工作站指派新的独特私有IP(UPIP)地址；以及

向所述客户端工作站发送所述入站数据报，

其中所述方法在所述第一VPN隧道正被利用时在所述客户端工作站与第二所有者网关之间额外地创建第二VPN隧道。

13.如权利要求12所述的方法，还包括：

加密所述出站数据报并且将所述出站数据报传递到所述第一所有者网关；以及

从所述第一所有者网关接收加密形式的入站数据报并且解密所述入站数据报。

14.如权利要求12所述的方法，还包括将所述出站数据报中的UPIP地址映射到私有IP地址。

15.如权利要求12所述的方法，还包括提供用于建立到所述客户端工作站的VPN隧道的用户接口。

16.如权利要求12所述的方法，还包括创建所述第一VPN隧道。

17.如权利要求12所述的方法，还包括将所述入站数据报转发到商用货架产品COTS明文处理组件以处理所述入站数据报。

18.一种用于提供多安全链路MSL架构的非暂态计算机可读介质，包括程序，所述程序当由计算设备执行时使所述计算设备执行至少以下各项：

在客户端工作站与第一所有者网关之间创建第一VPN隧道；

从所述客户端工作站向所述第一所有者网关发送出站数据报；

接收从所述第一所有者网关到所述客户端工作站的入站数据报，其中所述入站数据报

包括源因特网协议IP地址和被设置为VPN所有者私有IP地址的目的地IP地址；

记录来自所述入站数据报中的所述源因特网协议IP地址的新的VPN所有者私有IP地址；

为所述入站数据报和所述客户端工作站指派新的独特私有IP(UPIP)地址;以及

向所述客户端工作站发送所述入站数据报，

其中所述程序在所述第一VPN隧道正被利用时在所述客户端工作站与第二所有者网关之间额外地创建第二VPN隧道。

19.如权利要求18所述的非暂态计算机可读介质,其中所述程序还使所述计算设备执行至少以下各项：

加密所述出站数据报并且将所述出站数据报传递到所述第一所有者网关;以及

从所述第一所有者网关接收加密形式的入站数据报并且解密所述入站数据报。

用于提供多安全链路架构的系统和方法

背景技术

[0001] 因特网当前支持使用各种标准协议的计算机之间的全球通信。这些协议之一——因特网协议(IP)——向每个计算机指派独特的地址,称作IP地址。IP当前在两个版本中可用:具有32位地址的IPv4和具有128位地址的IPv6。IPv4是当今在使用中的最常见版本。

[0002] 因特网的发展已经使用了IPv4中所有可用的32位地址。有限数量的地址的一个结果是大多数组织现在使用由IPv4定义的三个私有地址空间中的一个。这些私有IP地址不可以在公共因特网上使用。网关路由器管理专用内联网和公共因特网之间的接口。网关路由器提供各种功能以当期望在专用网外面的通信时隐藏或掩蔽(mask)私有内部IP。

[0003] 在商业环境中由网关路由器使用的一种常见方法是创建虚拟专用网(VPN)以将外部用户连接到内部专用网。VPN提供包封或包装协议,以当分组跨公共因特网路由至客户端工作站时隐藏内部IP地址和数据。

[0004] VPN通过在客户端工作站连接到VPN网关时向客户端工作站指派内部私有IP地址来扩展内部专用网。VPN创建将客户端工作站上的应用连接到VPN网关(或所有者网关)后面的内部专用网的网络或VPN隧道。客户端工作站的本地专用网和公共因特网通过VPN隧道对客户端工作站上的应用是隐藏的。结果,在VPN的当前版本中,客户端工作站一次仅可以连接到一个VPN。如果客户端工作站曾能够连接到多于一个VPN,那么由于不能保证每个VPN的内部私有地址域是独特的,因此不能将分组可靠地路由至期望的目的地。

发明内容

[0005] 本文中所公开的实施例包括一种用于提供多安全链路(MSL)架构的系统。该系统的一些实施例包括MSL虚拟专用网(VPN)组件,其包括第一逻辑,第一逻辑当由处理器执行时使该系统在客户端工作站与所有者网关之间创建VPN隧道、从客户端工作站向所有者网关发送出站数据报并且接收从所有者网关到客户端工作站的入站数据报,其中入站数据报包括源IP地址和被设置为VPN所有者私有IP地址的目的地因特网协议(IP)地址。在一些实施例中,第一逻辑使该系统发送具有目的地IP地址的入站数据报。该系统的实施例还可包括MSL双网络地址转换器(NAT),MSL双网络地址转换器包括第二逻辑,第二逻辑当由处理器执行时使该系统从MSL VPN接收入站数据报、记录来自入站数据报中的源IP地址的新的VPN所有者私有IP地址、为入站数据报和客户端工作站指派新的UPIP地址并且促进向客户端工作站发送入站数据报。

[0006] 类似地,本文中所公开的一些实施例包括MSL虚拟专用网(VPN)组件,其包括逻辑,该逻辑当由处理器执行时使该MSL VPN在客户端工作站与所有者网关之间创建VPN隧道并且从客户端工作站向所有者网关发送出站数据报。在一些实施例中,该逻辑使MSLVPN组件接收从所有者网关到客户端工作站的入站数据报,其中该入站数据报包括源IP地址和被设置为VPN所有者私有IP地址的目的地因特网协议(IP)地址,并且发送具有目的地IP地址的入站数据报。

[0007] 本文中所公开的另一些实施例包括MSL双网络地址转换器(NAT),其包括逻辑,该

逻辑当由处理器执行时使该MSL双NAT从MSL VPN接收入站数据报并且记录来自入站数据报中的源IP地址的新的VPN所有者私有IP地址。在一些实施例中，该逻辑使该MSL双NAT为入站数据报和客户端工作站指派新的UPIP地址并且促进向客户端工作站发送入站数据报。

[0008] 本公开的其他实施例和/或优点在查阅以下附图和具体实施方式之后对本领域技术人员将明显或者对本领域技术人员可变得明显。旨在使所有这些附加的系统、方法、特征和优点包含在本说明书中并且在本公开的范围内。

附图说明

[0009] 本公开的许多方面可参考以下附图而被更好的理解。附图中的组件不一定是成比例的，而是着重于清楚地例示本公开的原理。此外，在附图中，相似的附图标记贯穿若干视图指示对应的部分。尽管若干实施例是结合这些附图来描述的，但是没有将本公开限制于本文中所公开的一个或多个实施例的意图。相反，意图是覆盖所有的替代物、变型例和等同物。

[0010] 图1描绘了根据本文中所公开的实施例的用于在客户端工作站上提供多安全链路架构的计算环境；

[0011] 图2描绘了根据本文中所公开的实施例的用于在MSL服务器上提供多安全链路架构的计算环境；

[0012] 图3描绘了根据本文中所公开的实施例的用于在MSL网关路由器上提供多安全链路架构的计算环境；

[0013] 图4描绘了根据本文中所公开的实施例的用于在客户端工作站上提供多安全链路架构的计算环境；

[0014] 图5描绘了根据本文中所公开的实施例的用于在MSL网络操作中心(NOC)上提供多安全链路架构的计算环境；

[0015] 图6描绘了根据本文中所公开的实施例的登录管理器提供多安全链路架构的流程图；

[0016] 图7描绘了根据本文中所公开的实施例的会话管理器提供多安全链路架构的流程图；

[0017] 图8A、8B描绘了根据本文中所公开的实施例的多个组件提供多安全链路架构的流程图；以及

[0018] 图9描绘了根据本文中所公开的实施例的可被利用用于提供多安全链路架构的计算设备。

具体实施方式

[0019] 本文中所公开的实施例包括用于提供多安全链路架构的系统和/或方法。具体而言，每个VPN所有者利用VPN所有者定义的私有IPv4寻址来定义网络域。VPN所有者网络域预计具有重叠的地址，因为所有的VPN所有者可使用10.0.0.0/24作为其网络定义。本文中所公开的实施例定义了在分组在MSL服务内时要使用的内部网络域。MSL提供了在分组进入或离开MSL服务时将所有VPN所有者定义的私有IP地址转换为MSL独特私有IP(UPIP)域地址和从MSL独特私有IP(UPIP)域地址转换为所有VPN所有者定义的私有IP地址的双NAT功能。在

经处理的分组中发现VPN所有者服务器时向VPN所有者服务器动态地指派MSL UPIP域地址。

[0020] 当客户端工作站打开第一VPN连接时，指派给客户端工作站的VPN所有者私有IP或者客户端工作站的UPIP地址可被用作客户端工作站的IP地址。当第二(或者更晚的)VPN被打开时，先前用于工作站IP的IP地址可被用作工作站的UPIP并且新的UPIP被指派给来自第二VPN的服务器。客户端工作站应用与MSL UPIP通信。MSL源和目的地NAT在UPIP和VPN所有者私有IP之间变换以使得服务器仅看见VPN所有者私有IP地址。这允许客户端工作站同时地促进与不同所有者网关和/或VPN的多个独立VPN连接。

[0021] 在IPv6环境中，VPN所有者网络地址被生成为128位UPIP并且如在上面针对IPv4的段落中所述在IPv6中使用。由于独特本地IPv6单播地址具有极高概率是唯一的，因此MSL可以为工作站生成IPv6UPIP并且使用私有IPv6地址用于VPN所有者网关后面的节点。MSL必须核实每个新的IPv6VPN未复制已经打开的VPN的独特本地IPv6单播地址。如果复制被发现，则将为该VPN中的节点生成UPIP，如在上面针对IPv4的段落中所述。本地IPv6地址是使用伪随机分配的全局ID来创建的。一个实施例可以具有表格1中的以下格式。

