(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 102835093 B
(45)授权公告日 2015.05.20

(21)申请号 201180018596.2

(22)申请日 2011.04.04

(30)优先权数据
61/324,723 2010.04.15 US
12/845,620 2010.07.28 US

(85)PCT国际申请进入国家阶段日
2012.10.11

(86)PCT国际申请的申请数据
PCT/US2011/031103 2011.04.04

(87)PCT国际申请的公布数据
WO2011/130038 EN 2011.10.20

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 D·劳 谭磊 郭鑫

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 蔡悦

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 1478232 A,2004.02.25,
US 2008077788 A1,2008.03.27,
CN 101163082 A,2008.04.16,
US 6412009 B1,2002.06.25,
雷为民,等.MSRP Relay服务器的设计与实现.《小型微型计算机系统》.2010,第31卷(第12期),
张伟,等.针对SIP /NAT问题的RTP中继服务器设计与实现.《小型微型计算机系统》.2005,第26卷(第12期),

审查员 段燕辉

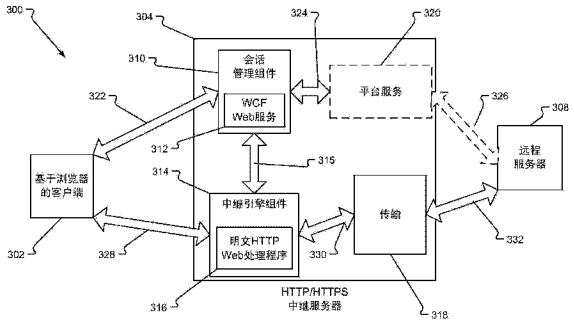
权利要求书2页 说明书15页 附图13页

(54)发明名称

用于通过HTTP的可靠协议隧穿的方法和系统

(57)摘要

本文所描述的实施例一般涉及用于在HTTP端点和任意目的之间隧穿任意二进制数据的方法和系统。这一数据隧穿在例如基于浏览器的客户端以HTTP协议通信并且想要与理解非HTTP通信的远程端点交互数据的实施例中是有价值的。中继服务器被用作为将客户端连接到目的的“中间人”,并且支持所需的用于数据交换的协议的组件被插入到中继服务器中。为了实现数据的可靠和有序传输,中继服务器通过分配会话标识符分组会话并通过分配顺序和确收号来跟踪消息的交换。此外,中继服务器提供向目的认证HTTP端点并且处理在基于web的客户端的受限环境中不可用的其它操作。



CN 102835093 B

1. 一种用于通过经由中继服务器通过超文本传输协议 (HTTP) 隧穿协议数据来扩展客户端的功能的计算机实现的方法，所述方法包括：

在所述中继服务器处接收来自所述客户端的通信以创建与远程端点的中继会话；

认证所述客户端，其中认证所述客户端包括发送质询响应数据给所述客户端；

配置所述中继会话；

为所述中继会话生成会话标识符；

发送所述会话标识符给所述客户端；以及

将 HTTP 请求和响应传输给所述客户端以与所述远程端点交换数据，其中所述 HTTP 请求包括所述会话标识符，其中顺序号和确收号被分配给属于相同会话的 HTTP 请求和响应。

2. 如权利要求 1 所述的方法，其特征在于，所述会话标识符被用于对属于相同中继会话的请求分组。

3. 如权利要求 2 所述的方法，其特征在于，所述会话标识符由密码随机数生成器生成。

4. 如权利要求 1 所述的方法，其特征在于，初始请求和响应发起所述中继会话，并且其中随后的 HTTP 请求经由 HTTP 将会话发起协议 (SIP) 数据经由所述中继服务器传输给所述远程端点。

5. 如权利要求 4 所述的方法，其特征在于，所述 SIP 数据经由 HTTP 被传输到传输机制上，并且其中所述传输机制包括由以下组成的组中的一个：传输控制协议 (TCP)、用户数据报协议 (UDP)、或传输层安全 (TLS)。

6. 如权利要求 1 所述的方法，其特征在于，初始请求和响应发起所述中继会话，并且其中随后的 HTTP 请求经由 HTTP 将远程桌面协议 (RDP) 数据经由所述中继服务器传输给所述远程端点。

7. 如权利要求 6 所述的方法，其特征在于，所述 RDP 数据经由 HTTP 被传输到传输机制上，并且其中所述传输机制包括由以下组成的组中的一个：RTP/SRTP、TLS、UDP 或 TCP。

8. 一种用于通过经由中继服务器通过超文本传输协议 (HTTP) 隧穿协议数据来扩展客户端的功能的计算机实现的方法，所述方法包括：

在所述中继服务器处接收来自所述客户端的通信以创建与远程端点的中继会话；

认证所述客户端，其中认证所述客户端包括发送质询响应数据给所述客户端；

配置所述中继会话；

为所述中继会话生成会话标识符；

分配所述会话标识符给所述客户端；

传输 HTTP 请求以与所述远程端点交换数据，其中所述 HTTP 请求包括所述会话标识符以及顺序号，并且其中所述顺序号作为 HTTP 头部由所述中继服务器接收；

传输 HTTP 请求和响应给所述客户端，其中给所述客户端的 HTTP 请求包括所述会话标识符；

通过所述中继服务器消费所述顺序号；

生成确收号；以及

将所述确收号与 HTTP 响应一起传递给所述客户端。

9. 如权利要求 8 所述的方法，其特征在于，还包括：

使用所述会话标识符来将属于相同中继会话的请求分组，其中一组请求包括 RDP 请

求。

10. 如权利要求 8 所述的方法，其特征在于，所述会话标识符是 GUID。

11. 如权利要求 8 所述的方法，其特征在于，所述认证通过所述中继服务器处的认证代理来执行。

12. 如权利要求 8 所述的方法，其特征在于，通过 HTTP 隧穿的协议数据包括任意协议数据。

13. 如权利要求 8 所述的方法，其特征在于，所述协议数据包括来自以下所组成的组中的一个或多个 ：远程桌面协议 (RDP) 数据以及会话发起协议 (SIP) 数据。

14. 一种配置成通过客户端和远程端点之间的中继服务器来通过超文本传输协议 (HTTP) 隧穿协议数据的系统，所述系统包括 ：

处理器 ；以及

耦合到所述处理器的存储器，所述存储器包括计算机程序指令，所述计算机程序指令能由所述处理器执行以提供 ：

位于所述中继服务器内的会话管理组件，其中所述会话管理组件生成会话标识符 (会话 ID) 以对 HTTP 请求分组并将所述会话 ID 返回给所述客户端 ；

位于所述中继服务器内的中继引擎组件，其中所述中继引擎组件分配一个或多个顺序号和一个或多个确收号给 HTTP 请求和响应 ；

位于所述中继服务器内的平台服务组件，其中所述平台服务组件启用所述客户端的认证以扩展所述客户端的功能 ；以及

位于所述中继服务器内的插入式传输模块，其中所述插入式传输模块支持所述协议数据隧穿。

用于通过 HTTP 的可靠协议隧穿的方法和系统

背景技术

[0001] Web 会议已成为越来越有用的工具，其用来通过因特网或万维网进行实时会议、演示、培训研讨会等。在典型的 Web 会议中，会议的多个参与者通过因特网从他们的个人计算机连接到彼此。用于提供 Web 会议能力的示例软件平台是由华盛顿州雷蒙德市的微软公司出品的 MICROSOFT COMMUNICATIONS SERVER(微软通信服务器)。当客户端想要加入在线会议但在其客户端计算机上没有安装例如 Office Communicator 时，基于 AJAX(“Asynchronous JavaScript and XML”)的 Communicator Web Access (CWA)客户端通常被用来使客户端能够加入会议。虽然基于 AJAX 的 CWA 客户端能够加入会议，但客户端体验受限于经由 Javascript 可用的功能。

[0002] 为了改进基于浏览器的客户端的会议体验且不要求客户端应用的显式安装，可使用与基于 AJAX 的 CWA 客户端不同类型的客户端。例如，可使用如从华盛顿州雷蒙德市的微软公司出品的微软 SIVERLIGHT 平台衍生的基于 SIVERLIGHT 的客户端。SIVERLIGHT 允许开发无论在功能还是用于与服务器通信的底层协议都几乎与本机应用同等水平的特征丰富的应用。然而，SIVERLIGHT 类型的平台可能仍然在能够开发这样的应用方面具有一些限制。例如，基于浏览器的客户机通常不支持连接到提供 Web 会议能力的远程服务器的传输控制协议(TCP)套接字连接。基于客户机的企业网络中固有的提高的安全特性不可能建立这样的套接字连接，在客户机的企业网络中，策略文件检索由于受限的端口和总体上不能穿越防火墙而被禁止。事实上，受限的网络连通性存在于诸如有防火墙的网络、代理服务器后的网络等情形中。在没有策略文件的情况下，基于浏览器的客户端拒绝向远程服务器开放套接字连接。此外，对诸如 NT LAN 管理器(NTLM)认证、Kerberos 认证协议、或证书认证之类的特定安全包的访问可能对应用不可用。没有这些认证能力，基于浏览器的客户机不能获准使用与本地客户端相同的协议加入会话发起协议(SIP)服务器。

[0003] 虽然本背景技术中着眼于特定的问题，但本发明决不旨在限于解决那些特定问题。

发明内容

[0004] 各实施例一般涉及通过利用服务器实体作为将基于 web 的客户端连接到会议平台中的远程端点(例如，远程服务器)的“中间人”而不要求对远程服务器作任何改动来为基于 web 的客户端提供丰富的会议体验和改进的功能。这一“中间人”服务器被称为例如“中继服务器”。各实施例由此提供了使受限环境中的客户端能够通过连接到中继服务器进而利用中继服务器的功能而扩展客户端的功能。中继服务器由此具有与它的诸如例如 Windows 平台之类的环境相关联的功能。基于 web 的客户端通常使用超文本传输协议(HTTP)或超文本传输协议安全(HTTPS)来用于 web 环境中的数据的通信和交换。以下实施例的描述涉及的是“HTTP”。然而，如本领域技术人员能够理解的，这些实施例在涉及“HTTP”时包括“HTTPS”。例如，当会议平台中的远程服务器(诸如 MICROSOFT OFFICE COMMUNICATIONS 服务器(“OCS 服务器”)具有不基于 HTTP 的现有通信协议，中继服务器的使

用准许在基于 web 的客户端和远程服务器之间通过在客户端或 HTTP 端点与远程服务器或其它任意目的之间经由 HTTP 隧穿任意二进制数据或任意协议数据来进行数据交换。各实施例由此提供了通过 HTTP 对任何任意数据的隧穿。例如，各实施例提供用于通过 HTTP 的可靠协议隧穿的中继服务器的以下示例使用：通过 HTTP 将任何数据隧穿到实时传输协议（RTP）/ 安全实时传输协议（SRTP）；通过 HTTP 将远程桌面协议（RDP）隧穿到任何传输机制（例如，TCP 或用户数据报协议（UDP））；通过 HTTP 将 RDP 隧穿到 RTP/SRTP 上；通过 HTTP 方案隧穿 SIP，等等。

[0005] 由于 HTTP 是简单请求 / 响应协议，它支持来自客户端对服务器的多个连接并且因此不保证请求和响应消息的有序递送。可靠的消息递送也不能保证，因为请求和响应消息在消息的发送中可能被丢弃。例如，中间的 HTTP 代理服务器可能丢弃 HTTP 响应。消息的可靠和有序的组织和递送对于 Web 会议环境是有价值的。因此，本公开的各实施例提供了用于将属于同一中继会话的请求分组的会话标识符。此外，消息的可靠和有序递送通过将请求限制为每次一个未决的上游请求和一个未决的下游请求来实现。各实施例还提供顺序 / 确收号，顺序 / 确收号被用来保证丢失消息的检测和丢失数据的重发。在各实施例中也处理否定的 HTTP 响应以再次尝试请求以促进通过 HTTP 的稳健的（例如，无损的）数据传输以及系统弹性。另外，各实施例提供平台服务作为中继服务器的一部分，其中这些平台服务包括例如执行通用密码操作、域名服务（DNS）操作、以及使用认证代理以协助基于 web 的客户端计算与会议环境中的目的的认证握手。另外，各实施例提供实质上可插入的并由此扩展基于 web 的客户端的功能的系统组件。例如，根据各实施例，通过将可插入的传输组件设置在中继服务器上实现了任意协议隧穿。这一可插入传输组件使得能够在 SIP 隧穿中使用传输层安全（TLS）/ 安全套接层（SSL）传输，而另一方面，SRTP 传输被用于例如 RDP 隧穿。此外，根据本公开的实施例，平台服务组件的可插入属性允许客户端使用认证代理来执行 SIP 认证。

[0006] 提供本发明内容是为了以简化的形式介绍将在以下具体实施例中进一步描述的一些概念。本概述并不旨在标识所要求保护的主题的关键特征或必要特征，也决不旨在用于限制所要求保护的主题的范围。

附图说明

[0007] 可以参考附图来更容易地描述本发明的各实施例，附图中相同的数字指示相同的项。

[0008] 图 1 示出了根据本文所公开的各实施例的用于发起基于 web 的客户端参与者之间的会议的环境或系统的示例逻辑表示。

[0009] 图 2 描绘了根据本文所公开的各实施例的使用图 1 中示出的用于会议的中继服务器来通过 HTTP 隧穿任意二进制数据的环境或系统的示例逻辑表示。

[0010] 图 3 示出了根据本文所公开的各实施例的使用图 2 中示出的中继服务器来通过 HTTP 进行协议隧穿的示例功能组件模块的逻辑表示。

[0011] 图 4 示出了根据本文所公开的各实施例的示出图 3 中描绘的功能组件模块的交互的过程的操作特性的流程图。

[0012] 图 5 描绘了根据本文所公开的各实施例的示出使用中继服务器的系统的可插入

性质的过程的操作特性的流程图。

[0013] 图 6 示出根据本文所公开的各实施例的描绘用于将属于中继会话的请求分组(通过使用会话标识符)的过程的操作特性的流程图。

[0014] 图 7 示出根据本文所公开的各实施例的示出用于将顺序和确收号分配给请求和响应以确保消息的可靠和有序递送的过程的操作特性的流程图。

[0015] 图 8A 示出根据本文所公开的各实施例的用于隧穿 SIP 数据的中继服务器的示例功能组件模块的逻辑表示。

[0016] 图 8B 示出了根据本文所公开的各实施例的示出图 8A 中描绘的功能组件模块的交互的过程的操作特性的流程图。

[0017] 图 9 示出根据本文所公开的各实施例的描绘用于使用中继服务器的认证代理来认证具有任意目的的 HTTP 端点的过程的操作特性的流程图。

[0018] 图 10 示出根据本文所公开的各实施例的用于隧穿 RDP 数据的中继服务器的示例功能组件模块的逻辑表示。

[0019] 图 11 示出了根据本文所公开的各实施例的示出图 10 中描绘的功能组件模块的交互的过程的操作特性的流程图。

[0020] 图 12 描绘其上可以实现本发明的各实施例的示例计算系统。

具体实施方式

[0021] 本发明现将参考其中示出了各具体实施例的附图来更完整地描述各示例实施例。然而,其它方面能以许多不同的形式来实现,并且在本发明中包括具体的实施例不应被解释为将这些方面限于在此所述的各实施例。相反,包括附图中描绘的各实施例是为了提供全面和完整且将预期的范围完全地传达给本领域技术人员的公开。虚线可用于示出可任选组件或操作。

[0022] 各实施例一般涉及使用中继服务器来扩展 web 会议环境中的基于浏览器或基于 web 的客户端的功能。在可替换实施例中,客户端不是基于浏览器或基于 web 的客户端,而是本领域技术人员能理解的任何类型的客户端。中继服务器提供例如基于 web 的客户端或 HTTP 端点与任意目的或远程服务器之间的任意二进制数据的隧穿(tunneling)。这种隧穿是有用的,因为基于 web 的客户端通常使用 HTTP 协议进行通信,但不能使用远程服务器所理解的传输协议来通信。这些传输协议包括例如 TCP、UDP、SRTP、TLS 等。这些协议仅作为示例来提供。远程服务器可使用本领域的技术人员说理解的任何数量的传输协议。由此通过使用中继服务器提供了通过 HTTP 的对诸如 SIP 和 RDP 之类的任何任意协议的隧穿。中继服务器用作一种“中间人”,以经由 HTTP 请求接收字节缓冲区并将该请求中继给目的。类似的,中继服务器接受来自目的的数据并且经由 HTTP 响应将数据中继给客户端。

[0023] 在一个实施例中,中继服务器被设计为位于例如因特网信息服务器(IIS)服务器处的 web 应用。在这类实施例中,中继服务器包括会话管理组件、中继引擎组件、以及可选的平台服务组件。在各实施例中可使用任何数量种类型的组件,无论是组合的还是单独的,并且如所示出的,一些组件在各实施例中也可以可选的。中继服务器被设计成可扩展的,以允许使用任何传输机制以接受来自 HTTP 端点的隧穿数据。中继服务器允许任何二进制数据被隧穿。例如,在各个实施例中,对 SIP 和 RDP 通信数据进行隧穿。然而,其它实施例提

供用于包括文件传输数据在内的任何数据的隧穿。在创建中继会话时，各实施例规定中继服务器与目的端点通信以建立连接，使得可交换目的端点所理解的特定协议数据。中继服务器因此被配置成以任意协议通信以建立连接。

[0024] 根据一实施例，为了建立中继会话，客户端请求在中继服务器的会话管理组件处创建一会话。客户端与中继服务器之间的这一交互可被称为中继会话的第一“旅程(leg)”。在各个实施例中，中继服务器被配置为具有可选的平台服务，以帮助会话创建，例如，无论这是认证还是 DNS 查找。中继服务器还被配置为具有一个或多个传输模块，其中传输模块以特定协议与远程服务器通信。会话管理组件驱动传输模块连接到远程服务器，其中有来自客户端的经由例如 web 服务调用的潜在帮助。“web 服务调用”仅仅是作为发送这类信息的方法中的一个示例来提供的。也可使用本领域技术人员说理解的其它类型的通信。在一个实施例中，对于中继会话的第一旅程，会话管理组件与中继引擎组件交互、生成会话标识符(会话 ID)来对 HTTP 侧通信流量分组、并将会话 ID 返回给客户端。利用会话 ID，通过 HTTP 建立客户端和中继服务器之间的虚拟连接。根据各个实施例，这一会话 ID 将存在于客户端发送的每个 HTTP 请求中。会话 ID 连同顺序 / 确收号、根据一实施例的每个方向(上游和下游)最多只有一个未决请求的规定、以及当例如发生故障时重新尝试发送 HTTP 请求预订次数，提供了一种用于通过 HTTP 在客户端和中继服务器之间的可靠和有序的双向数据递送。如所提到的，在各个实施例中，这一连接是中继会话的一个旅程，而中继会话的第二旅程是从中继服务器到远程服务器，其中使用了任意传输协议。根据各个实施例，在中继服务器上加载传输栈以准许协议的隧穿。

[0025] 通过经由 HTTP 隧穿协议数据，本公开的各实施例显著地扩展了基于 web 的客户端的功能，因为中继服务器允许适应于用于连接到每个可能的目的端点的不同的各种装置。例如，当目的端点是服务器时，不同装置被用来连接到特定类型的服务器，诸如将 TLS 连接至 SIP 服务器，将 RTP/SRTP 连接至屏幕共享服务器等。

[0026] 此外，本公开的各个实施例还补偿了由用于增强安全特性的受限端口和企业防火墙所导致的限制。由于企业网络中存在的受限端口，即使不是不可能，也难以从基于 web 的客户端检索策略文件。例如，端口 943 将策略文件实施保存在 SILVERLIGHT 平台。SILVERLIGHT 客户端计算机发送请求给 web 站点以在端口 943 上访问策略文件。然而，端口 943 在企业网络中通常是不开放的。因此，策略文件检索即使没有变得完全不可能也是被阻碍。在没有策略文件的情况下，基于浏览器的客户端拒绝向远程服务器开放套接字连接。基于 web 的客户端和远程服务器之间的通信因此通常不可能。然而，本公开的各个实施例使用中继服务器来连接基于 web 的客户端和远程服务器。中继服务器的以 HTTP 与客户端通信的能力使得能够穿越企业防火墙。例如，使用 HTTP 作为传输机制减少了在穿越企业防火墙时的问题，因为端口 80/443(HTTP 80/TCP 即万维网 HTTP;HTTPS 443/TCP 即通过 TLS/SSL 的 HTTP 协议)在企业网络中通常都是开放的。

[0027] 在各个实施例中，基于 web 的客户端因此能够向中继服务器开放 HTTP 连接，中继服务器作为客户端和远程服务器之间的通信的中继。基于 web 的客户端随后使用 HTTP 请求与中继服务器通信。当接收到 HTTP 请求后，中继服务器“解开”用于交换的实际数据并使用远程服务器所理解的传输协议将其转发给远程主机。类似地，在以远程服务器所使用的传输协议接收到数据之后，中继服务器用 HTTP 协议对数据“打包”，并将其作为 HTTP 响应

的一部分发送或传输给基于 web 的客户端。

[0028] 由于 HTTP 是简单请求 / 响应协议，并且支持从客户端到服务器的多个连接，因此不能保证消息的有序递送。此外，HTTP 协议的简单请求 / 响应属性没有提供用于确保消息的可靠递送的内建机制，并因此响应在抵达客户端之前可能被丢弃。此外，这些协议没有提供对请求分组以形成会话的方式。不能确保信息的可靠和有序递送对成功的 web 会议是妨碍。因此，本公开的实施例提出使用会话标识符（会话 ID），诸如像 GUID 的会话标识符或其它加密的强标识符，来将属于同一中继会话的请求分组，如以上讨论的。会话标识符是在中继服务器处使用密码随机数生成器随机生成的。通过使用密码随机数生成器，防止第三方猜测号码并攻击由系统所提供的服务。为了进一步的安全性，会话标识符还可用仅中继服务器知晓的秘密（secret）来签名，以防止任何猜测攻击。会话标识符能力因此增强了安全性，并且将 HTTP 环境中固有的多连接组织到具体的中继会话中。

[0029] 为了进一步实现消息的有序递送，本公开的实施例跟踪上游和下游请求，以在同一时间仅允许一个未决的上游请求和一个未决的下游请求。顺序号和确收号被分配给请求和响应消息以追踪数据交换并检测丢失的消息。但检测到丢失消息或接收到否定 / 失败的 HTTP 响应（诸如，具有除 200OK 以外的任何状态代码的响应）的指示之后，对应于该否定 / 失败的 HTTP 响应的 HTTP 请求在结束会话之前被重新发送和 / 或重新尝试预定次数。这样的消息追踪有助于实现无丢失数据传输和系统弹性。

[0030] 在为了扩展受限制的环境中的基于 web 的客户端的用于与目的通信的功能的进一步实施例中，可选平台服务组件帮助提供受限制的环境中不可用的功能。当中继不同协议数据时，可能需要不同平台服务。这些服务可插入到系统。作为示例，在隧穿 SIP 数据时，平台服务包括认证代理，用于帮助客户端成功地响应 SIP 服务器发起的安全质询。基于 web 的客户端无法成功地响应这些质询是源于缺少足够的用于受限制的客户端环境中的安全性的软件包。在本公开的实施例中，基于 web 的客户端通过将认证能力委托给认证代理来扩展其被限制的功能，认证代理是用于隧穿 SIP 数据的平台服务的一部分，虽然它的使用不被限制于隧穿 SIP 数据。在各实施例中，中继服务器具有比受限制的客户机环境更多的功能，因为它是一个全功能服务器。例如，在各个实施例中，中继服务器安装了更多的软件包。在各个实施例中，当中继服务器自己不能提供需要的功能时，中继服务器平台服务可寻求其它服务器组件来协调让客户机满意的结果。例如，在一个实施例中，中继服务器上的认证代理模块被用来协助客户端计算与目的的认证握手。基于 web 的客户端因此将密码调用委托给中继服务器并使用中继服务器作为处理远程服务器处的协议通信所需的密码调用和地址的工具。其它实施例通过例如将散列计算（通过在中继服务器上实施必要的算法）或域名解析 API 调用（用于将主机名称解析为 IP 地址）的处理委托给中继服务器的平台服务组件来扩展基于 web 的客户端的功能。本文所提供的操作仅作为示例来提供。

[0031] 图 1 中示出了主持多个参与者之间的 web 会议的示例逻辑环境或系统 100。参与者 102 和 104 想要与彼此进行 web 会议。为此，客户端 106 和 118 分别跨网络 108 和 120 联系诸如例如 SIP 服务器之类的服务器 110 以分别请求加入会议 114 和 124。如果会话发起请求被理解并被启用，则 SIP 服务器 110 分别向客户端 106 和 118 发送接受消息 116 和 122。然而，当例如在客户端 106 和 SIP 服务器 110 之间没有建立连接时，会话请求 114 可以是开放式的或者完全拒绝的（未示出）。这一情形可存在于例如当诸如基于 web 的客户端之类的

客户端 106 的受限制的环境阻止套接字连接(未示出)向服务器 110 开放的情况下。此外，客户端 106 能够仅以 HTTP 通信并且因此不能以服务器 110 所理解的协议来通信，诸如通过 TLS 或 TCP。因此想要通过 HTTP 隧穿例如 SIP，其中客户端 106 是仅使用 HTTP 通信的基于 web 的客户端或者具有某些其它形式的受限网络连通性，诸如企业防火墙网络、代理服务器之后的网络、NAT 等。

[0032] 图 1 示出了普通会议环境，而图 2 描绘了用于通过使用中继服务器 206 以启用与目的 208 的丰富会议体验来扩展受限环境中的基于 web 的客户端 202 的功能的示例逻辑环境或系统 200。在图 2 中，基于 web 的客户端 202 也被称为隧穿客户端 202。此外，在各个实施例中，基于 web 的客户端可指代任何类型的任意端点，诸如“基于浏览器的客户端”等。术语“基于 web 的”客户端仅作为示例来提供。当基于 web 的客户端 202 的通信是基于 HTTP 的，如果目的端点 208 采用不是基于 HTTP 的现有通信协议，则客户端 202 不能连接到目的端点 208。在一个实施例中，目的 208 是远程服务器，诸如 SIP 服务器。在另一实施例中，目的 208 是屏幕共享服务器。在又一实施例中，目的 208 是客户端自身。此外，可使用任何数量的目的端点 208，如省略号 210 和目的 212 所示。

[0033] 基于 web 的或隧穿客户端 202 通过网络 204 发送 HTTP 请求 214 给中继服务器 206。中继服务器 206 解开请求 214 中的数据并使用目的 208 所理解的协议将解开的数据 216 通过网络 218 转发给目的 208。在各个实施例中，中继服务器 206 因此通过 HTTP 隧穿了数据，例如 SIP 和 RDP 协议数据。如上说讨论的，中继服务器 206 可隧穿任何任意二进制数据。在这一实施例中，中继服务器 206 已经具有诸如 RTP/SRTP 或 TLS 之类的合适的传输栈，如果需要的话，这些传输栈被加载到中继服务器上(未示出)以实现这一隧穿。

[0034] 在处理接收到的协议数据 216 之后，目的 208 将协议数据 220 发送给中继服务器 206。中继服务器 206 随后以 HTTP 协议打包从目的 208 接收的数据，并将其作为 HTTP 响应 222 的一部分发送给客户端 202。根据本文所公开的实施例，任何类型的任意数据可被隧穿。例如，根据各实施例，环境或系统 200 可允许：通过 HTTP 将任何数据隧穿到 RTP/SRTP；通过 HTTP 将 RDP 隧穿到 RTP/SRTP；通过 HTTP 将 RDP 隧穿到任何传输机制(诸如 TCP 或 UDP)；以及通过 HTTP 隧穿 SIP。

[0035] 逻辑环境 200 不被限制于任何特定实现，相反，可以由其上可实现本文所描述的环境的功能的任何计算环境来实现。例如，根据各个实施例，可使用本领域技术人员理解的任何类型的客户端计算机 202。此外，网络 204 和 218 虽然被显示为独立的单个网络，但它们可以是本领域技术人员按照惯例理解的任何类型的网络。根据一实施例，网络可以是全球网络(例如，因特网或万维网，即简写为“web”)。其还可以是局域网(例如，内联网)或广域网。根据各个实施例，网络 204 和 218 上的通信按照一个或多个标准的基于分组的格式(例如，H.323、IP、以太网、和 / 或 ATM)来进行。

[0036] 此外，根据本公开的实施例，可使用本领域技术人员说理解的任何可能的环境或系统。图 2 仅为了理解本文所公开的实施例的教示而作为示例来提供。例如，图 2 示出了中继服务器 206 和目的 208、210、以及 212。然而，各实施例也覆盖任何类型的服务器、分开服务器、服务器场或其他消息服务器。此外，图 2 显示了客户端计算机 202。然而，如本领域技术人员所理解的，可使用任何类型的小型计算设备而不违背本文所公开的实施例的精神和范围。例如，尽管仅示出一个客户端计算机 202，另一实施例提供多个小型计算机设备来