[0022]

7位	1	40位	16位	64位
前缀	L	全局ID	子网ID	接口ID
1111110	1	伪随机		

[0023] 表格1

[0024] 现在参考附图，图1描绘了根据本文中所公开的实施例的用于在客户端工作站102上提供多安全链路架构的计算环境。如所例示的，MSL架构创建与公共因特网IP地址和VPN所有者的私有IP地址两者隔离的私有IP域或地址空间(MSL独特私有IP域)。

[0025] 如所例示的，图1中的架构包括客户端工作站102、第一VPN(VPN A 104a)和第二VPN(VPN B 104b)。客户端工作站102可包括用户应用A 108a和用户应用B 108b。用户应用108a、108b可被利用来与VPN A 104a和VPN B 104b通信。也被包括在客户端工作站102中的是MSL双NAT组件110、MSL VPN用户接口组件114和MSL管理组件116，其构成MSL UPIP域106。MSL VPN组件112也被包含在客户端工作站102中。该配置可以允许经由广域或公共网络118与VPN A 104a和/或VPN B 104b的VPN通信。公共网络118可包括因特网和/或其他公共可访问的网络。

[0026] 因此，客户端工作站102可包括多个组件，其可以或者可以不被包含在MSL独立客户端软件中。作为示例，MSL独立客户端软件的组件可包括MSL管理组件116，MSL管理组件116可操作作为用来保持客户端工作站102的会话信息的会话管理器。会话管理器可被配置为向MSL双NAT组件110指派UPIP并且提供UPIP协调信息。类似地，组件也可包括MSL用户接口组件114，MSL用户接口组件114提供一个或多个用户接口以使得用户可以识别VPN连接、删除VPN连接、打开VPN连接或者关闭打开的VPN连接。MSL VPN组件112可被利用来提供来自所有者网关120a、120b的外部分组上的源IP以识别所有者网关120a、120b和/或VPN 104a、104b。来自MSL双NAT组件110的分组可包括用来识别目的地网关/VPN的目的地公共IP。MSL双NAT组件110也被包含并且将明文分组中的源和目的地IP地址两者转换为指派的UPIP地址和/或从指派的UPIP地址转换为明文分组中的源和目的地IP地址两者。对于入站数据报(包括响应数据报)，MSL双NAT组件110使用由MSL VPN组件112提供的源IP来识别所有者网

关120a、120b。对于出站数据报，MSL双NAT组件110使用源和目的地UPIP来识别所有者网关120a、120b和/或VPN 104a、104b的目的地公共IP。

[0027] 因此，利用客户端工作站102中的组件，可以与VPN A 104a和VPN B 104b上的一个或多个计算设备进行安全通信。VPN A 104a可包括所有者网关120a，所有者网关120a经由本地网络122a而被耦接到一个或多个计算设备(诸如远程计算设备124a)。类似地，VPN B104b还可包括所有者网关120b，所有者网关120b促进经由本地网络122b与诸如远程计算设备124b之类的一个或多个远程计算设备的通信。

[0028] 多安全链路架构为使用MSL技术与客户端工作站102通信的每个主机(诸如远程计算设备124a、124b、服务器等)指派独特私有IP地址(UPIP)，以使得所有的用户组织主机(系统)在MSL私有IP域106内具有独特IP地址。MSL架构提供了用来管理MSL私有IP域106的双NAT功能。MSL双NAT 110在VPN所有者指派的私有IP地址和指派的UPIP之间转换，以使得即使当多个VPN所有者具有相同的私有IP地址时工作站对于所有VPN所有者主机也具有独特的IP地址。

[0029] 因此，用户应用A 108a和用户应用B 108b看见UPIP，而VPN所有者主机仅看见VPN所有者的内部私有IP地址。MSL双NAT 110被协调以在VPN所有者指派的私有IP地址与MSL架构指派的UPIP之间转换，以使得用户应用A 108a和用户应用B 108b看见UPIP并且VPN所有者的主机仅看见VPN所有者的内部私有IP地址。

[0030] 客户端工作站102使用MSL用户接口和管理功能连接到VPN A104a。MSL管理组件116向包括远程计算设备124a的VPN A 104a节点指派UPIP。客户端工作站102现在可以以通常的方式访问VPN A104a。

[0031] 客户端工作站102可使用MSL用户接口组件114和MSL管理组件116而另外连接到VPN B 104b。MSL管理组件116向VPN B 104b上的节点(诸如远程计算设备124b)指派UPIP。由于VPN A 104a已经向客户端工作站102指派了UPIP，因此MSL管理组件116使用相同的UPIP值用于VPN B 104b IP。客户端工作站102现在可以以通常的方式利用用户应用108a、108b来访问计算设备，诸如VPN B104b上的远程计算设备124b。

[0032] 下面的表格2示出了IP地址指派的示例。应当注意到，IP可能是为了简化对指派的追踪而选择的。

[0033]

	VPN所有者私有IP	MSL UPIP
VPN A服务器	10.0.0.10	192.168.0.10
VPN A工作站	10.0.1.1	192.168.1.1
VPN B服务器	10.0.2.20	192.168.2.20
VPN B工作站	10.0.3.30	192.168.1.1

[0034] 表格2

[0035] 客户端工作站102被指派当客户端工作站102登录到VPN A 104a时生成的UPIP。当客户端工作站102登录到VPN B 104b上时，VPNB 104b后面的计算设备被指派UPIP但是客户端工作站102继续使用为VPN A 104a生成的工作站UPIP。应当理解，用户应用108a、108b现在在MSL UPIP域106中操作。

[0036] 图2描绘了根据本文中所公开的实施例的用于在MSL服务器204上提供多安全链路

架构的计算环境。如所例示的，图2的实施例包括客户端工作站202、MSL服务器204、VPN A 206a和VPN B 206b。客户端工作站202可包括用户应用A 210a、用户应用B 210b、商用货架产品(COTS)明文处理客户端212、第一MSL VPN组件214、MSL VPN用户接口组件216和第一MSL管理组件218。这些组件可包括MSL UPIP域208，并且可被配置为经由诸如因特网之类的公共网络220建立与VPN A 206a和/或VPN B 206b的VPN通信。

[0037] 为了促进该通信，MSL服务器204可包括COTS VPN组件224、COTS明文处理组件226、MSL双NAT组件228和第二MSL管理组件230，其也是MSL UPIP域208的部分。第二MSL VPN组件232也可被包含。因此，这些组件也可以远离VPN A 206a和/或VPN B206b，并且可以将一个或多个数据报发送到所有者网关234a、234b，所有者网关234a、234b被耦接到本地网络122a、122b用于发送和/或接收来自VPN A 206a和/或VPN B 206b上的远程计算设备238a、238b和/或其他计算设备的数据。

[0038] 因此，除了图2的实施例利用远离客户端工作站202的MSL服务器204之外，图2的实施例可以类似于关于图1描述的那样来操作。因此，该配置将MSL UPIP域208扩展到MSL服务器204，其可以容宿诸如加速之类的COTS明文功能，以使得COTS明文功能可被应用于由多个不同客户端工作站使用的每个VPN。另外，提供了连接MSL服务器204和客户端工作站202的COTS VPN组件224，以在数据通过公共网络220在客户端工作站202和MSL服务器2044之间移动时保护该数据。

[0039] 图3描绘了根据本文中所公开的实施例的用于在MSL网关路由器304上提供多安全链路架构的计算环境。如所例示的，图3的实施例包括客户端工作站302、MSL网关路由器304、VPN A 306a和VPNB 306b。客户端工作站302包括用户应用A 310a、用户应用B 310b、第一COTS VPN组件314、MSL VPN用户接口组件316和MSL管理组件318，其构成MSL UPIP域308的一部分。

[0040] 因此，客户端工作站302可以经由本地和/或专用网320与MSL网关路由器304通信。MSL网关路由器304可包括第二COTS VPN组件322、MSL双NAT组件324和MSL服务器管理组件326，其也是MSL UPIP域308的部分。MSL VPN 328也与MSL网关路由器304一起被包含，并且可以促进经由公共网络330与VPN A 306a和/或VPN B 306b的通信。

[0041] 如上面关于其他VPN讨论的，VPN A 306a包括被耦接到专用网334a的所有者网关332a。专用网334a可被耦接到一个或多个计算设备，诸如远程计算设备336a。类似地，VPN B 306b包括被耦接到专用网334b的所有者网关332a。专用网334b可被耦接到一个或多个计算设备，诸如远程计算设备336b。

[0042] 因此，图3的实施例将MSL UPIP域308扩展到MSL网关路由器304，MSL网关路由器304支持多个客户端工作站。这种配置在单个组件可被利用用于多个客户端工作站的情况下(诸如在学校网络、商业网络等处)可以是经济的。另外，COTS VPN组件332被耦接到客户端工作站302以在数据通过专用网320在工作站与MSL路由器之间移动时保护该数据。

[0043] 还应当理解，尽管用户应用310可以是完全独立地操作的多个分离的应用，这只是一个实施例。具体而言，一些实施例被配置使得共用的浏览器应用可以通过显示不同的标签或页面而充当应用A 310a和应用B 310b两者。

[0044] 图4描绘了根据本文中所公开的实施例的用于在客户端工作站402上提供多安全链路架构的计算环境。如所例示的，图4的实施例包括客户端工作站402、MSL装置404、MSL服

务器406、VPN A 408a和VPN B 408b。客户端工作站402可包括用户应用A 412a、用户应用B 412b、第一COTS VPN组件414以及MSL VPN用户接口组件418，其构成MSL UPIP域410的一部分。另外，客户端工作站402可以经由加密隧道和/或在专用网416上以加密形式被耦接到MSL装置404。