与中继服务器 206 通信。在一个实施例中，每个小型计算机设备与网络 204 通信，或者，在其它实施例中，多个单独网络与小型计算机设备通信。在又一实施例中，每个小型计算机设备与单独的网络通信。事实上，环境或系统 200 表示实现本文所公开的实现实施例的一种有效方式，但完全不意图限制本公开的范围。此外，示例网络环境 200 可以被视为由所描述的具体组件组成，例如中继服务器、客户端计算机等，或者可替换地，可被视为由对应于这些单元的类似模块组成。

[0037] 图 2 显示了用于通过 HTTP 进行协议隧穿的示例环境或系统 200，而图 3 示出了根据本公开的实施例的用于通过中继服务器 304 扩展基于浏览器的客户端 302 的功能的软件功能模块 300。根据本文公开的实施例，软件功能模块 300 执行在图 3 中所示的计算系统中。在图 3 中示出的实施例中，基于浏览器的客户端 302 诸如经由 web 服务调用 322 来联系中继服务器 304 以创建中继会话。中继服务器 304 的会话管理组件 310（其包括 web 服务 312）经由例如方法调用 315 与中继引擎 314 交互，中继引擎 314 包括用于配置所请求的中继会话的明文 HTTP web 处理程序 316。在各个实施例中，会话管理组件 310 提供通过生成会话标识符等发起以及建立客户端 302 和目的（诸如远程服务器 308）之间的连接的功能、例如建立会议中涉及的实体间的连接的功能、以及将属于相同中继会话的请求分组的功能。根据一个实施例，会话标识符经由例如 web 服务调用返回值来返回给客户端。一旦建立了会话，中继引擎组件 314 提供客户端 302 和远程服务器 308 之间的数据交换。在各实施例中，中继引擎 314 还提供分配顺序号和确收号以确保请求和响应消息的可靠和有序递送。

[0038] 在一个实施例中，会话管理组件 310 首先联系平台服务组件 320 或认证组件 320 以获取配置中继会话的许可。（在一些实施例中，平台服务组件 320 是可选的，如虚线 320 所示。）根据各实施例，平台服务组件 320 提供例如执行客户端 302 的认证，以及处理密码调用操作和 DNS 解析操作。这些服务仅作为示例来提供。其它和额外类型的服务由平台服务组件 320 执行。在一些实施例中，平台服务组件 320 可直接由基于浏览器的客户端 302 调用。根据一实施例，基于浏览器的客户端 302 可能需要被认证以加入与远程服务器或目的 308 的会议。在进一步实施例中，认证组件 320 具有诸如质询数据之类的信息或数据以供传递给基于浏览器的客户端 302 以在创建中继会话之前进行认证，其中中继服务器 304 用作基于浏览器的客户端 302 和远程服务器 308 之间的“中间人”。在又一实施例中，认证组件 320 联系 326 远程服务器 308 以验证客户端 302，以便通过如下方式来加入会议：向远程服务器 308 呈现创建中继会话的客户端请求；和 / 或获取认证信息或数据（例如，质询数据）以及唯一标识符以便发送 322 给客户端 302 以构成质询响应消息 322。虚线 326 显示了认证组件 320 和远程服务器 308 之间的联系的可选属性。根据各实施例，当远程服务器 308 被联系时，它可验证由中继服务器 304 提供的秘密，并且当该验证成功时，提供质询数据（根据各实施例，包括唯一标识符）给验证组件 320（如联系 326 的双向属性所示）。在又一其它实施例中，没有秘密被提供给远程服务器 308，并且远程服务器 308 提供质询 / 标识符数据而不对来自中继服务器 304 的请求进行任何验证。

[0039] 在认证被要求并成功（或者其中认证起初不被要求，如以上所讨论的）的实施例中，会话管理组件 310 通过例如方法调用来与中继引擎组件 314 交互 315 以配置中继会话。当成功地创建中继会话之后，会话管理组件 310 分配会话 ID 给客户端 302。在一个实施例中，分配给客户端 302 的会话 ID 被用来对属于同一会话的请求分组。在一个实施例中，会话

ID 是 GUID 状或其它密码强的会话标识符。GUID 状标识符仅作为示例提供。根据本公开的各实施例，可使用其它类型的会话标识符，诸如那些用来进一步增强安全性的标识符。在一个实施例中，一个会话 ID 被分配给 SIP 请求，而另一会话 ID 被分配给例如来自基于浏览器的客户端 302 的 RDP 请求。该会话 ID 被从中继服务器 304 发送 322 给基于浏览器的客户端 302，并且客户端 302 随后使用该会话 ID 作为 HTTP 头部以与中继引擎 314 通信 328。当接收到来自基于浏览器的客户端 302 的数据时，中继引擎 314 与传输组件 318 交互 330 以将数据 332 中继到远程服务器 308 或中继来自远程服务器 308 的数据 332。中继引擎 314 由此解开 HTTP 请求中接收或传输的数据并将该数据以用于该传输的适当的协议转发给远程服务器 308。中继服务器 304 由此用作为用于以想要网络协议来通信的“隧道”。软件功能模块 300 是作为所描述的各实施例的可能的软件功能模块的示例来提供的。其它实施例可包括所描绘的模块、比所描绘的模块和 / 或子模块少的模块、额外的模块和 / 或子模块、模块和 / 或子模块的组合、所描绘的模块和 / 或子模块的扩充等。

[0040] 根据各实施例，对应于中继服务器 304 上的那些模块的模块也存在于基于浏览器的客户端 302 和远程服务器 308 上以允许这些通信和传输。在客户端侧，一个实施例包括例如对应于中继服务器的模块以发起 HTTP 请求，将会话 ID 作为 HTTP 头部放在请求中，分配顺序号并使用上游数据的确收号，使用顺序号并生成下游数据的确收号等。根据各实施例，在远程服务器处，对应于中继服务器的部分是协议参与者。在一个实施例中，协议参与者是例如 TCP 参与者，用来协助在中继服务器和远程服务器之间移动数据。

[0041] 根据本文所公开的实施例，图 3 中描绘的各个软件功能模块的交互进一步示出在图 4 所描绘的用于经由 HTTP 隧穿协议数据的操作步骤中。开始操作 402 启动，并且过程 400 前进到接收例如来自基于浏览器的客户端的联系，诸如经由 web 服务调用，以创建中继会话 404。在配置所请求的中继会话 410 之前，过程 400 可任选地（如虚线所示）首先前进至查询 406 以从平台服务组件确定客户机是否被准许（例如，被认证和 / 或被授权）创建与目的的会话。在作出这一确定 406 时，中继服务器可诸如通过平台服务组件 320 可选地联系目的 408（诸如图 3 中的远程服务器 308）以获取质询数据和 / 或其它认证数据，以完成客户端和目的之间的握手以配置所请求的会话。虽然根据描述的实施例，步骤 406 和 408 都被显示为可选步骤，但其它实施例要求 406 处的这一认证确定但不要求联系远程服务器 408。在又进一步的实施例中，步骤 406 和 408 都被要求认证和 / 或授权步骤。步骤 406 和 408 中涉及的认证显示本公开的实施例中使用的平台服务的可插入属性，例如认证代理。如果查询 406 确定客户端被认证和 / 或授权建立中继会话，则过程 400 前进（是）至配置中继会话 410。根据本公开的实施例，如果客户端没有被认证以及这一认证没有被要求进行，则过程 400 前进（否）至结束操作 422，在操作 422，过程 400 中止。当客户端被准许配置中继会话并且该会话被配置 410，过程 400 分别前进至生成和分配会话 ID412 和 414，其中会话 ID 被生成并分配给客户端。在一个实施例中，会话 ID 被生成和分配以用来对属于同一中继会话的请求分组。在一个实施例中，这一会话 ID 是在中继服务器处（诸如在例如会话管理组件处）通过密码随机数生成器随机生成的。如所讨论的，虽然描述的是 GUID 会话 ID，但这一类型的标识符仅作为示例提供。然而，如本领域技术人员所理解的，可使用任何数量种类型的标识符而不违背本文所公开的精神和范围。

[0042] 接着，过程 400 前进至发送会话 ID 给客户端 416，其中被分配给属于特定中继会话

的请求的会话 ID 被发送给客户端。客户端随后使用会话 ID 作为 HTTP 头部以与中继服务器通信以进一步交换数据，其中中继服务器接收具有会话 ID 的 HTTP 请求 418。数据随后通过中继服务器与远程服务器 420 交换，随后过程 400 在结束操作 422 终止。图 4 是根据本文公开的各实施例的用于通过使用中继服务器经由 HTTP 进行协议隧穿的可能的操作特性的示例。所描绘的操作步骤可被组合到其他步骤中和 / 或被重新安排。此外，可使用例如更少或更多的步骤。

[0043] 图 5 接着示出根据本公开的实施例的系统的可插入特性。例如，如以上讨论的，平台服务组件是可插入的，以向受限环境中的客户端提供服务。例如，根据各实施例，作为平台服务组件的一部分的认证代理协助客户端进行 SIP 认证。此外，传输是可插入的。传输的可插入特性允许对任意数据隧穿，因为可以为想要被隧穿的数据使用任何适当协议。例如，在各实施例中，SIP 隧穿使用 TLS 作为传输，而在各实施例中，RDP 隧穿使用 SRTP 作为传输。图 5 示出了根据一实施例的用于诸如通过开发者来配置中继服务器以在属性方面可插入的过程。在开始操作 502 启动过程 500，并且前进至查询 504 以确定是否想要配置中继服务器以隧穿数据。如果否，过程 500 前进到结束操作 528，则过程 500 终止。如果是，过程 500 前进(是)到确定操作 506，其中确定是否隧穿 SIP 数据。如果是，过程 500 前进到添加插入式 TLS/SSL 传输模块 508，其中在一个实施例中，TLS/SSL 被用作 SIP 隧穿中的传输。在另一实施例中，另一类型的协议被用于传输以供 SIP 隧穿。接着，过程 500 前进以查询 510 以确定是否有任何插件要被添加。如果不想要任何其他插件，过程 500 前进(否) 到结束操作，并且过程 500 终止。如果想要其它插件，过程 500 前进(是)到例如添加认证代理插件 512。在各实施例中，认证代理是协助客户端执行 SIP 认证的一组平台服务。在添加插入式认证代理 512 之后，过程 500 前进至查询 514 以确定是否想要任何其它插件。如果是，添加插件 516，并且步骤 514-516 重复直到不想要其它插件。如果不想要其它插件，过程 500 前进(否) 到结束操作 534 并终止。

[0044] 返回查询 506，如果不想要 SIP 隧穿，过程 500 前进(否)至查询 518 以确定是否想要隧穿 RDP 数据。如果想要隧穿 RDP 数据，过程 500 前进(是)到添加用于 RTP/SRTP 传输模块 520 的插件，其中 RDP 隧穿使用 RTP/SRTP 作为传输。接着，确定是否有任何其它插件想要被添加 522。如果不想要其它插件，过程 500 前进(否) 到结束操作 534 并且过程 500 终止。如果想要其它插件，过程 500 前进(是)至添加插件 524，接着前进至查询 522 以再次确定是否想要任何其它插件，并且这些步骤重复。如果不想要其它插件，过程 500 前进(否)以在结束操作 534 终止过程 500。

[0045] 回到步骤 518，如果不想要 RDP 隧穿，过程 500 前进(否)至查询 526 以确定是否想要任何任意数据的隧穿。如果否，则过程 500 在结束操作 528 终止。如果想要隧穿任意数据，过程 500 前进(是)至插入式适当的协议传输模块 530 以支持任意协议数据隧穿。接着，在操作 532 确定是否有任何其它插件想要被添加。如果想要其它插件，则过程 500 前进(是)至添加插件 524 并且这些步骤重复直到不想要其它插件。当不想要其它插件，过程 500 前进(否)到结束操作 534 并且过程 500 终止。图 5 是根据本文公开的各实施例的诸如由开发者来将中继服务器配置成可插入属性的可能的操作特性的示例。所示出的操作步骤可被组合到其他步骤中和 / 或被重新安排。此外，可使用例如更少或更多的步骤。

[0046] 图 6 接着示出根据本文公开的实施例的用于分配会话 ID 以将属于相同的中继会

话的请求分组的示例操作步骤 600。过程 600 起始于开始操作 602，并且前进至接收创建中继会话 604 的请求，其中在中继服务器处接收到来自基于浏览器的客户端的诸如 SIP 请求之类的请求。在操作 606 创建中继会话，并且通过密码随机数生成器随机生成会话 ID 608 用于将请求（例如，SIP 请求）分配给属于相同中继会话的组。在一个实施例中，会话 ID 是 GUID 状的会话 ID。接着，过程 600 前进至操作 610，分配随机数给组 1。例如，组号被发送给“组 1”的客户端 612。接着，过程 600 前进至例如从基于浏览器的 web 应用 614 接收对 RDP 数据的请求。接着生成另一会话 ID 616 以将对例如 RDP 数据的请求分组到例如“组 2”中。用于将组号分配给“组 2”的客户端的会话 ID 被发送给客户端 618，并且过程在结束操作 620 终止。图 6 是根据本文公开的实施例的用于分配会话 ID 以将属于相同的中继会话的请求分组的可能的操作特性的示例。所示出的操作步骤可被组合到其他步骤中和 / 或被重新安排。此外，可使用例如更少或更多的步骤。

[0047] 另外，图 7 描绘了根据本文公开的各实施例的用于执行用于分配顺序号和确收号以确保客户端（诸如基于 web 浏览器的客户端）和中继服务器之间的数据的可靠和有序递送的方法的示例操作步骤 700。过程 700 起始于开始操作 702，并且前进至在基于浏览器的客户端处生成 HTTP 请求 704，其中过程 700 示出经由中继服务器从基于浏览器的客户端移动至远程服务器的上游数据。在操作 704，还将顺序号分配给客户端的请求。接着，在中继服务器处接收具有顺序号的请求 706。中继服务器使用该顺序号 708，其中该顺序号被作为 HTTP 头部传递给中继服务器。中继服务器接着生成确收号 710。根据各实施例，中继服务器作为 HTTP 响应的 HTTP 头部和 / 或作为响应的主体将确收号与 HTTP 响应一起传回客户端 712。在客户端侧，HTTP 响应（如果接收到的话）被匹配于未决的请求（未示出）。根据一个实施例，将 HTTP 响应与其请求的匹配在客户端处由诸如 web 浏览器之类的底层平台执行。在这一实施例中，在客户端处经由与发送请求相同的连接（诸如，TCP）接收 HTTP 响应。在各个实施例中，请求 / 响应顺序和确收号的这一匹配和追踪使得能够协助通过 HTTP 的有序和可靠数据传输。

[0048] 由于响应消息和确收号可能在从中继服务器到客户端的传输期间被丢弃，过程 700 提出在查询 714 中确定客户端是否接收到对应于 HTTP 中发送的数据的确收。例如，根据本文公开的实施例，对于上游数据，由客户端发起的每个 HTTP 请求为该特定请求携带的第一个字节的数据携带一顺序号。另外，每个请求具有指示请求所携带的数据的字节数的长度数。在中继服务器侧，为响应消息生成的确收号是中继服务器接收到的最后一个字节。在这一确收号之前的所有具有顺序号的数据也因此通过最近确收号而确认。一旦客户端确认了字节已被接收到，它就将这些字节从其高速缓存中移除。否则，根据各实施例，在没有接收到确认的情况下，数据被重新递送。例如，当顺序号从 1 开始并且请求的长度包括 100 字节，则客户端查找的确收号为 100。当发送第二请求，顺序号起始于 101，并且如果长度是 200，则客户端查找对应的确收号 300。

[0049] 回到图 7，如果在 714 接收到确收（指示请求 / 响应消息的可靠递送），则过程 700 前进（是）至查询 716 以确定客户端是否想要经由中继服务器发送其它请求给远程服务器。如果想要其它请求，则过程 700 前进（是）至生成 HTTP 请求并分配顺序号 704 给下一请求。如果不想要其它请求，过程 700 前进（否）到结束操作 718 并且过程 700 终止。

[0050] 当查询 714 确定没有收到确收，或者在其它实施例中，接收到指示否定处理和 / 或

失败处理，则过程 700 前进（否）至查询 720 以确定预定等待时间是否超过。如果诸如在各实施例中由定时器指示的用于确收的等待时间还没有超过，则过程 700 回到查询 714 以确定确收是否被接收，并且步骤 714 和 720 重复。如果预定的等待时间已超过，则过程 700 前进（是）至操作 722 以重新尝试发送请求，并且过程 700 随后再次前进至操作 706。在重复步骤 706 至 716 之后，过程 700 最终前进至结束操作 718，并且过程 700 终止。图 7 是根据本文所公开的各实施例的用于分配顺序号并追踪请求的确收以确保消息的有序和可靠递送的可能的操作特性的示例。所示出的操作步骤可被组合到其他步骤中和 / 或被重新安排。此外，可使用例如更少或更多的步骤。

[0051] 通过使用确收查询和 / 或确收号并等待直到第一请求被确认收到再发送第二请求，过程 700 提供了通过追踪消息来防止丢失数据并实现具有系统弹性的无丢失的数据传输的可靠和有序消息递送。此外，根据本文公开的各实施例，追踪请求 / 响应消息使得系统能够通过使同一时间只有一个未决的上游请求和一个下游请求来维持有序递送，其中第二请求不能被发送直到第一请求 / 响应被确认。此外，确收号的使用使得系统能够追踪为了与新数据（除了携带请求的数据之外）一起发送而重新尝试的请求。另外，如所讨论的，在 HTTP 允许例如同一时间的多个连接的条件下，消息的有序发送在 HTTP 请求 / 响应会议环境中是有益的。虽然图 7 示出了用于实现客户端和中继服务器之间（反之亦然）的可靠和有序的数据递送，但根据本文公开的各实施例，中继服务器和远程服务器之间的可靠和有序的数据递送可由在其间使用的协议来规定。

[0052] 虽然图 7 显示了用于上游数据（即，经由中继服务器从客户端到远程服务器）的顺序 / 确收号，但根据本文所公开的各实施例，下游数据（即经由中继服务器从远程服务器到客户端）也涉及对应步骤。在一个实施例中，顺序号在中继服务器侧生成并且由客户端消费。根据各实施例，客户端随后生成在中继服务器处消费的确收号。

[0053] 以上的图 3 示出了通过中继服务器 304 扩展了基于浏览器的客户端 302 的功能的示例软件功能模块 300，而图 8A 描绘了根据本文公开的各实施例的用于隧穿 SIP 数据以及用于使用被插入到系统中的用于协助隧穿 SIP 数据的可选的平台服务（诸如通过执行认证）的示例软件功能模块 800。基于浏览器的客户端 802 例如经由 web 服务调用 822 联系中继服务器 804 以配置中继会话。中继服务器 804 的会话管理组件 810（其包括 web 服务 812）经由例如方法调用 806 与中继引擎 814 交互，中继引擎 814 包括用于配置所请求的中继会话的明文 HTTP web 处理程序 816。在各个实施例中，会话管理组件 810 提供通过生成会话标识符等发起以及建立具有客户端 802 和目的（诸如远程服务器 808）之间的连接的 SIP 会话的功能、建立例如会议中涉及的实体间的连接的功能、以及将属于相同中继会话的请求分组的功能。根据一个实施例，会话标识符被经由例如 web 服务调用返回值 822 来返回给客户端。一旦建立了会话，中继引擎组件 814 提供客户端 802 和远程服务器 808 之间的数据交换。在各实施例中，中继引擎 814 还提供分配顺序号和确收号以确保请求和响应消息的可靠和有序递送。

[0054] 在一个实施例中，首先联系 824 可选的（如虚线 820 所示）平台服务组件 820 以访问配置想要的中继会话的许可。根据各实施例，平台服务组件 820 提供例如执行客户端 802 的认证，以及处理密码调用操作和 DNS 解析操作。在一进一步实施例中，认证代理 821 被用作协助客户端执行 SIP 认证的一组可插入平台服务。在这一实施例中，认证代理具有诸如

质询数据之类的信息或数据以传递给基于浏览器的客户端 802 以在创建中继会话之前进行认证，其中中继服务器 804 用作基于浏览器的客户端 802 和远程服务器 808 之间的“中间人”。在又一实施例中，认证组件 826 联系 326 远程服务器 808 以验证客户端 802，以便例如通过如下方式来加入会议：向远程服务器 808 呈现创建中继会话的客户端请求；和 / 或通过获取认证信息或数据（例如，质询数据）以及唯一标识符以便发送 822 给客户端 802 以构成质询响应消息 822。虚线 826 显示了认证组件 820 和远程服务器 808 之间的联系 826 的可选属性。根据各实施例，当远程服务器 808 被联系时，它可验证由中继服务器 804 提供的秘密，并且当该验证成功时，提供质询数据（根据各实施例，包括唯一标识符）给验证组件 820（如联系 826 的双向属性所示）。在又一其它实施例中，没有秘密被提供给远程服务器 808，并且远程服务器 808 提供质询 / 标识符数据而不对来自中继服务器 804 的请求进行任何验证。

[0055] 在认证被执行并成功（或者其中认证起初不被执行，如以上所讨论的）的实施例中，会话管理组件 810 通过例如方法调用来与中继引擎组件 814 交互以配置中继会话。当成功地创建中继会话之后，会话管理组件 810 分配会话 ID 给客户端 802。在一个实施例中，分配给客户端 802 的会话 ID 被用来对属于同一会话的 SIP 请求分组。该会话 ID 被从中继服务器 804 发送 822 给基于浏览器的客户端 802，并且客户端 802 随后使用该会话 ID 作为 HTTP 头部以与中继引擎 814 通信 828。当接收到来自基于浏览器的客户端 802 的数据时，中继引擎 814 与 SSL 流传输模块 818 交互 830 以使用例如 TLS/SSL 832 来将数据 832 中继到远程服务器 808 以及中继来自远程服务器 808 的数据 832。中继引擎 814 由此解开 HTTP 请求中接收或传输的数据并将该数据以用于传输的 TLS/SSL 协议转发给远程服务器 808。中继服务器 804 因而用作用于以 SIP 通信的“隧道”。示例软件功能模块 800 是作为所描述的各实施例的可能的软件功能模块的实例来提供的。其它实施例可包括所描绘的模块、比所描绘的模块和 / 或子模块少的模块、额外的模块和 / 或子模块、模块和 / 或子模块的组合、所描绘的模块和 / 或子模块的组合等。

[0056] 继续到图 8B，示出了用于使用图 8A 中描绘的并且根据本文公开的各实施例的 SSL 流传输模块和可插入认证模块来隧穿 SIP 数据的示例操作步骤 834。过程 834 起始于开始操作 836 并且前进至在中继服务器的会话管理组件处经由例如 web 服务调用接收联系以创建中继会话 838。会话管理组件接着与中继引擎交互以配置所请求的中继会话 844。然而，过程 834 可首先可选地前进至查询 840 以从平台服务组件确定客户端是否被准许（例如，被认证和 / 或被授权）创建该会话。在进行这一确定中 840，中继服务器可诸如通过平台服务组件 820 和 / 或认证代理 821 可选地联系 842 远程服务器 808 以获取质询数据和 / 或认证数据以便完成客户端 802 和远程服务器 808 之间的握手（如步骤 840 和 842 间的箭头的可选双向属性所示）。在其它实施例中，认证代理 821 提供质询数据和 / 或认证数据以完成握手。如果客户端 802 没有被认证和 / 或授权创建中继会话，则过程 834 前进（否）至结束操作 856，过程 834 终止。如果认证和 / 或授权是想要的并且成功，则过程 834 前进（是）到配置中继会话操作 844，其中中继会话被配置 844。在会话管理组件处生成 846 会话 ID 并将其分配 848 给客户端，并且发送给客户端 850。中继引擎随后与用于 SIP 隧穿的传输模块（例如，SSL 流模块）交互以将数据中继到远程服务器 852 并且中继来自远程服务器 852 的数据。SSL 流传输模块随后与远程服务器通信以交换数据 854，并且过程 834 在结束操作 856

终止。图 8B 是根据本文公开的各实施例的用于使用客户端和远程服务器之间的中继服务器通过 HTTP 隧穿 SIP 的可能的操作特性的示例。所示出的操作步骤可被组合到其他步骤中和 / 或被重新安排。此外，可使用例如更少或更多的步骤。

[0057] 接着，图 9 示出显示可选的平台服务如何被插入到整个系统中以协助隧穿某个协议（例如，SIP）数据的示例操作步骤 900。例如，图 9 显示根据本文公开的各实施例的用于协助客户端（例如，HTTP 端点）完成与目的（例如，远程服务器）的认证握手的可插入认证模块的使用。过程 900 因此显示了基于浏览器的客户端将认证委托给中继服务器。过程 900 起始于开始操作 902，并且前进至接收来自基于浏览器的 web 应用 904 的质询数据。中继服务器随后使用从基于浏览器的客户端接收的质询数据来执行认证 906 以生成质询响应以便发送该质询响应给客户端 908。在一实施例中，中继服务器在执行认证 906 时联系远程服务器，而在另一实施例中，中继服务器自己执行认证以为基于浏览器的客户端生成质询响应。当接收到质询响应，基于浏览器的应用将所返回的质询响应组装到新的请求响应中，诸如用于发起与中继服务器和远程服务器的会话的新的 SIP 消息。中继服务器随后接收具有组装的质询响应的新的请求 910 并且发送新的请求给远程服务器 912 以例如发起会话。当确定客户端是有效参与者（未示出），远程服务器发送批准给中继服务器，该批准被中继服务器接收 914。中继服务器随后通知基于浏览器的 web 应用该批准以及会话的发起 916。随后在中继服务器从基于浏览器的 web 应用接收用于交换的数据 918，并且过程 900 在结束操作 920 终止。图 9 是根据本文公开的各实施例的用于通过将认证委托给中继服务器来认证基于浏览器的 web 应用与目的之间的握手的可能的操作特性的示例。所示出的操作步骤可被组合到其他步骤中和 / 或被重新安排。此外，可使用例如更少或更多的步骤。

[0058] 接着，图 10 示出根据本公开的实施例的用于将传输栈（诸如媒体栈）插入到整个系统中以协助通过 RTP/SRTP 隧穿 RDP 数据的示例软件功能模块 1000。基于浏览器的客户端 1002 例如经由 web 服务调用 1018 联系中继服务器 1004 的配置组件以配置 SRTP 信道。在各个实施例中，配置组件 1008 包括 web 服务 1010 并通过例如方法调用 1026 与中继引擎 1012 交互以配置信道。接着，配置组件 1008 配置 1020 加载在中继服务器 1004 上的媒体栈 1016。

[0059] 在模块中，尤其是媒体栈 1016 使得中继服务器 1004 能够扩展基于浏览器的客户端 1002 的功能。根据各个实施例，在中继服务器上加载媒体栈以准许某些协议的隧穿。例如，在 RDP 中继情景中，为了经由 RTP/SRTP 加载 RDP 数据，各实施例还使用了对 RTP/SRTP 以及交互式连接建立（ICE）的知识。例如，ICE 被用于使 RTP/SRTP 通信流量能够穿越防火墙。中继服务器由此加载支持 RTP/SRTP/ICE 的媒体栈，因为 RDP 数据通常经由 RTP/SRTP 运送到屏幕共享服务器。在涉及 RDP 中继和建立与屏幕共享服务器的连接的实施例中，基于 web 的客户端以 SIP 与屏幕共享服务器通信以建立中继服务器和屏幕共享服务器之间的 RTP/SRTP/ICE 连接。在中继服务器上加载 RTP/SRTP/ICE 对这一过程有帮助。客户端随后能够以 SIP 与屏幕共享服务器通信，因为一部分 SIP 消息主体（即会话描述协议（SDP）部分）是经由 web 服务调用从中继服务器检索到的。类似的，来自屏幕共享服务器的 SIP 请求的 SDP 被经由 web 服务调用传递到中继服务器。因此，中继服务器对媒体栈的加载使得能够在各个环境中传输 RDP 数据，而在其他情况下，在这些环境中这些传输的进行将受到限制。例如，RTP/SRTP 和 ICE 的媒体栈通常在 Mac 平台不可用。例如，在 Mac 平台，开发者要么将媒

体栈转接到本机 Mac，要么在基于 web 的客户端里开发媒体栈。然而，这些解决方案是复杂的，并且通过这种转接和 / 或开发仍然存在受限的功能。

[0060] 回到图 10，如以上所讨论的，为了经由 RTP/SRTP 加载 RDP 数据，在各实施例中使用 RTP/SRTP 以及 ICE 的知识。在一实施例中，这一配置涉及与远程 SIP/RTP 端点 1006 通信以进行连通性检查，以确定连接是否能被进行。在另一实施例中，不进行连通性检查。当配置 SRTP 信道和媒体栈时，客户端 1002 经由 HTTP 发送 / 接收 RDP 数据 1022 给包括明文 (plain) HTTP web 处理程序 (handler) 1014 的中继引擎 1012 以便配置中继会话。中继引擎 1012 随后与媒体栈 1016 通信 1024 以通过在媒体栈 1016 和远程 RTP 端点 1006 之间交换与 RTP 有关的消息 1028 来获取 RDP 数据。软件功能模块 1000 是作为所描述的各实施例的可能的软件功能模块的实例来提供的。其它实施例可包括所描绘的模块、比所描绘的模块和 / 或子模块少的模块、额外的模块和 / 或子模块、模块和 / 或子模块的组合、所描绘的模块和 / 或子模块的组合等。