[0045] MSL装置404可包括第二COTS VPN组件422、第一COTS明文处理客户端424、第三COTS VPN组件426和第一MSL服务器管理组件430，其也是MSL UPIP域410的部分。MSL装置404可被耦接到公共网络428用于经由MSL服务器406与VPN408a、408b通信。

[0046] 还被耦接到公共网络428的是MSL服务器406。MSL服务器406包括第四COTS VPN组件432、COTS明文处理434和第二MSL服务器管理组件438，其也是MSL UPIP域410的部分。MSL VPN组件439也是MSL服务器406的部分并且被耦接到公共网络428。

[0047] 还被耦接到公共网络428的是VPN A 408a和VPN B 408b。VPNA 408a包括所有者网关440a、专用网442a以及一个或多个计算设备，诸如远程计算设备444a。VPN B 408b包括所有者网关440b、专用网442b以及一个或多个计算设备，诸如远程计算设备444b。

[0048] 因此，图4的实施例提供了将MSL UPIP域410扩展到支持多个不同客户端工作站(类似于图3)的MSL装置404的实现方式，但是也利用MSL服务器406。应当理解，在一些实施例中，MSL装置404可被实现在支持小办公室的网关路由器中。另外，第三COTS VPN组件426和第四COTS VPN组件432被耦接在MSL服务器406和MSL装置404之间，以在数据通过公共网络428在MSL装置404和MSL服务器406之间移动时保护该数据。第一COTS VPN组件414和第二COTS VPN组件422被设置在MSL装置404和客户端工作站402之间，以在数据通过专用网416在客户端工作站402和MSL装置404之间移动时保护该数据。

[0049] 图5描绘了根据本文中所公开的实施例的用于在MSL网络操作中心(NOC)504上提供多安全链路架构的计算环境。如所例示的，图5的实施例包括客户端工作站502、MSL网络操作中心(NOC)504、VPN A 506a和VPN B 506b。COTS组件包括：COTS VPN和COTS明文处理。

[0050] 客户端工作站502包括用户应用A 510a和用户应用B 510b。作为MSL客户端逻辑的部分也被包含在客户端工作站502中的是COTS明文处理客户端512、COTS VPN客户端514、MSL VPN用户接口组件516和MSL管理组件518。这些组件构成MSL私有IP域508的部分。

[0051] 将客户端工作站502与MSL NOC 504耦接的是公共网络520。因此，MSL NOC 504包括COTS VPN组件524、COTS明文处理组件526、MSL双NAT组件528、登录管理器组件529和会话管理器组件530，其也是MSL私有IP域508的部分。MSL VPN组件531也是MSL NOC 504的部分。COTS明文处理组件526可被实现为网络加速产品并且可被实现为对明文分组进行操作以为用户客户提供服务的未修改的功能。

[0052] 另外，一些实施例包括客户端工作站502上的客户端会话管理器，其与会话管理器组件530通信并且保持客户端工作站502的会话信息。VPN A 506a和VPN B 506b包括所有者网关532a、532b、专用网534a、534b以及远程计算设备536a、536b。会话管理器组件530可被配置为保持登入服务的每个客户端工作站的会话信息。会话管理器组件530可以向MSL双NAT组件528提供UPIP协调信息，并且可以利用每个所有者网关532a、532b的指派的UPIP来更新客户端会话管理器。会话管理器也可被配置为保持所有者网关532a、532b和/或VPN 506a、506b的UPIP和公共IP之间的关系。登录管理器组件529可被配置为处理来自客户端登录管理器(其可以是MSL管理组件518的部分)的登录请求以验证对服务的客户端访问并建

立VPN隧道。

[0053] 如上所述，MSL VPN组件531可被利用来提供来自所有者网关532a、532b的外部分组上的源IP以识别源网关和/或VPN。相比之下，来自MSL双NAT组件528的出站数据报包括用来识别目的地网关和/或VPN的目的地公共IP。MSL VPN用户接口组件516管理客户端工作站502的启动处理。MSL VPN用户接口组件516与登录管理器通信以验证客户端许可证并且建立到MSL NOC 504的VPN。另外，MSL VPN用户接口组件516可被配置为使用会话管理器组件530来启动和关闭由客户端工作站502所请求的每个VPN连接。

[0054] 类似地，MSL双NAT组件528可被配置为将明文分组中的源和目的地IP地址两者转换为指派的UPIP地址和/或从指派的UPIP地址转换为明文分组中的源和目的地IP地址两者。对于入站分组，MSL双NAT组件528使用由MSL VPN组件531提供的源IP来识别VPN所有者。对于出站分组，MSL双NAT组件528利用源和目的地UPIP来识别用于目的地网关和/或VPN的目的地公共IP。应当理解，在MSL双NAT组件528与MSL VPN组件531之间的链路上，分组可被以包括公共源和目的地IP的私有MSL架构定义的IP协议包装。还应当理解，本文所描述的实施例可以指派与客户指派的私有IP地址重叠的UPIP。这不会产生路由问题，因为指派的地址在MSL私有IP域508内是独特的并且被会话管理器组件530映射到所有者网关532a、532b的公共IP。如将会理解的，本文所描述的实施例可被配置为使得在VPN所有者的网络中将不需要变化。

[0055] 应当理解，尽管在上面描述的一些实施例中，描绘了单个工作站。尽管这样的实施例可以支持一个工作站，但是上面描述的每个实施例取决于特定配置可被配置用于容纳多个工作站。

[0056] 图6描绘了根据本文中所公开的实施例的登录管理器提供多安全链路架构的流程图。如在方框652中例示的，登录管理器可以验证用于访问系统的许可证ID。在方框654中，可以识别要服务的客户。在方框656中，会话管理器可被利用来创建用来追踪用户的会话。在方框658中，COTS VPN组件可被利用来创建VPN隧道以创建到客户端工作站的VPN隧道，并且向客户端工作站指派许可证ID的UPIP。在方框660中，可以利用指派给许可证的UPIP到客户私有IP映射来更新客户端工作站上的客户端会话管理器。在方框662中，MSL VPN可被利用来创建到客户端网关的VPN隧道。在方框664中，可以向客户端工作站提供指示系统准备好的消息并且提供所请求的服务。

[0057] 图7描绘了根据本文中所公开的实施例的会话管理器提供多安全链路架构的流程图。如在方框752中例示的，可以利用指派给许可证的UPIP来更新客户端工作站上的客户端会话管理器。在方框754中，MSL VPN组件可被利用来创建到客户端网关的VPN隧道。在方框756中，对用户登入客户端网关的仿真可被执行。在方框758处，客户VPN登录页面可被发送回用户接口用于用户输入登录凭证。在方框760中，可以利用登录结果来更新客户端会话管理器。在方框762处，可以利用用于所有者网关的UPIP来更新MSL双NAT组件。

[0058] 图8A、8B描绘了根据本文中所公开的实施例的多个组件提供多安全链路架构的流程图。如在图8A中的方框850中例示的，用户应用可以基于用户输入创建请求数据报。在方框852中，COTS处理客户端处理该数据报。在方框854中，COTS VPN客户端和COTS VPN将该数据报传递到MSL NOC。在方框856中，COTS明文处理处理该数据报并且为VPN所有者服务器生成新数据报。在方框858中，MSL双NAT将数据报中的UPIP地址映射到客户定义的私有IP地

址。在方框860中，MSL VPN可以加密新数据报并且随后将新数据报传递到所有者网关。在方框862中，所有者网关解密新数据报并且将新数据报转发到VPN所有者远程计算设备用于处理。在方框864中，VPN所有者远程计算设备为做出请求的客户端工作站生成具有设置为VPN所有者私有IP的目的地IP地址的响应数据报。在方框866中，VPN所有者网关加密响应数据报并且将响应数据报转发到MSLVPN组件。在方框868中，MSL VPN解密响应数据报并且将具有原始源IP地址的响应数据报转发到MSL双NAT。

[0059] 在图8B中的方框870中继续，MSL双NAT将响应数据报中的VPN所有者定义的私有IP地址映射到UPIP地址。在方框872中，MSL双NAT将来自解密后的响应数据报中的源IP的新VPN所有者私有IP记录在会话管理器中并且指派新UPIP。在方框874中，MSL双NAT将响应数据报转发到COTS明文处理组件。在方框876中，COTS明文处理组件处理响应数据报并且为用户应用生成新的响应数据报。在方框878中，COTS VPN和COTS VPN客户端将新的响应数据报传递到客户端工作站。在方框880中，COTS处理客户端处理新的响应数据报。在方框882中，用户应用将新的响应数据报中的结果呈现给用户。

[0060] 图9描绘了根据本文中所公开的实施例的可被利用用于提供多安全链路架构的计算设备。在例示的实施例中，MSL服务器204包括一个或多个处理器930、输入/输出硬件932、网络接口硬件934、数据存储组件936(其存储登录数据938a和会话数据938b)以及存储器组件940。存储器组件940可以被配置为易失性和/或非易失性存储器，并且因此可包括随机存取存储器(包括SRAM、DRAM和/或其他类型的RAM)、闪存、寄存器、紧凑盘(CD)、数字通用盘(DVD)和/或其他类型的非暂态计算机可读介质。取决于特定实施例，非暂态计算机可读介质可以驻留于MSL服务器204内和/或MSL服务器204外部。

[0061] 另外，存储器组件940可被配置为存储操作逻辑942、MSL VPN逻辑944a、MSL双NAT逻辑944b以及诸如上述的其他逻辑，它们中的每个作为示例可以实施为计算机程序、固件和/或硬件。本地通信接口946也包含在图9中，并且可以实现为总线或其他接口以促进MSL服务器204的组件之间的通信。

[0062] 处理器930可包括可操作以接收并执行(诸如来自数据存储组件936和/或存储器组件940)的指令的任何处理组件。输入/输出硬件932可包括监视器、键盘、鼠标、打印机、照相机、麦克风、扬声器和/或用于接收、发送和/或呈现数据的其他设备，并且/或者可被配置为与上述各项相接口。网络接口硬件934可包括任何有线或无线的联网硬件、卫星、天线、调制解调器、LAN端口、无线保真(Wi-Fi)卡、WiMax卡、移动通信硬件、光纤和/或用于与其他网络和/或设备通信的其他硬件，并且/或者可被配置用于与上述各项通信。根据该连接，可以促进在MSL服务器204与如上所述的其他计算设备之间的通信。

[0063] 类似地，应当理解，数据存储组件936可驻留于MSL服务器204本地和/或远离MSL服务器204，并且可被配置为存储用于由MSL服务器204和/或其他组件访问的一条或多条数据。在一些实施例中，数据存储组件936可位于远离MSL服务器204，并且从而可经由网络连接访问。然而在一些实施例中，数据存储组件936可以仅是外围设备，但是在MSL服务器204外部。

[0064] 包含在存储器组件940中的是操作逻辑942、MSL VPN逻辑944a和MSL双NAT逻辑944b以及其他逻辑944c。操作逻辑942可包括用于管理MSL服务器204的组件的操作系统和/或其他软件。类似地，MSL VPN逻辑944a可包括用于执行上述MSL VPN功能的逻辑。MSL双NAT

逻辑944b可包括用于执行上述MSL双NAT功能的逻辑。其他逻辑944c被包含于此以表示上述的其他逻辑和功能。

[0065] 应当理解，图9中例示的组件仅是示例性的，并且并非旨在限制本公开的范围。虽然图9中的组件被例示为驻留于MSL服务器204内，但是这仅是示例。在一些实施例中，组件中的一个或多个可以驻留于MSL服务器204外部。还应当理解，虽然在图9中描绘了MSL服务器204，但是图1-图6或其他附图中描述的其他计算设备可包括用于提供所描述功能的类似硬件和软件。作为示例，客户端工作站102、202、302、402和/或502可包括上面描述的硬件和软件组件中的一些或者全部。因此，在可适用的程度上，图1-图6中描述的组件可被实施为在包括必要硬件的计算设备内执行的逻辑和/或软件，其中的一些在图9中表示出。

[0066] 应当注意到，本文中所包含的流程图显示了软件的可能的实现方式的架构、功能和操作。在这点上，每个方框可被解释为代表模块、片段或者代码部分，代码部分包括用于实现一个或多个指定的逻辑功能的一个或多个可执行指令。还应当注意到，在一些替代实现方式中，在方框中标注的功能可能不按次序发生和/或毫不发生。例如，取决于所涉及的功能，连续显示的两个方框可能实际上被实质上同时地执行，或者所述方框可能有时以倒序执行。

[0067] 应当强调的是，上面描述的实施例仅仅是实现方式的可能示例，仅仅是为了清楚理解本公开的原理而阐述。在实质上不偏离本公开的精神和原理的情况下可对上面描述的一个或多个实施例做出许多变型和修改。此外，本公开的范围旨在覆盖上面讨论的所有元素、特征和方面的所有排列和子排列。本文中所有这样的修改和变型旨在被包含在本公开的范围内。

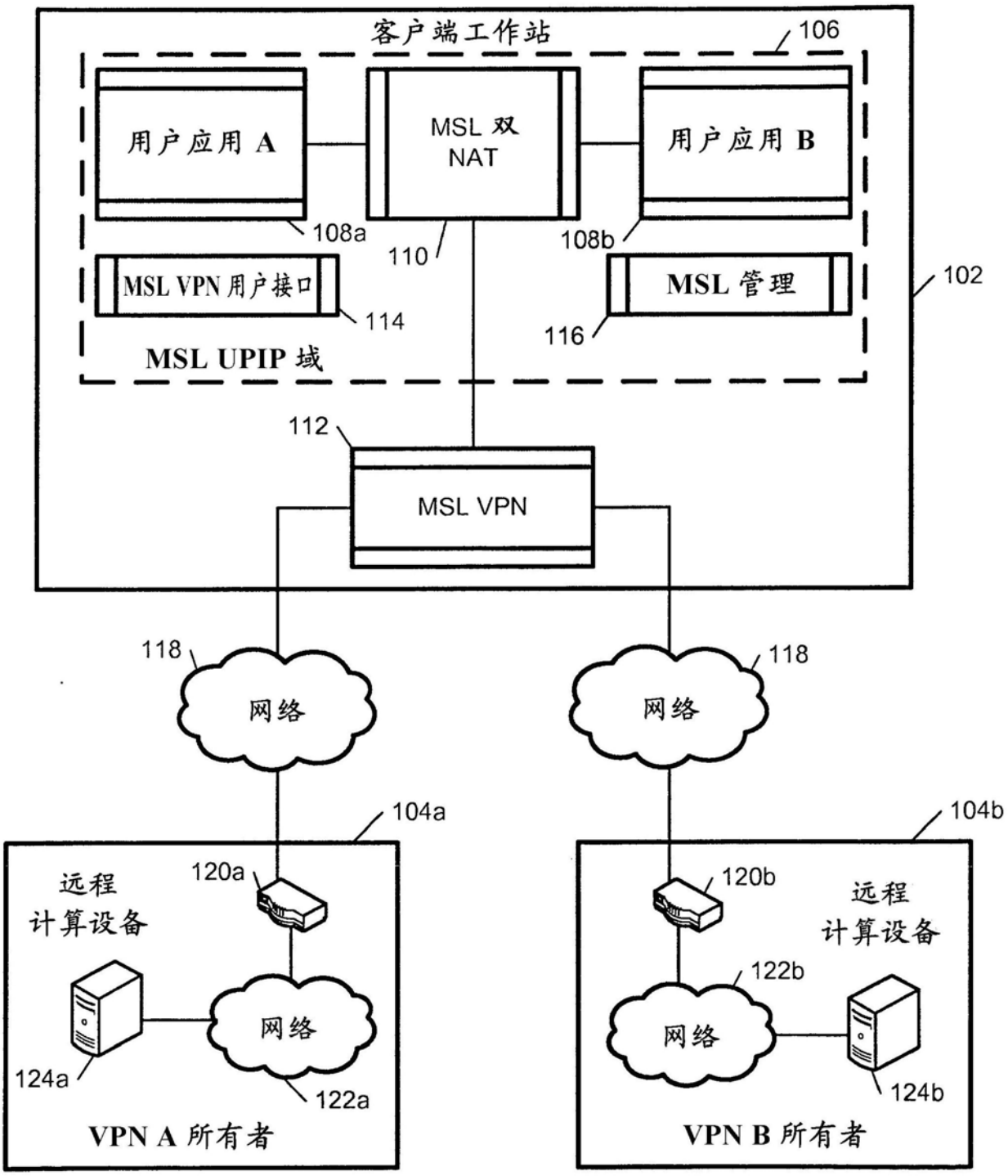

客户端工作站
106
用户应用 A
MSL 双
NAT
用户应用 B
108a
110
108b
MSL VPN 用户接口
114
MSL 管理
116
102
MSL UPIP 域
112
MSL VPN
118
网络
118
网络
104a
104b
远程
计算设备
120a
120b
远程
计算设备
122b
网络
网络
124a
122a
124b
VPN A 所有者
VPN B 所有者