[0061] 图 10 描绘了用于将诸如媒体栈之类的传输栈插入到整个系统中以协助通过 RTP/SRTP 隧穿 RDP 数据的示例软件功能模块，而图 11 示出了根据本公开的实施例的用于使用可插入传输栈来通过 RTP/SRTP 隧穿 RDP 数据的示例操作步骤 1100。过程 1100 起始于开始操作 1102，并且前进至操作 1104，其中诸如经由例如 web 服务调用来联系客户端和远程 RTP 端点之间的中继服务器来配置用于隧穿 RDP 数据的 SRTP 信道。接着，配置组件配置可插入媒体栈 1106 并且在这样做时可选地 (如虚线所示) 与远程 RTP 端点通信以进行连通性检查 1107。RTP 端点通过如 1106 和 1107 之间的箭头的双向属性所显示的信息来响应。客户端随后经由 HTTP 发送 RDP 数据至中继引擎 1108/ 从中继引擎 1108 接收 RDP 数据。接着中继引擎与媒体栈通信以获取 RDP 数据 1110。为了获取 RDP 数据，媒体栈与远程 RTP 端点 1112 交换 RTP 消息。过程 1100 在结束操作 1114 中止。图 11 是根据本文公开的各实施例的用于使用可插入传输栈通过 RTP/SRTP 隧穿 RDP 数据的可能的操作特性的示例。所示出的操作步骤可被组合到其他步骤中和 / 或被重新安排。此外，可使用例如更少或更多的步骤。

[0062] 最后，图 12 示出可在其上实现本文公开的各实施例的示例计算机系统 1200。根据本文公开的各实施例，描绘了诸如客户端计算机 202、中继服务器 206 或远程服务器 208 之类的、具有至少一个处理器 1202 用于如图 2 中所示的交换消息数据的计算机系统 1200。系统 1200 具有系统存储器 1204，包括例如易失性存储器和非易失性存储器。在其最基本的配置中，计算系统 1200 在图 12 中由虚线 1206 示出。另外，系统 1200 还可包括另外的存储 (可移动和 / 或不可移动)，其中包括但不限于磁盘、光盘或磁带。在图 12 中通过可移动存储 1208 和不可移动存储 1210 示出这样的附加存储。

[0063] 本文所使用的术语计算机可读介质可包括计算机存储介质。计算机存储介质可包括以用于存储诸如计算机可读指令、数据结构、程序模块、或其他数据等信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。系统存储器 1204、可移动存储 1208 和不可移动存储 1210 都是计算机存储介质 (即，存储器存储) 的示例。计算机存储介质可包括，但不限于，RAM、ROM、电可擦除只读存储器 (EEPROM)、闪存或其他存储器技术、CD-ROM、数字多功能盘 (DVD) 或其他光存储、磁带盒、磁带、磁盘存储或其他磁性存储设备、或者可用于存储信息且可由计算设备 1200 访问的任何其他介质。任何这样的计算机存储

介质都可以是设备 1200 的一部分。图 12 中的说明不意图以任何方式限制本公开的范围。

[0064] 本文所使用的术语计算机可读介质还可包括通信介质。通信媒介可由诸如载波或其他传输机制等已调制数据信号中的计算机可读指令、数据结构、程序模块、或其他数据来体现，并且包括任何信息传递介质。术语“已调制数据信号”可以描述以对该信号中的信息进行编码的方式设定或者改变其一个或多个特征的信号。作为示例而非限制，通信介质包括诸如有线网络或直接线连接等有线介质，以及诸如声学、射频（RF）、红外线和其他无线介质等无线介质。

[0065] 系统 1200 还可包含允许该设备与其它设备通信的通信连接 1216。此外，为了输入内容到例如客户端计算机 202 上的用户界面（UI）（例如由客户端计算机 202 上的相应 UI 模块（未示出）所提供的）的各字段中，根据本公开的一实施例，系统 1200 可具有诸如键盘、鼠标、笔、语音输入设备、触摸输入设备等之类的输入设备 1214。还可包括输出设备 1212，诸如显示器、扬声器、打印机等。所有这些设备在本领域中是公知的并且不必在此详细讨论。上述设备是示例，并且可使用其他设备。

[0066] 以上参考附图描述了本发明的各实施例，可以理解，可以对本发明做出本领域技术人员易于想到且被包含在所公开并如所附权利要求书所定义的本发明的精神和范围内的众多修改。尽管出于本发明的目的描述了各实施方式，但可以做出落入本发明的范围内的各种改变和修改。

[0067] 同样地，虽然本发明使用了对结构特征、方法动作和含有这些动作的计算机可读介质专用的语言，但是应该理解，在所附权利要求书中定义的本发明不必限于此处描述的具体结构、动作、特征或介质。相反，上述具体特征和动作是作为实现权利要求的示例形式而公开的。实施例的各方面允许多个客户端计算机、多个远程服务器、多个中继服务器、以及多个网络等。或者，在其它实施例中，使用具有单个远程服务器、单个中继服务器、以及单个网络的单个客户端计算机。所属领域技术人员将认识到在本公开的范围和精神内的其他实施例或改进。因此，这些具体结构、动作、或介质是作为实现所要求保护的本发明的示例性实施例而公开的。本发明由所附权利要求书进行定义。

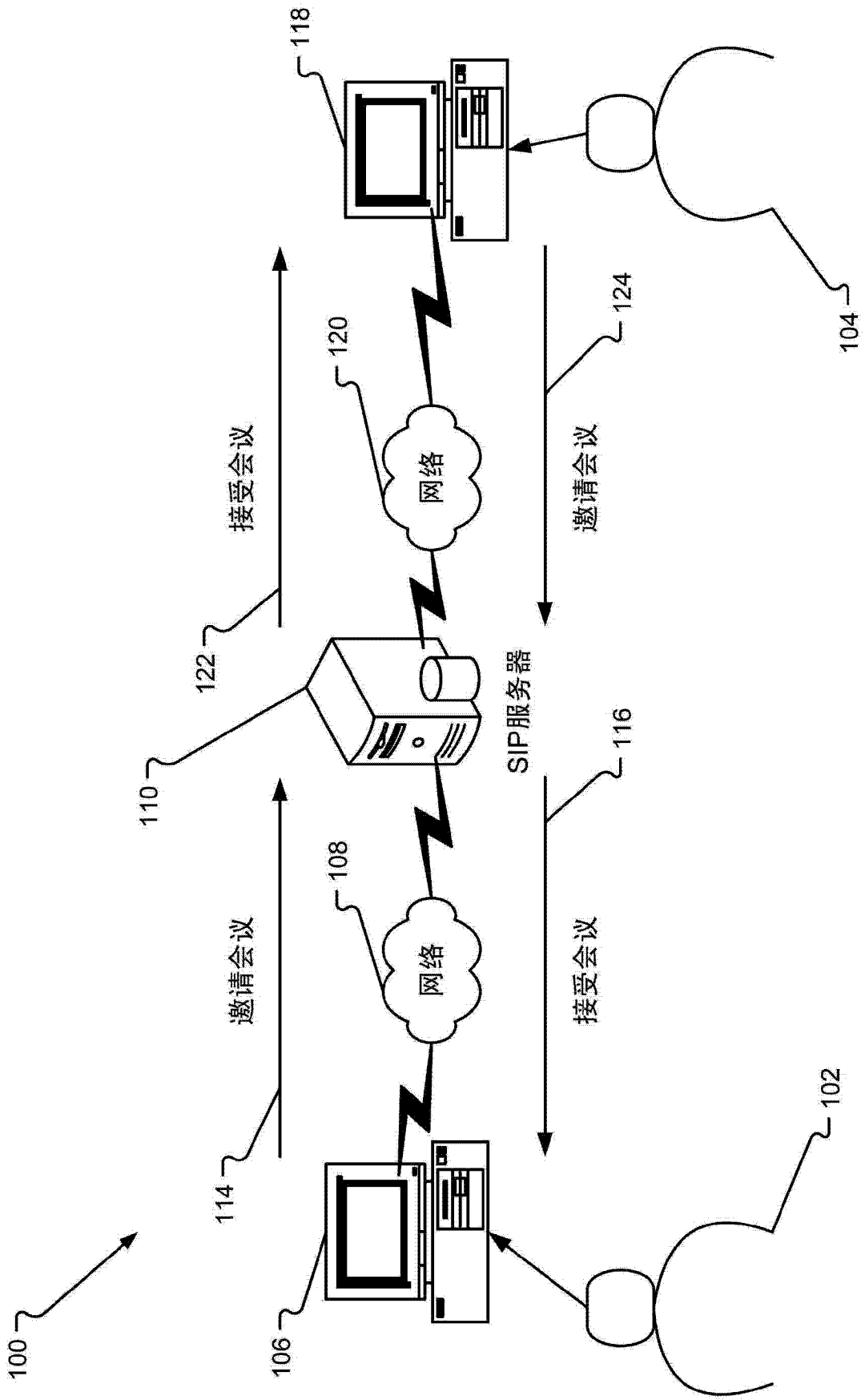

100
102
104
106
108
110
114
116
118
120
122
124
网络
网络
SIP服务器
邀请会议
接受会议
接受会议
邀请会议

图 1

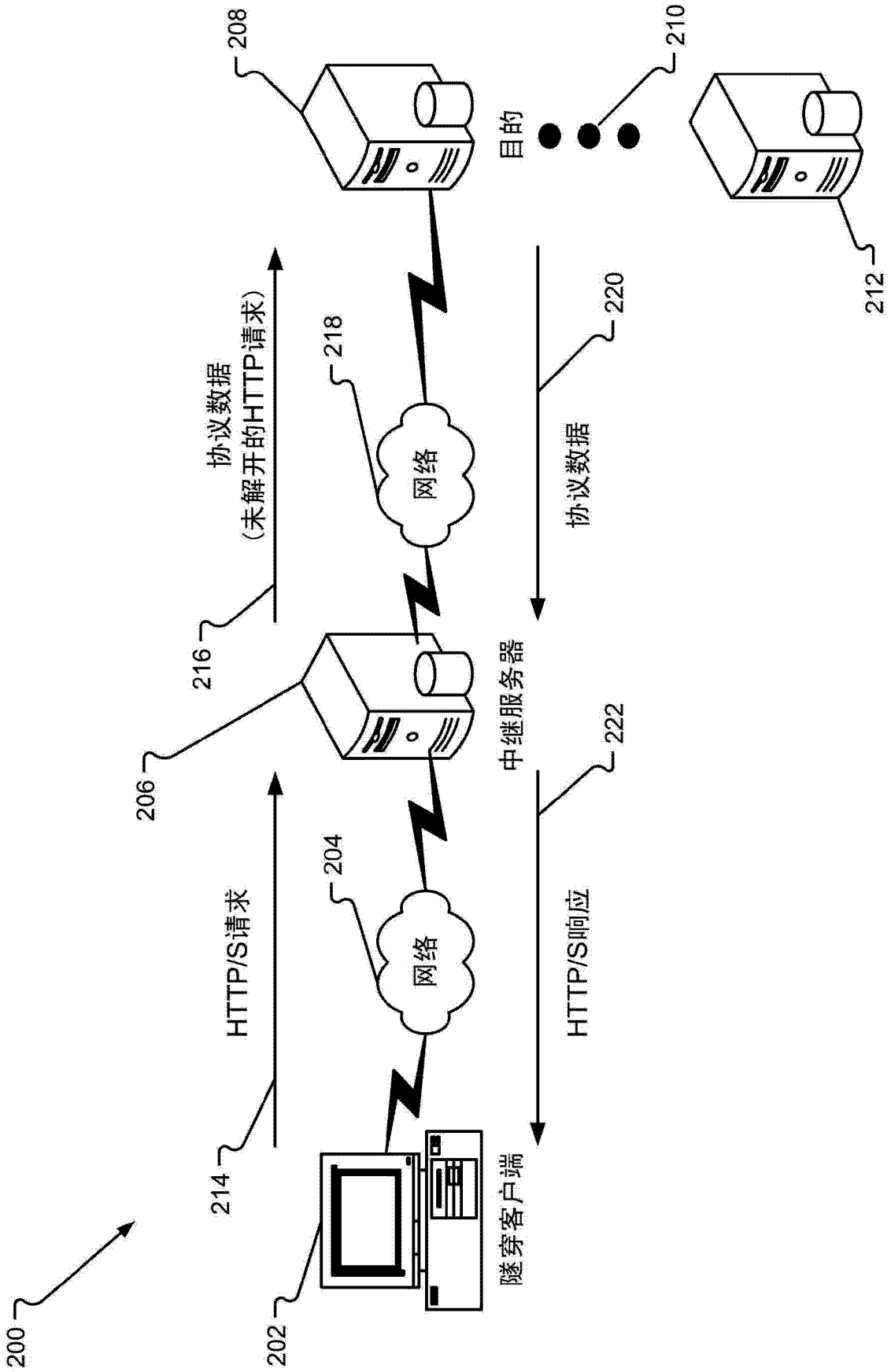

200
202
隧穿客户端
214
HTTP/S请求
204
网络
206
中继服务器
216
协议数据
(未解开的HTTP请求)
218
网络
208
目的
210
212
220
协议数据
222
HTTP/S响应

图 2

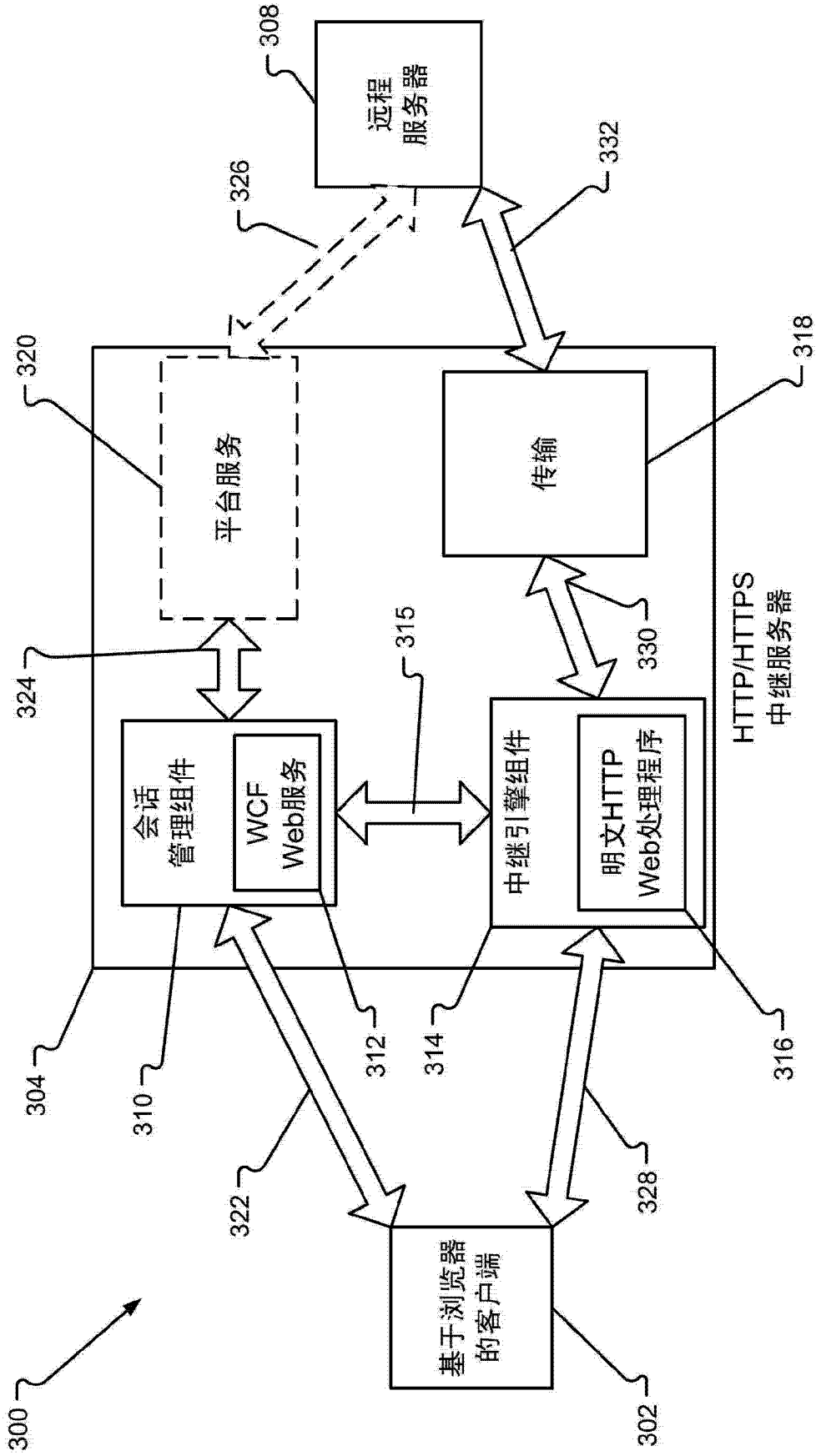

远程
服务器
308
332
326
320
平台服务
传输
318
HTTP/HTTPS
中继服务器
315
330
324
会话
管理组件
WCF
Web服务
中继引擎组件
明文HTTP
Web处理程序
304
310
312
314
316
322
328
基于浏览器
的客户端
300
302

图 3

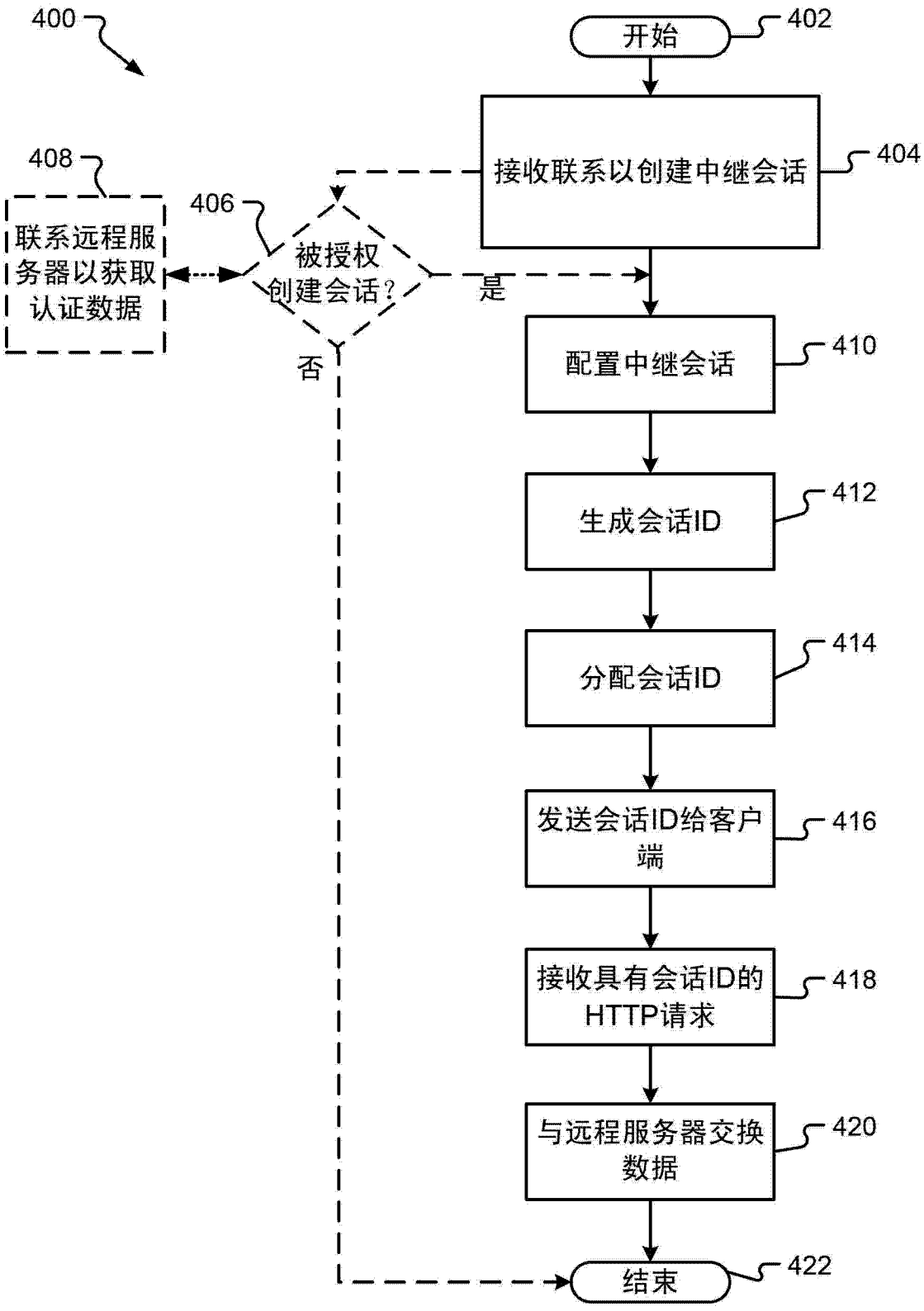

400
开始
402
接收联系以创建中继会话
404
408
联系远程服务器以获取认证数据
406
被授权创建会话?
是
否
配置中继会话
410
生成会话ID
412
分配会话ID
414
发送会话ID给客户端
416
接收具有会话ID的HTTP请求
418
与远程服务器交换数据
420
结束
422

图 4

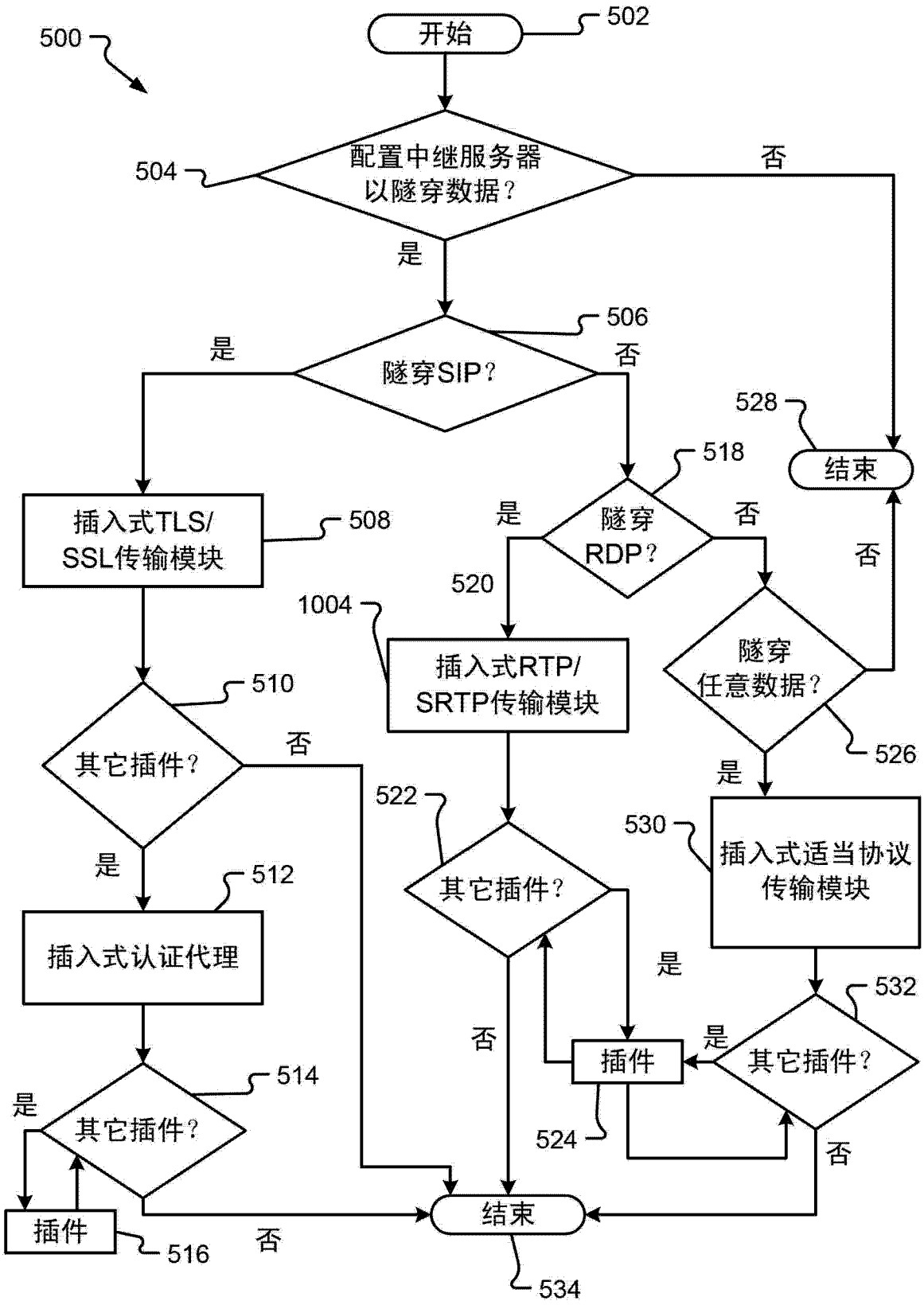

500
开始
502
配置中继服务器以隧穿数据？
504
否
是
隧穿SIP？
506
是
否
528
结束
518
插入式TLS/SSL传输模块
508
是
隧穿RDP？
否
否
520
1004
插入式RTP/SRTP传输模块
隧穿任意数据？
526
是
510
其它插件？
否
522
530
插入式适当协议传输模块
是
512
其它插件？
插入式认证代理
是
否
532
插件
是
其它插件？
514
是
其它插件？
524
否
插件
516
否
结束
534

图 5

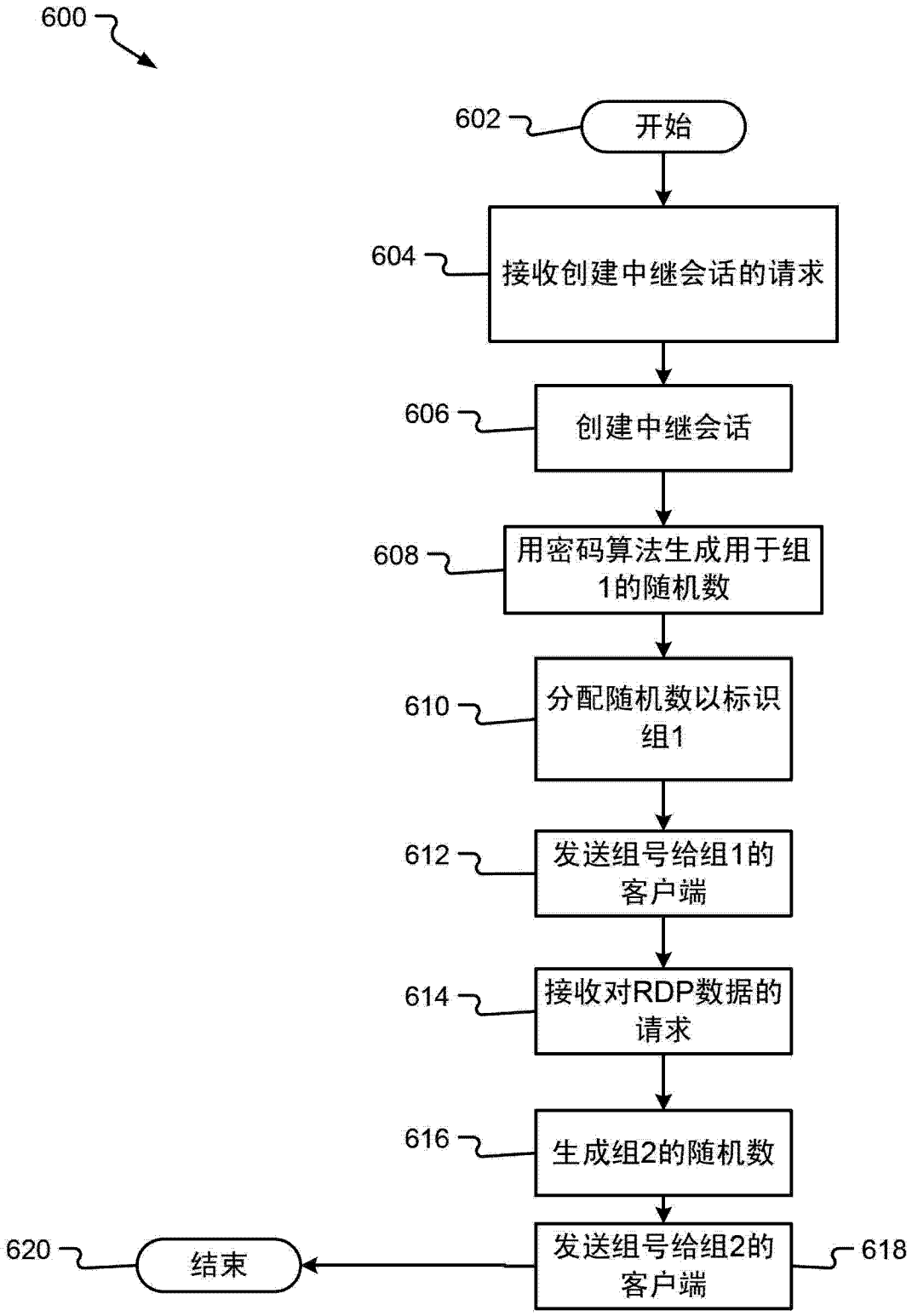

600
602
开始
604
接收创建中继会话的请求
606
创建中继会话
608
用密码算法生成用于组1的随机数
610
分配随机数以标识组1
612
发送组号给组1的客户端
614
接收对RDP数据的请求
616
生成组2的随机数
618
发送组号给组2的客户端
620
结束