图1

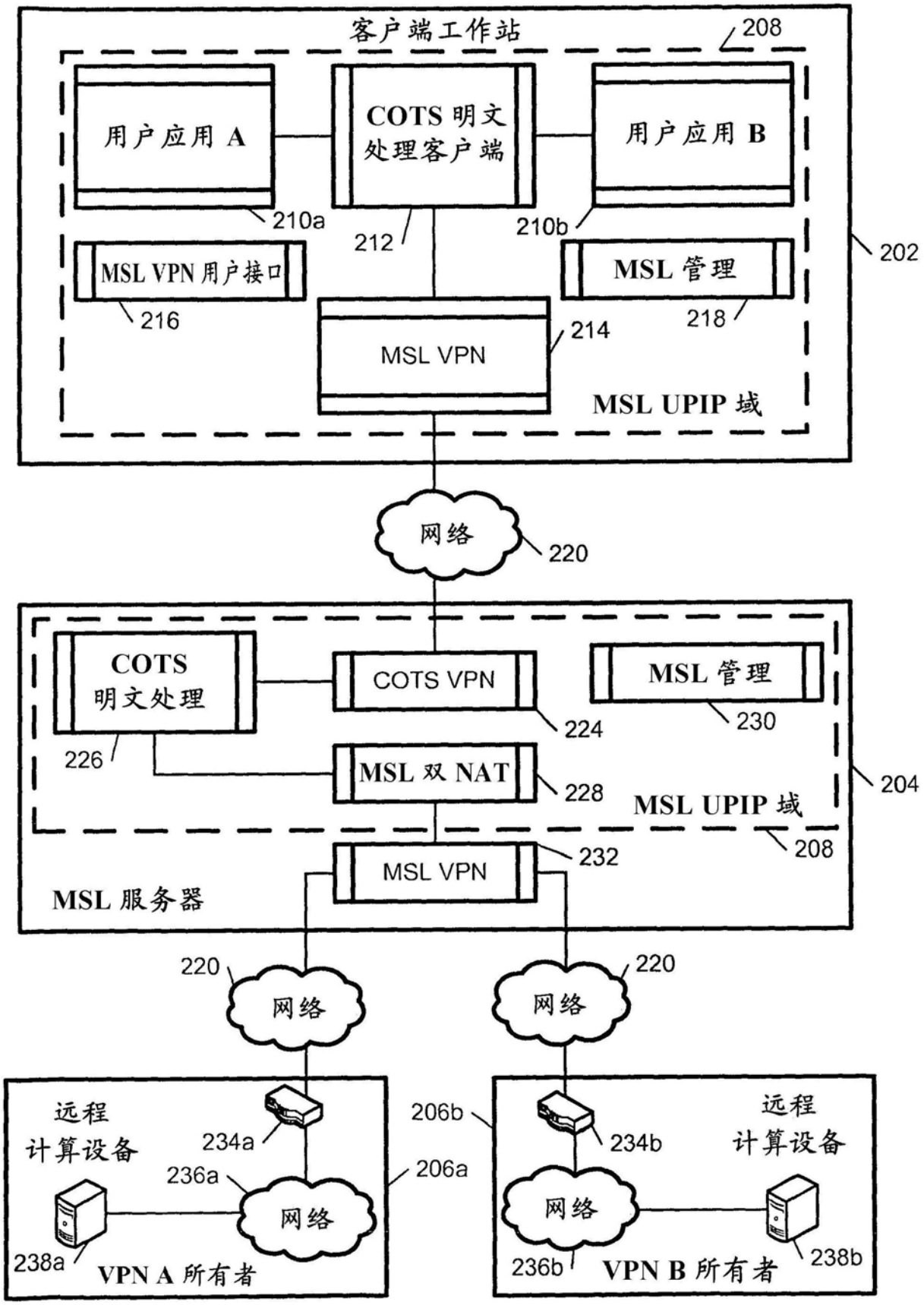

客户端工作站
208
用户应用 A
COTS 明文处理客户端
用户应用 B
210a
212
210b
202
MSL VPN 用户接口
216
MSL 管理
218
MSL VPN
214
MSL UPIP 域
网络
220
COTS 明文处理
COTS VPN
MSL 管理
224
230
226
MSL 双 NAT
228
204
MSL UPIP 域
208
232
MSL VPN
MSL 服务器
220
网络
220
网络
远程计算设备
234a
206b
234b
远程计算设备
236a
206a
网络
网络
238a
VPN A 所有者
236b
VPN B 所有者
238b

图2

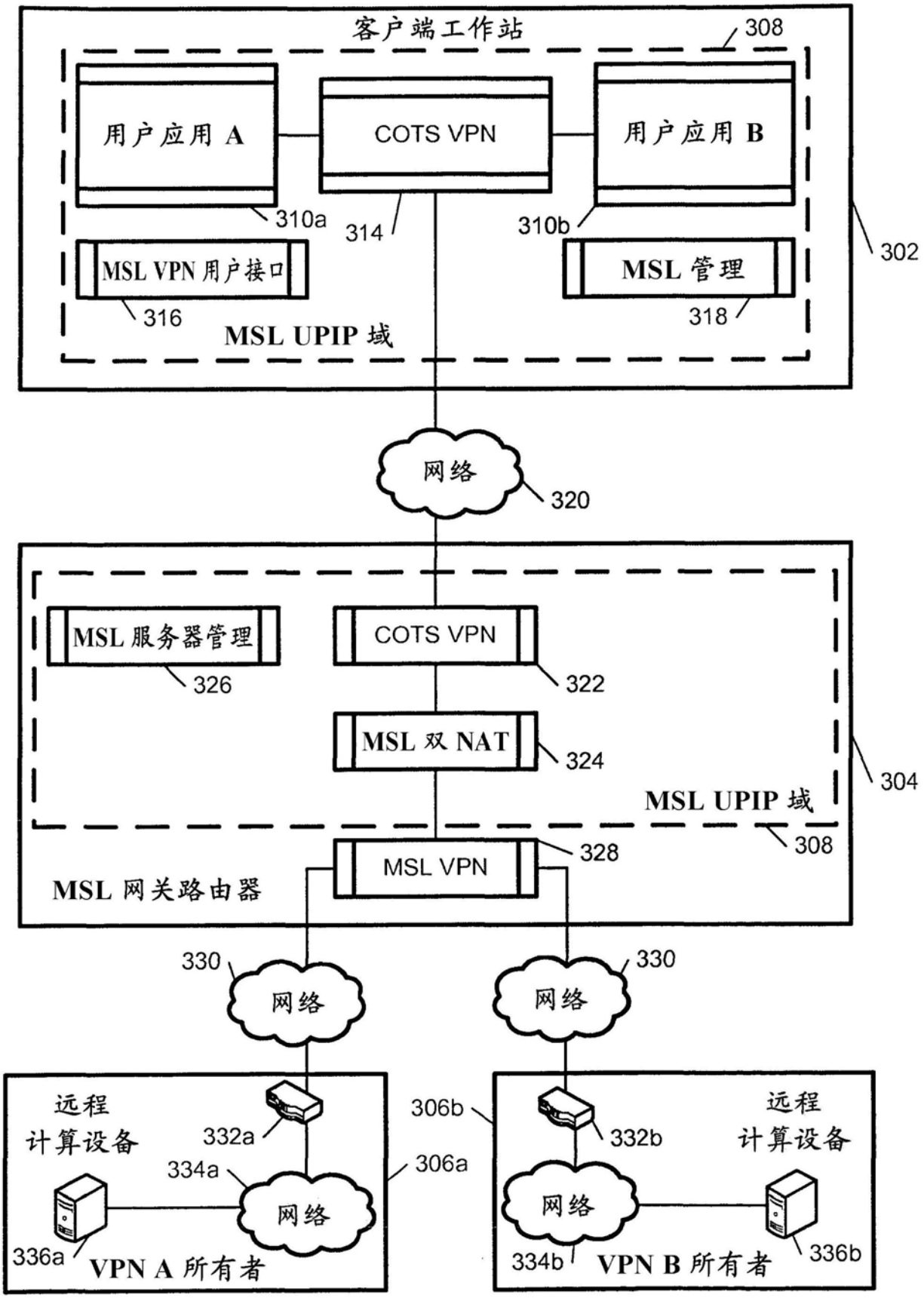

客户端工作站
308
用户应用 A
COTS VPN
用户应用 B
310a
314
310b
302
MSL VPN 用户接口
316
MSL 管理
318
MSL UPIP 域
网络
320
MSL 服务器管理
326
COTS VPN
322
MSL 双 NAT
324
304
MSL UPIP 域
308
328
MSL VPN
MSL 网关路由器
330
网络
330
网络
远程
计算设备
332a
306b
332b
远程
计算设备
334a
306a
网络
网络
336a
VPN A 所有者
334b
VPN B 所有者
336b

图3

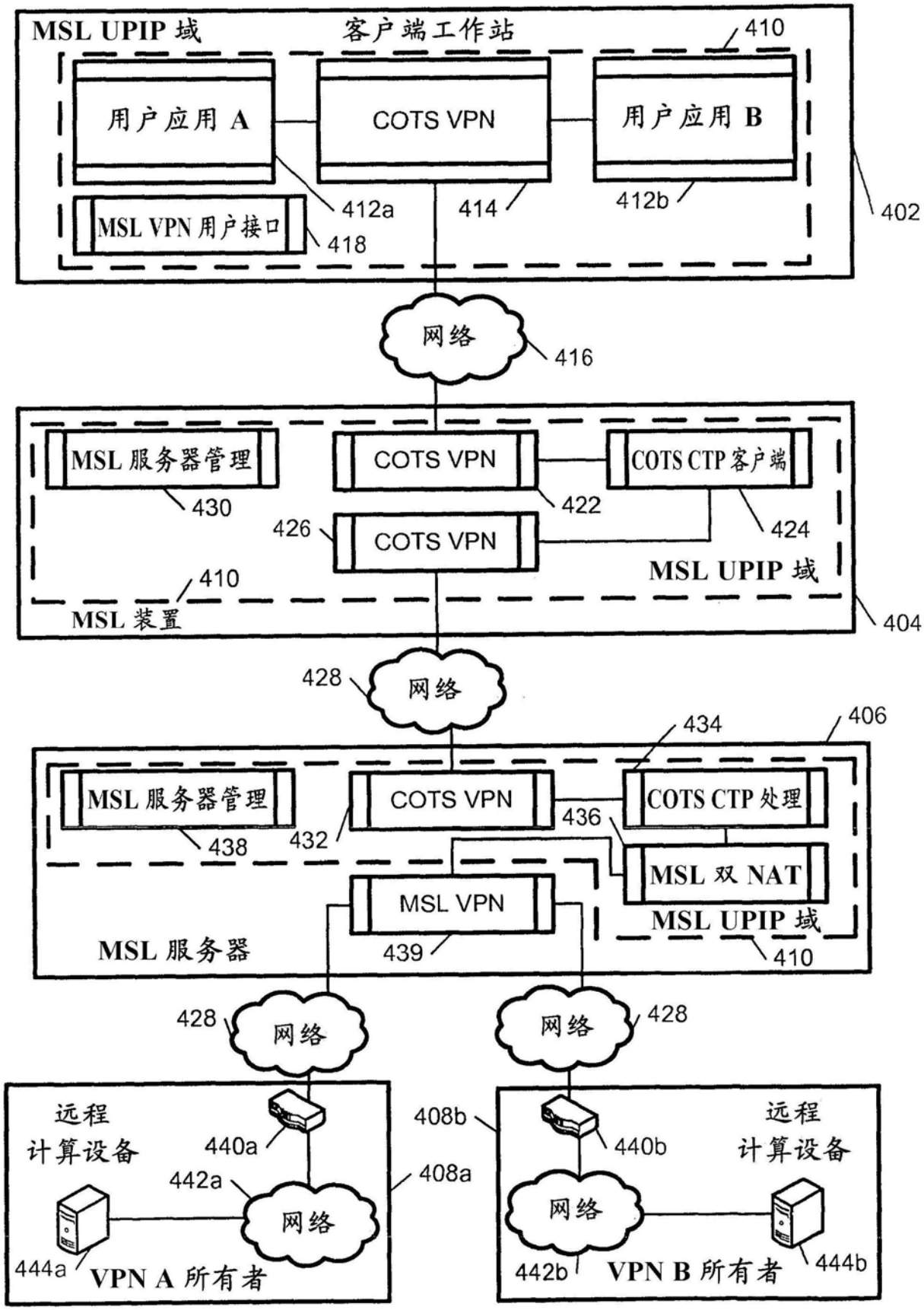

MSL UPIP 域
客户端工作站
410
用户应用 A
COTS VPN
用户应用 B
412a
414
412b
402
MSL VPN 用户接口
418
网络
416
MSL 服务器管理
COTS VPN
COTS CTP 客户端
430
422
424
426
COTS VPN
MSL UPIP 域
410
MSL 装置
404
428
网络
406
434
MSL 服务器管理
COTS VPN
COTS CTP 处理
438
432
436
MSL 双 NAT
MSL VPN
MSL UPIP 域
MSL 服务器
439
410
428
网络
网络
428
远程
计算设备
440a
408b
440b
远程
计算设备
442a
408a
网络
网络
444a
VPN A 所有者
442b
VPN B 所有者
444b

图4

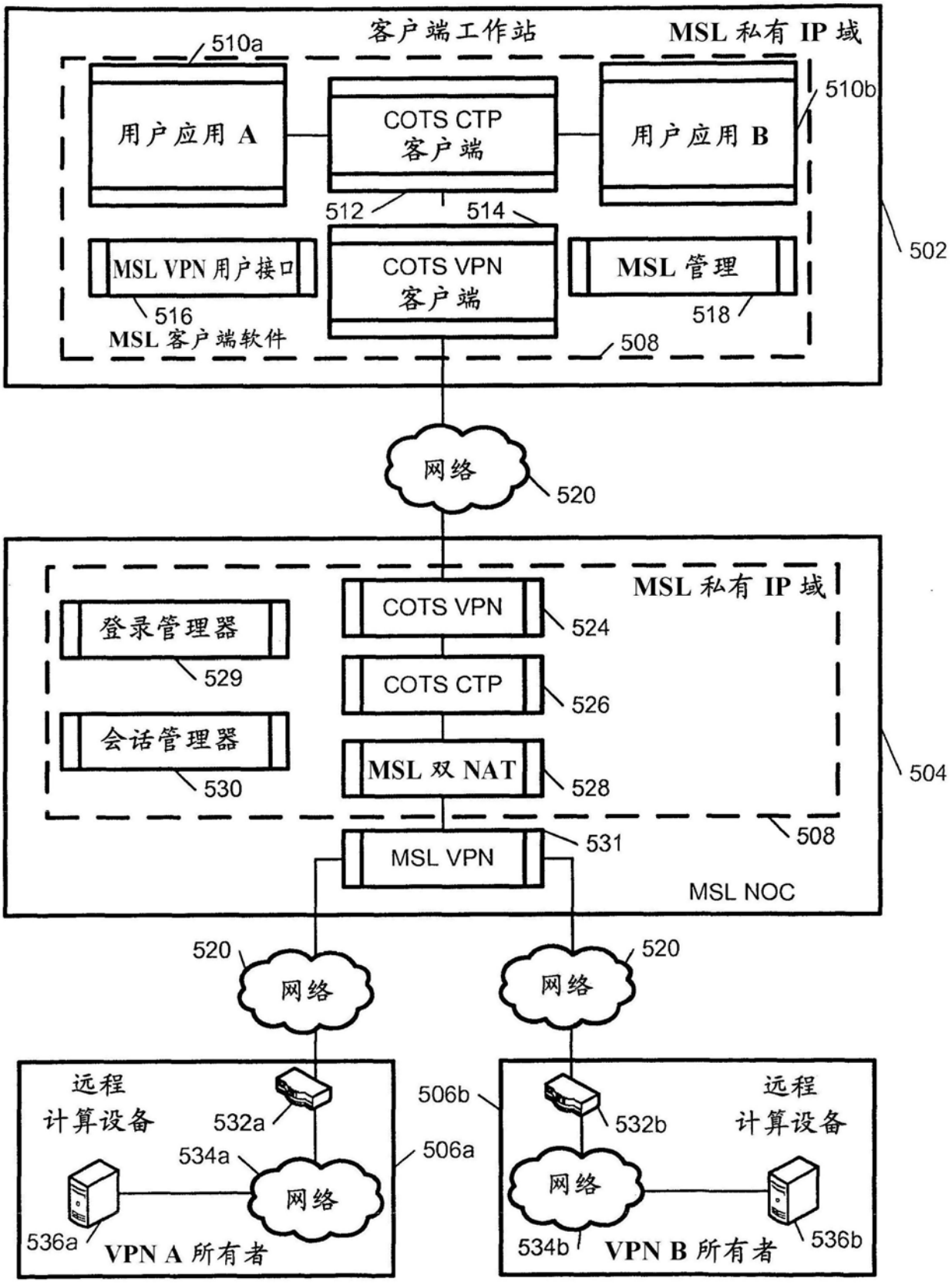

客户端工作站
MSL 私有 IP 域
510a
用户应用 A
COTS CTP
客户端
用户应用 B
510b
512
514
MSL VPN 用户接口
516
COTS VPN
客户端
MSL 管理
518
MSL 客户端软件
508
502
网络
520
MSL 私有 IP 域
登录管理器
529
COTS VPN
524
COTS CTP
526
会话管理器
530
MSL 双 NAT
528
504
508
MSL VPN
531
MSL NOC
520
网络
520
网络
远程
计算设备
532a
506b
532b
远程
计算设备
534a
506a
网络
网络
536a
VPN A 所有者
534b
VPN B 所有者
536b

图5

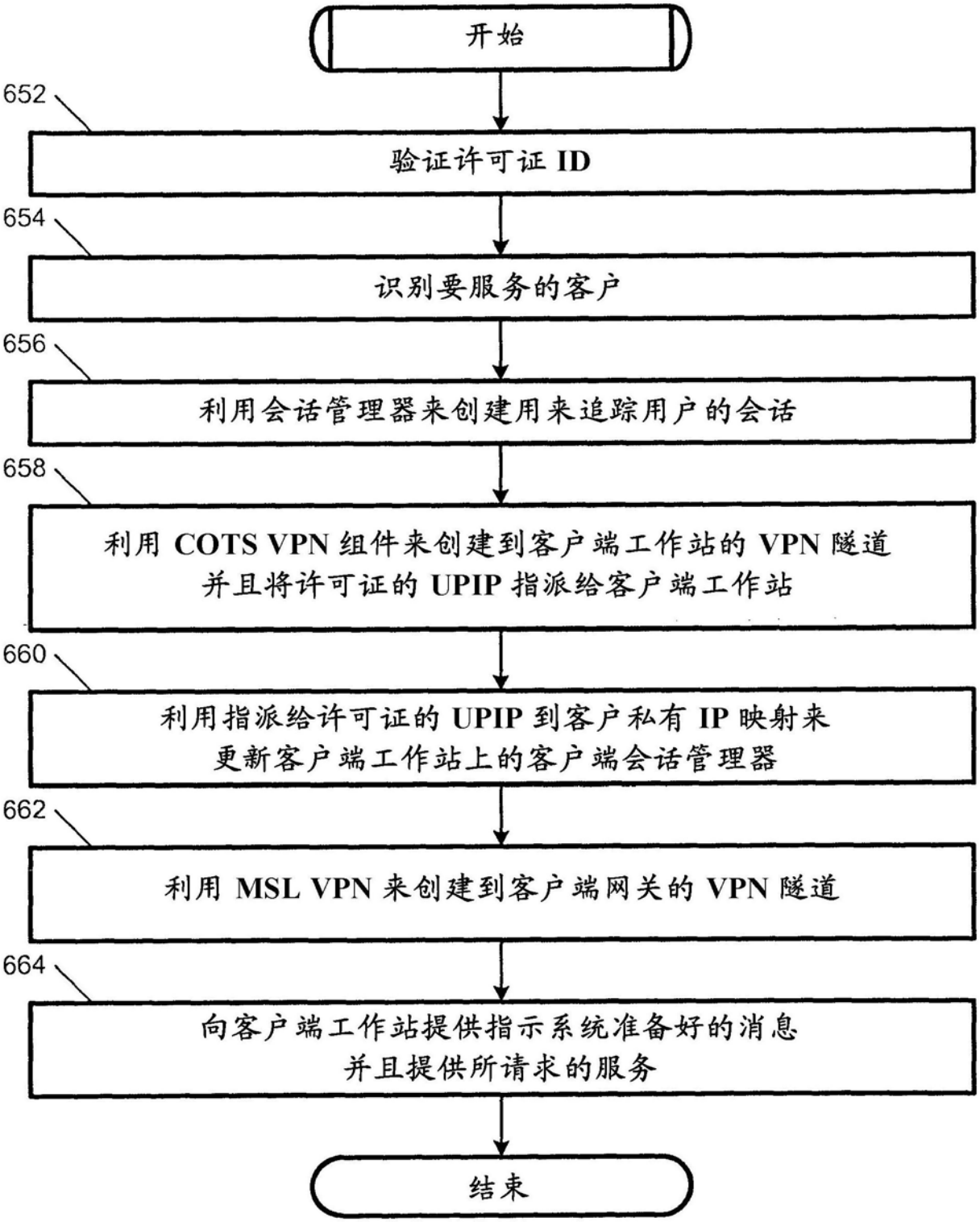

开始
652
验证许可证 ID
654
识别要服务的客户
656
利用会话管理器来创建用来追踪用户的会话
658
利用 COTS VPN 组件来创建到客户端工作站的 VPN 隧道
并且将许可证的 UPIP 指派给客户端工作站
660
利用指派给许可证的 UPIP 到客户私有 IP 映射来
更新客户端工作站上的客户端会话管理器
662
利用 MSL VPN 来创建到客户端网关的 VPN 隧道
664
向客户端工作站提供指示系统准备好的消息
并且提供所请求的服务
结束