图 6

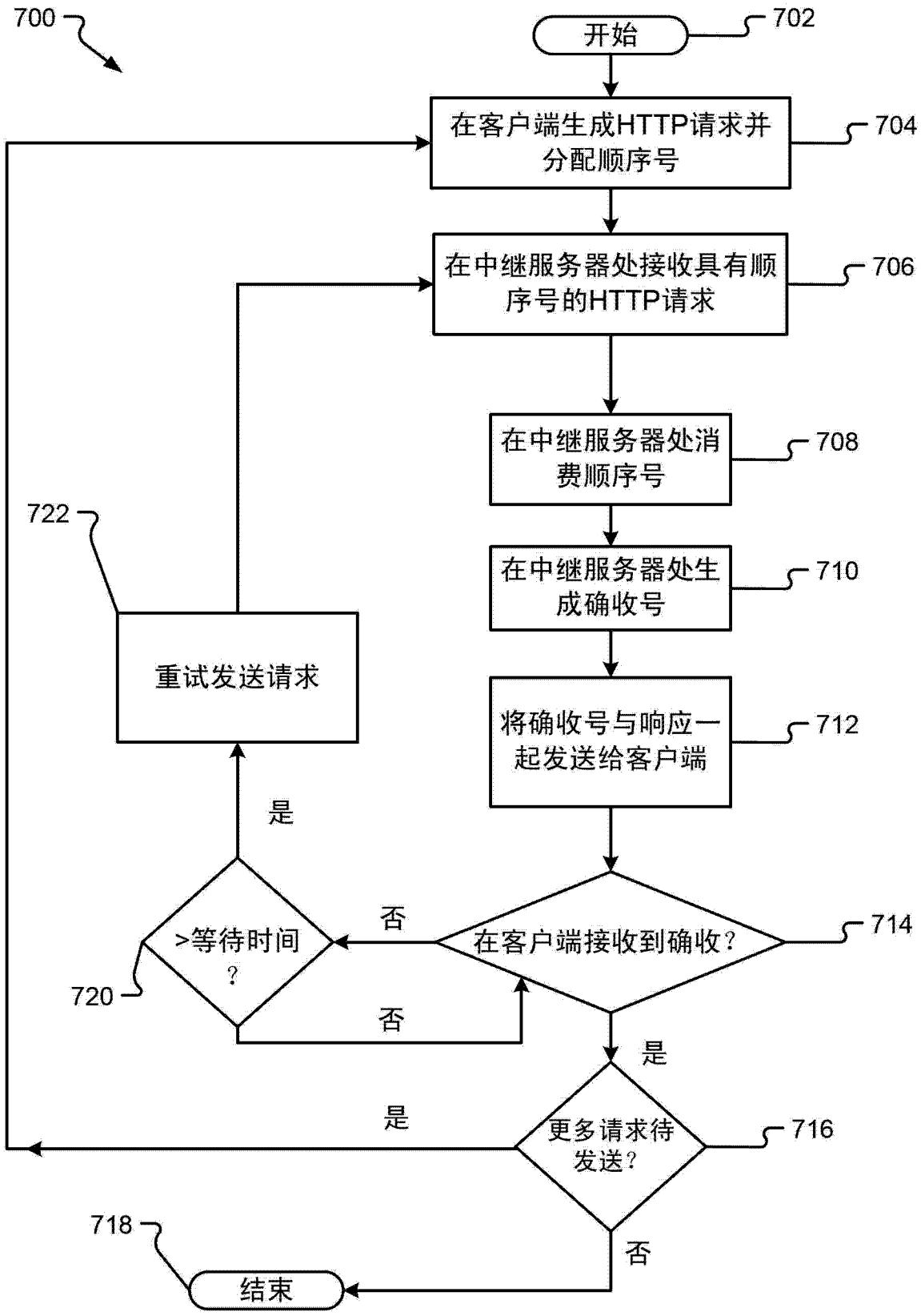

700
开始
702
在客户端生成HTTP请求并分配顺序号
704
在中继服务器处接收具有顺序号的HTTP请求
706
在中继服务器处消费顺序号
708
在中继服务器处生成确收号
710
将确收号与响应一起发送给客户端
712
在客户端接收到确收？
714
否
>等待时间？
720
否
是
722
重试发送请求
是
更多请求待发送？
716
是
否
结束
718

图 7

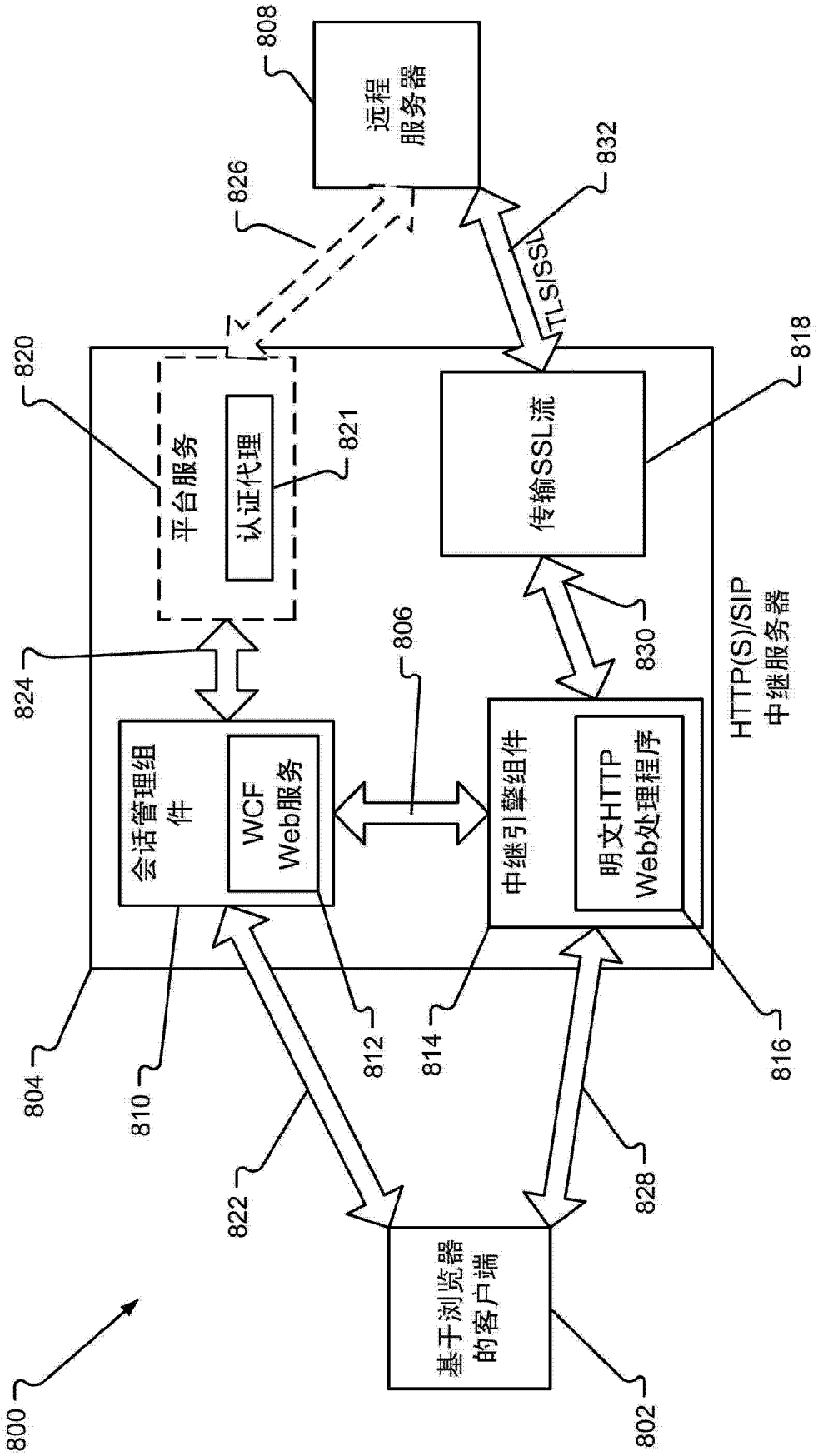

远程服务器
808
826
832
TLS/SSL
820
平台服务
认证代理
821
传输SSL流
818
824
806
830
会话管理组件
WCF Web服务
中继引擎组件
明文HTTP Web处理程序
HTTP(S)/SIP 中继服务器
804
810
812
814
816
822
828
基于浏览器的客户端
800
802

图 8A

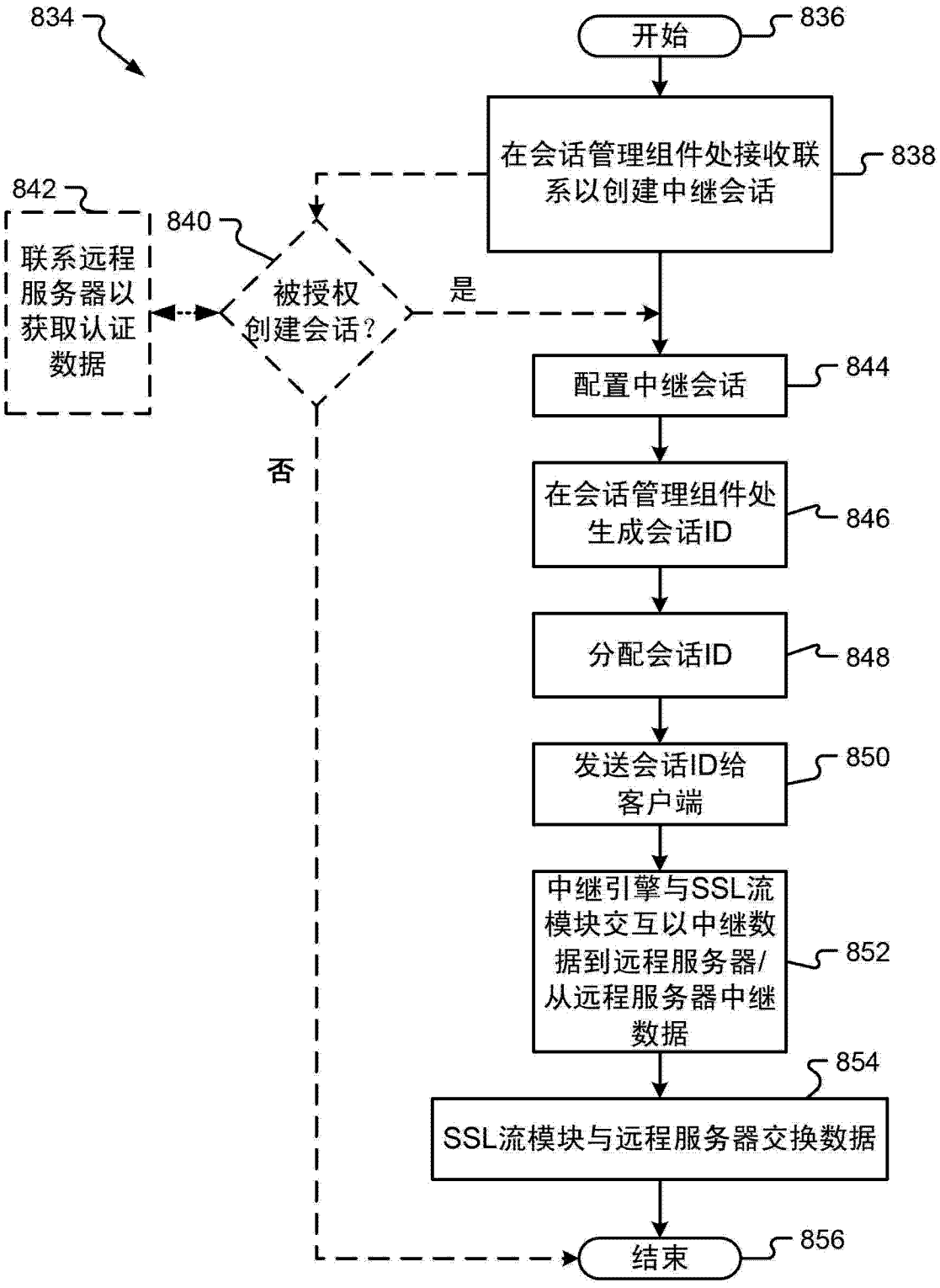

834
开始
836
在会话管理组件处接收联系以创建中继会话
838
842
联系远程服务器以获取认证数据
840
被授权创建会话？
是
否
配置中继会话
844
在会话管理组件处生成会话ID
846
分配会话ID
848
发送会话ID给客户端
850
中继引擎与SSL流模块交互以中继数据到远程服务器/从远程服务器中继数据
852
854
SSL流模块与远程服务器交换数据
结束
856