图6

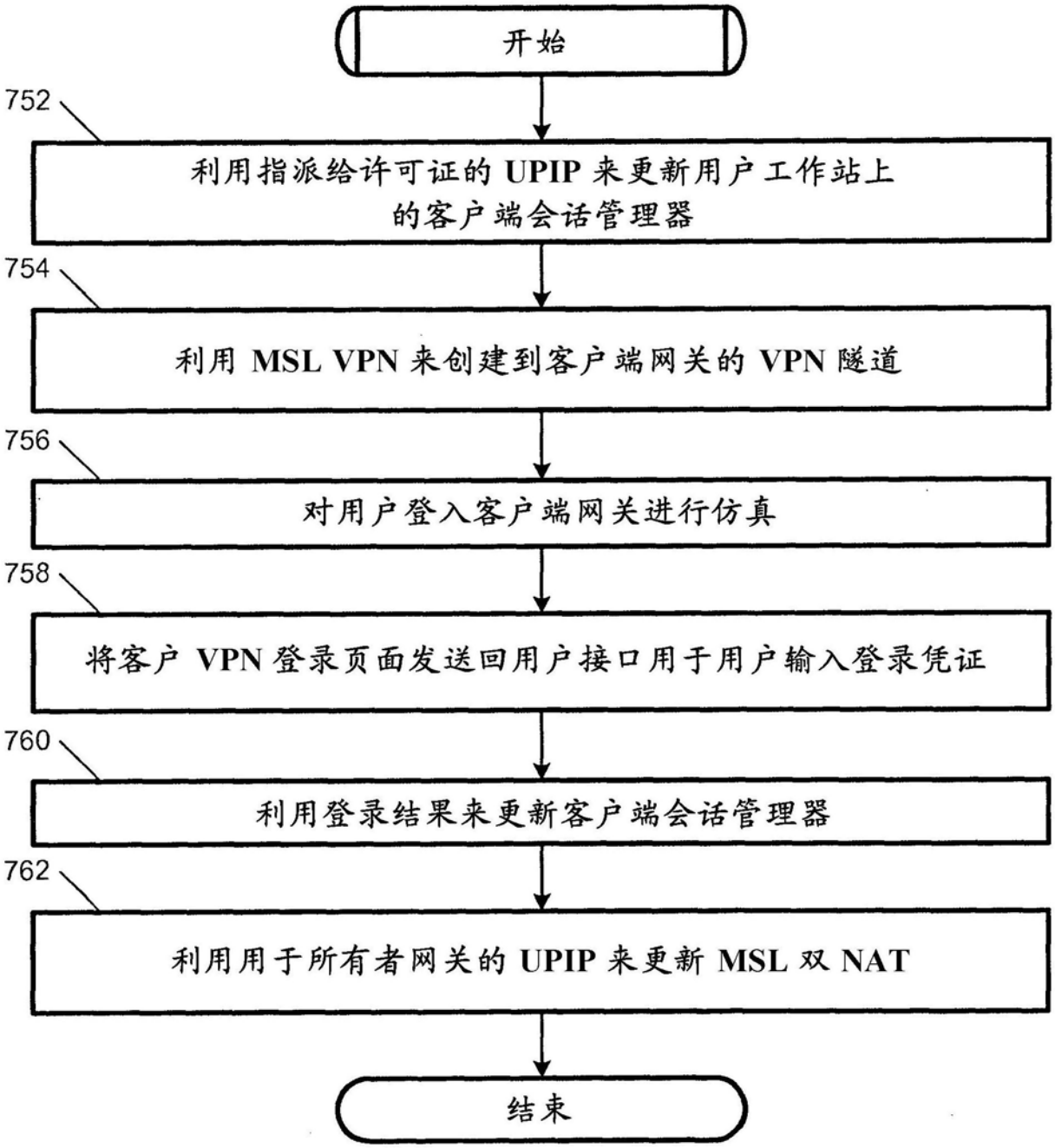

开始
752
利用指派给许可证的 UPIP 来更新用户工作站上的客户端会话管理器
754
利用 MSL VPN 来创建到客户端网关的 VPN 隧道
756
对用户登入客户端网关进行仿真
758
将客户 VPN 登录页面发送回用户接口用于用户输入登录凭证
760
利用登录结果来更新客户端会话管理器
762
利用用于所有者网关的 UPIP 来更新 MSL 双 NAT
结束

图7

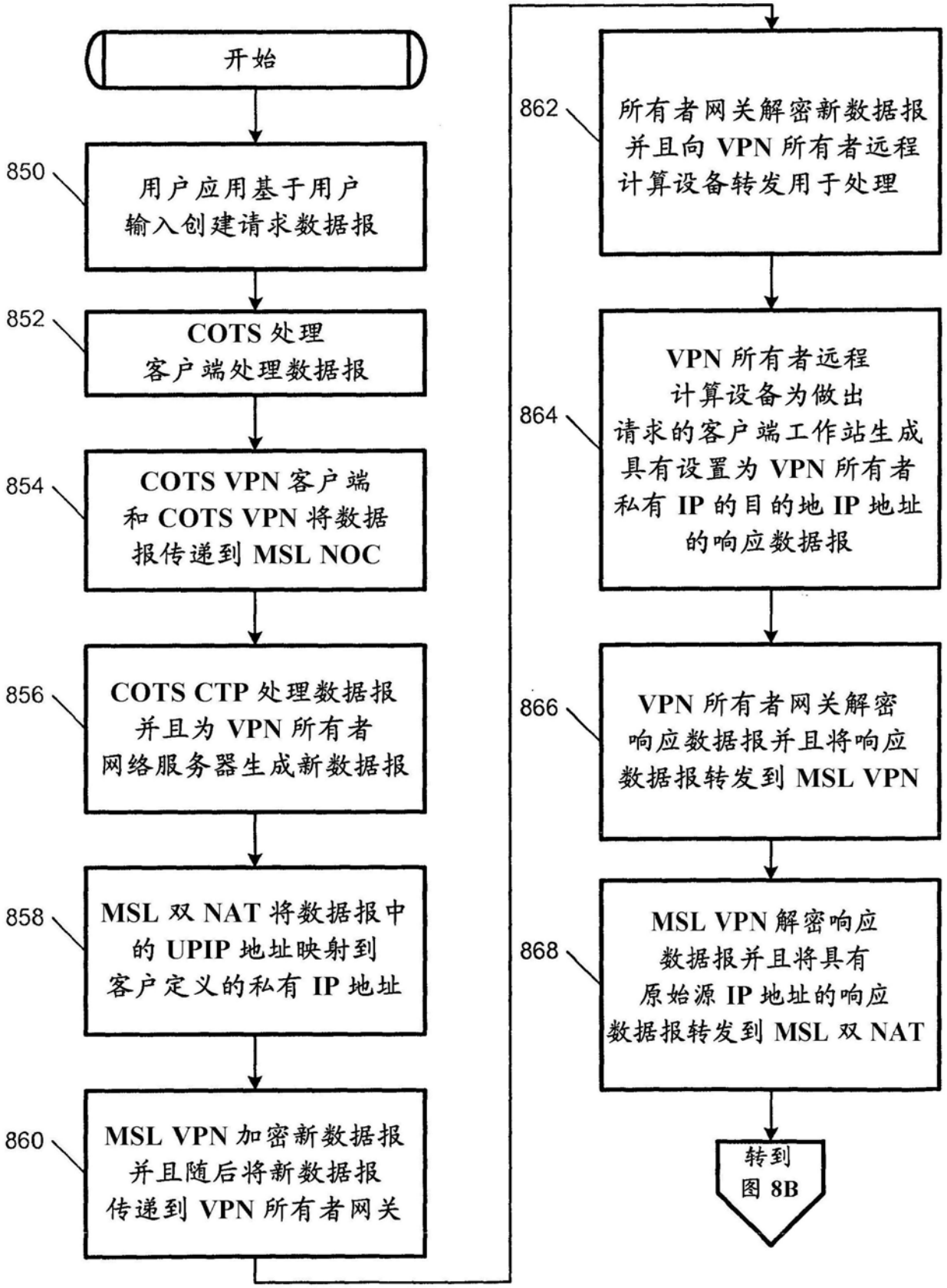

开始
850
用户应用基于用户输入创建请求数据报
852
COTS 处理客户端处理数据报
854
COTS VPN 客户端和 COTS VPN 将数据报传递到 MSL NOC
856
COTS CTP 处理数据报并且为 VPN 所有者网络服务器生成新数据报
858
MSL 双 NAT 将数据报中的 UPIP 地址映射到客户定义的私有 IP 地址
860
MSL VPN 加密新数据报并且随后将新数据报传递到 VPN 所有者网关
862
所有者网关解密新数据报并且向 VPN 所有者远程计算设备转发用于处理
864
VPN 所有者远程计算设备为做出请求的客户端工作站生成具有设置为 VPN 所有者私有 IP 的目的地 IP 地址的响应数据报
866
VPN 所有者网关解密响应数据报并且将响应数据报转发到 MSL VPN
868
MSL VPN 解密响应数据报并且将具有原始源 IP 地址的响应数据报转发到 MSL 双 NAT
转到图 8B