图 8B

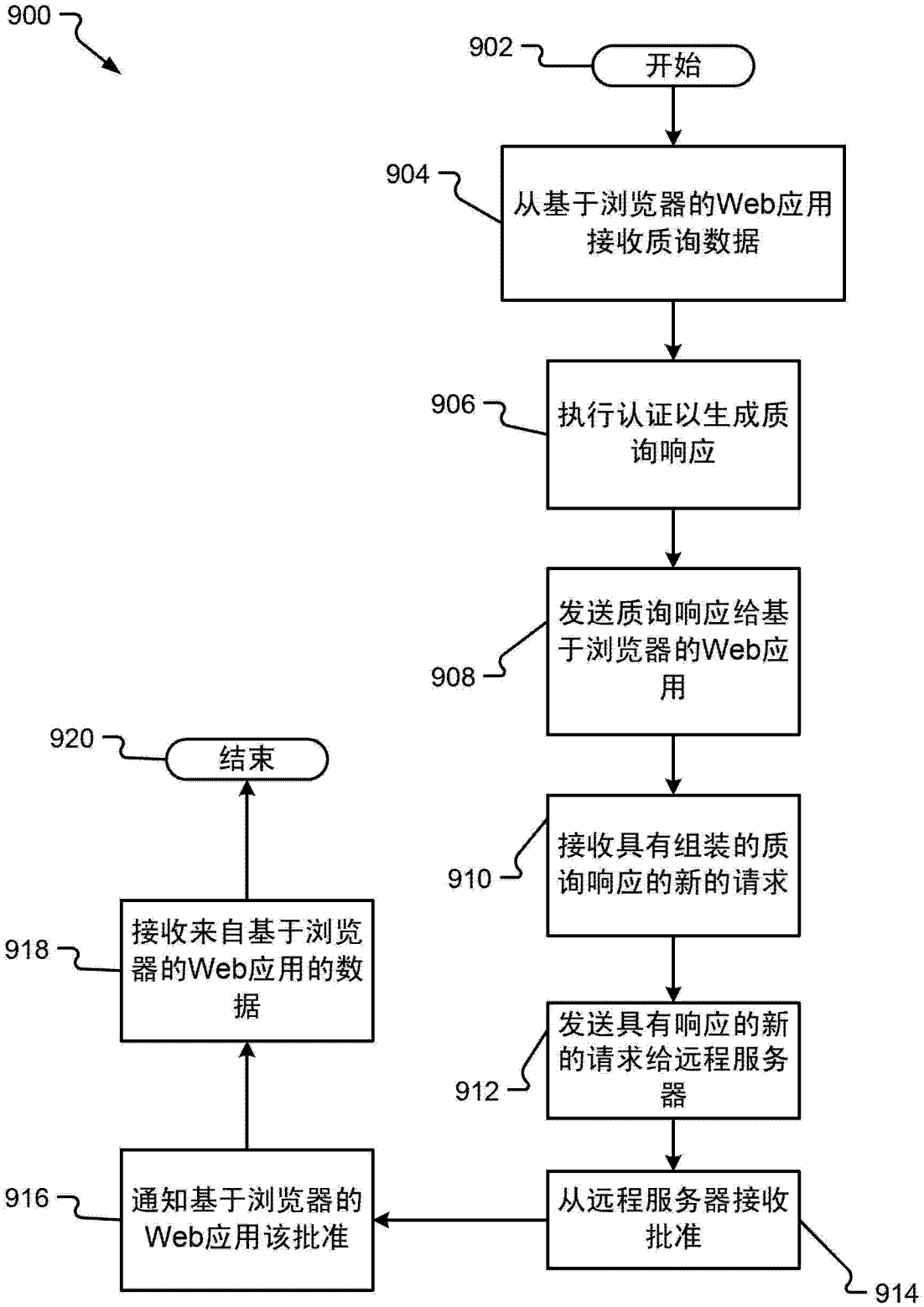

900
902
开始
904
从基于浏览器的Web应用接收质询数据
906
执行认证以生成质询响应
908
发送质询响应给基于浏览器的Web应用
910
接收具有组装的质询响应的新的请求
912
发送具有响应的新的请求给远程服务器
914
从远程服务器接收批准
916
通知基于浏览器的Web应用该批准
918
接收来自基于浏览器的Web应用的数据
920
结束

图 9

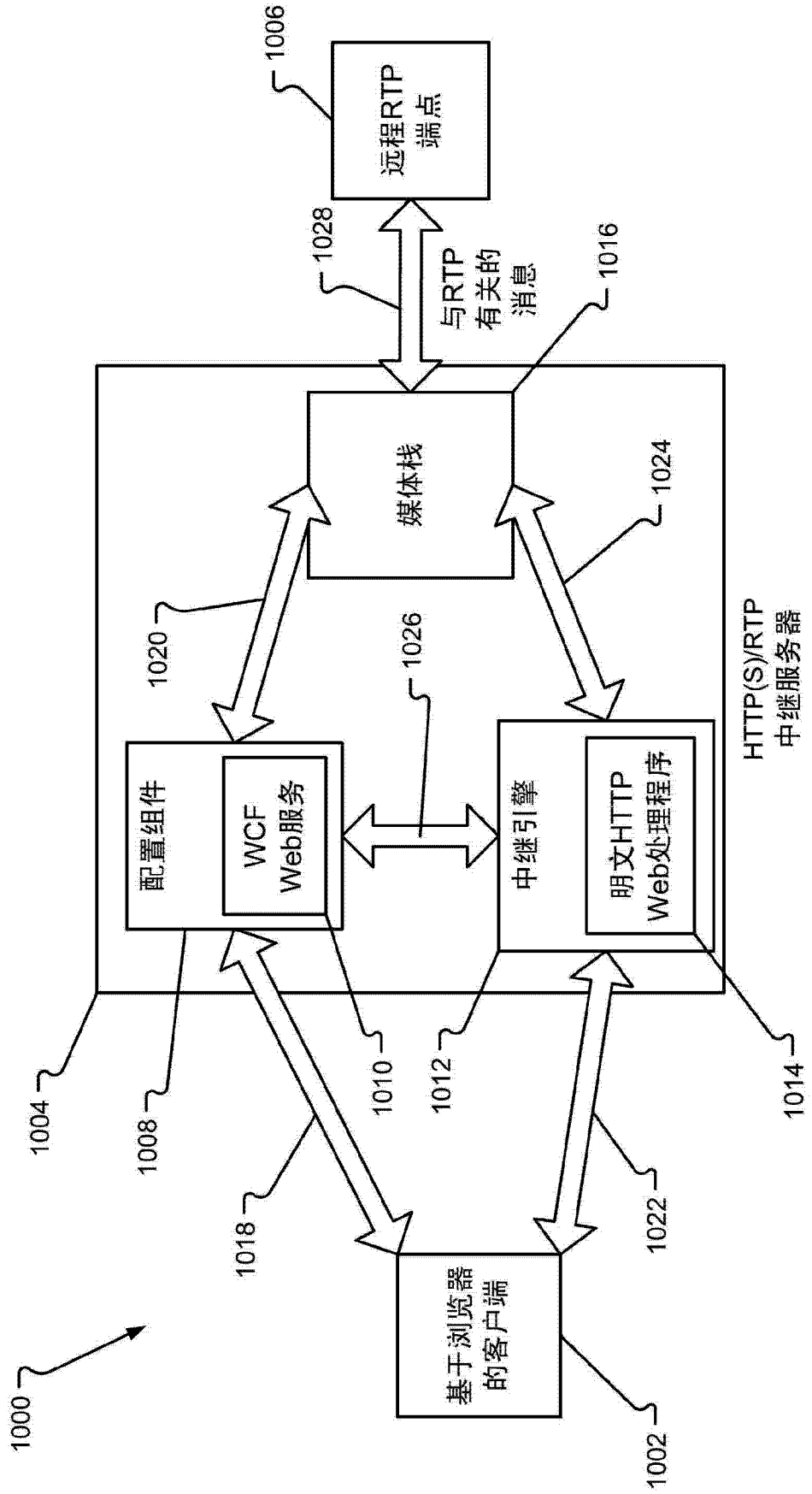

1006
远程RTP
端点
1028
与RTP
有关的
消息
1016
媒体栈
1024
1020
1026
配置组件
WCF
Web服务
中继引擎
明文HTTP
Web处理程序
HTTP(S)/RTP
中继服务器
1004
1008
1010
1012
1014
1018
1022
基于浏览器
的客户端
1000
1002

图 10

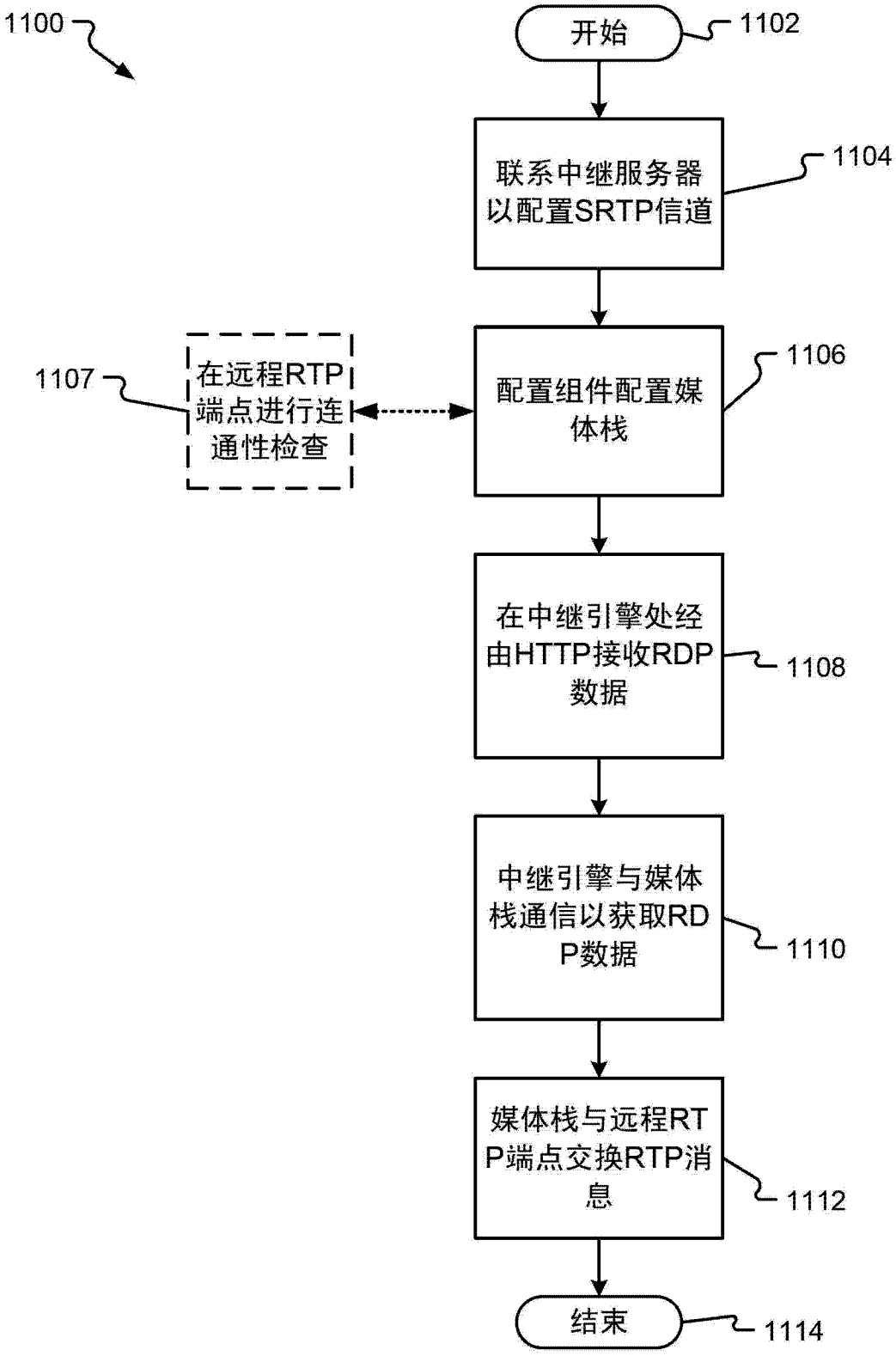

1100
开始
1102
联系中继服务器以配置SRTP信道
1104
在远程RTP端点进行连通性检查
1107
配置组件配置媒体栈
1106
在中继引擎处经由HTTP接收RDP数据
1108
中继引擎与媒体栈通信以获取RDP数据
1110
媒体栈与远程RTP端点交换RTP消息
1112
结束
1114

图 11

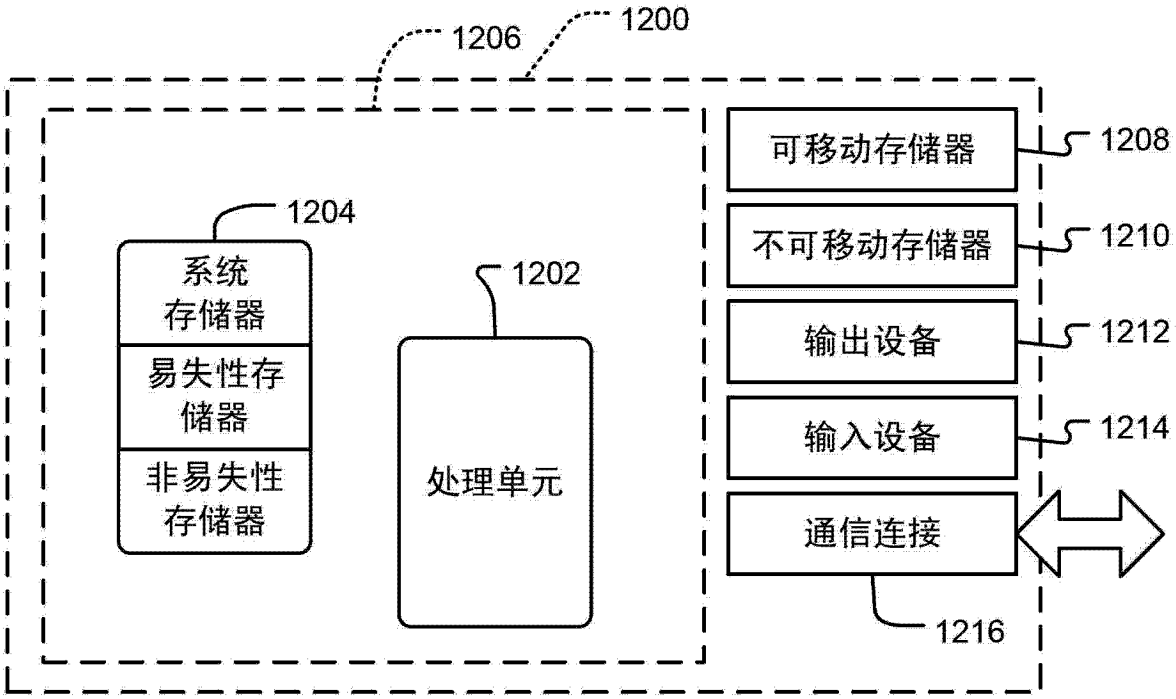

1206
1200
1204
系统
存储器
易失性存
储器
非易失性
存储器
1202
处理单元
可移动存储器
1208
不可移动存储器
1210
输出设备
1212
输入设备
1214
通信连接
1216

图 12