图8A

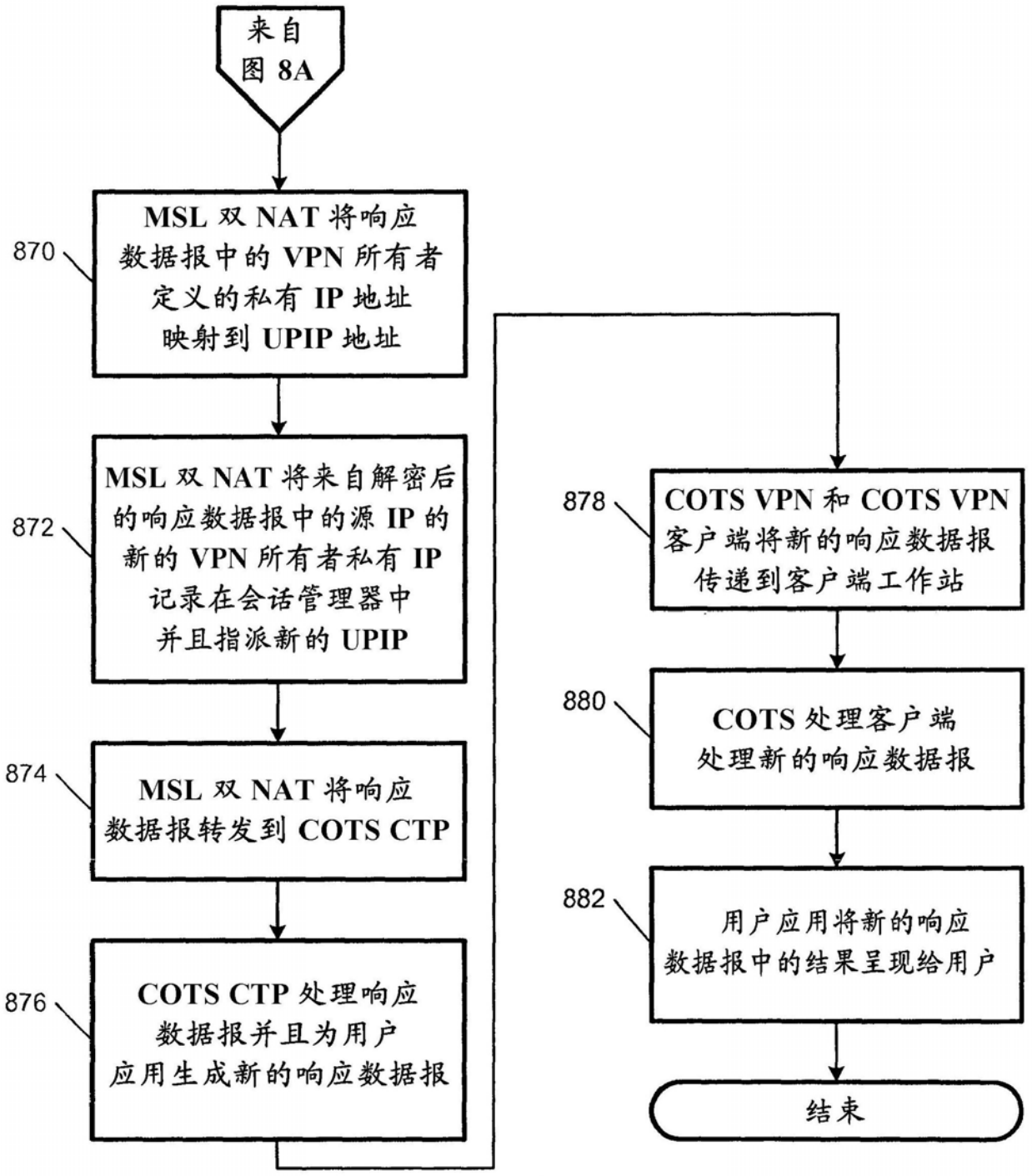

来自
图 8A
870
MSL 双 NAT 将响应数据报中的 VPN 所有者定义的私有 IP 地址映射到 UPIP 地址
872
MSL 双 NAT 将来自解密后的响应数据报中的源 IP 的新的 VPN 所有者私有 IP 记录在会话管理器中并且指派新的 UPIP
874
MSL 双 NAT 将响应数据报转发到 COTS CTP
876
COTS CTP 处理响应数据报并且为用户应用生成新的响应数据报
878
COTS VPN 和 COTS VPN 客户端将新的响应数据报传递到客户端工作站
880
COTS 处理客户端处理新的响应数据报
882
用户应用将新的响应数据报中的结果呈现给用户
结束

图8B

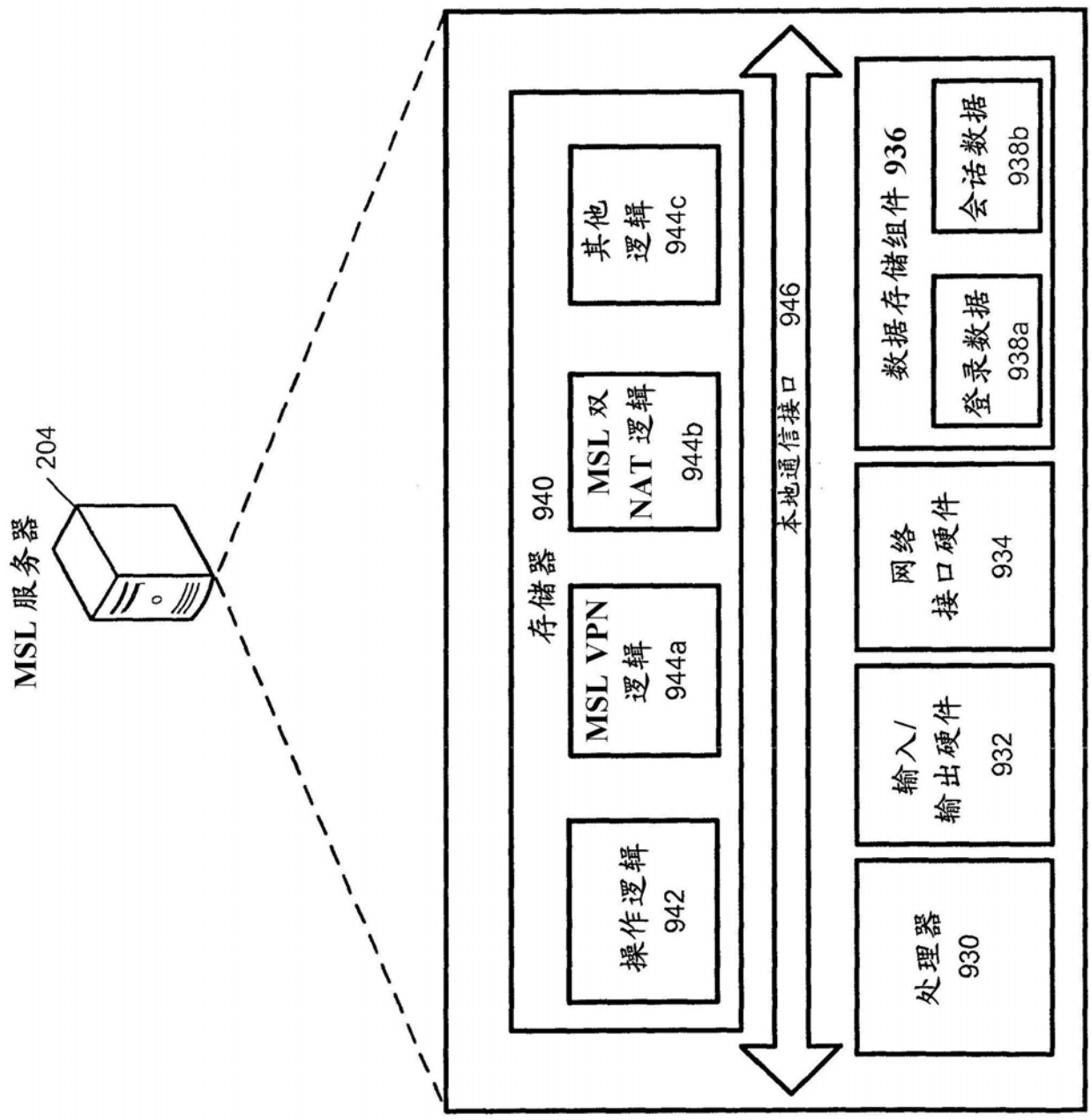

MSL 服务器
204
存储器 940
操作逻辑 942
MSL VPN 逻辑 944a
MSL 双 NAT 逻辑 944b
其他逻辑 944c
本地通信接口 946
处理器 930
输入/输出硬件 932
网络接口硬件 934
数据存储组件 936
登录数据 938a
会话数据 938b

图9