

一种虚拟内网加速方法及系统、配置方法、存储介质和计算机设备

本文要求在 2018 年 11 月 30 日提交中国专利局、申请号为 201811459242.1, 发明名称为“一种虚拟内网加速方法、系统和计算机设备”的中国专利申请的优先权, 其全部内容通过引用结合在本文中。

技术领域

本文涉及软件定义广域网 (SD-WAN) 领域, 尤其涉及一种虚拟内网加速方法及系统、配置方法、存储介质和计算机设备。

背景技术

传统大型企业通常会有大量全国分公司或分部。分部规模通常都比较大, 主要是承担区域本地化职能, 有专门的 IT 部门负责网络管理和运营, 部署独立的服务。总部需要访问分部的服务, 分部也需要访问总部的服务。在互联网云时代, 企业也会大量使用云服务, 购买云机房, 企业要访问云机房内服务。通常为了安全及方便管理等方面, 企业通常会将总部和分部及云机房采用网络技术实现内网打通, 相互访问都是内网服务形式。

由于直接部署专线的方案成本居高不下, 以及使用虚拟专用网络 (Virtual Private Network, VPN) 方式不能保证链路稳定等原因, 很多企业会采购 SD-WAN 产品来实现分支及云机房互联, 以下以分支互联来具体说明。基本架构如图 1 所示, 分支之间通过部署客户终端设备 (Customer Premise Equipment, CPE) 实现内网打通, 内网之间交换的数据通过 SD-WAN 动态链路加速传输, 大部分情况下可以良好满足企业需求。

当前预防传输过程中丢包的通常做法是对同一数据包进行多份传输, 通过多份传输的方式尽量降低丢包的几率。比如内网用户的一个传输控制协议 (Transmission Control Protocol, TCP) 包, 在 SD-WAN 网络内网使用发送两到三份相同的数据, 走不同路径。多份传输占用不同路径, 在传输数据量较大的情况下会增加对网络资源的消耗, 且不能完全避免丢包的发生。

发明内容

为克服相关技术中存在的问题，本文提供一种虚拟内网加速方法及系统、配置方法、存储介质和计算机设备。

根据本文的第一方面，提供一种虚拟内网加速方法，包括：

发起端的客户端设备 CPE 在接收到发起端的服务器向接收端的服务器发送的 TCP 请求时，将所述 TCP 请求的信息传输至接收端的 CPE；

所述接收端的 CPE 根据所述 TCP 请求的信息，配置所述发起端的服务器与所述接收端的服务器之间的连接链；

通过所述连接链，传输 TCP 请求和/或 TCP 响应数据。

其中，上述方法中，所述发起端的 CPE 在接收到发起端的服务器向接收端的服务器发送的 TCP 请求时，将所述 TCP 请求的信息传输至接收端的 CPE 的步骤包括：

所述发起端的 CPE 检测到 TCP 请求；

所述发起端的 CPE 将分支服务器发送的 TCP 请求的信息使用私有协议封装后，通过与所述 TCP 请求对应的端口向所述接收端的 CPE 发送，所述 TCP 请求的信息至少包含如下信息：

请求数据、作为目标的接收端的服务器的 IP 及端口、作为请求来源的发起端的服务器的 IP 及端口。

其中，上述方法中，所述发起端的 CPE 通过 SD-WAN 的可靠传输方式将所述 TCP 请求的信息传输至所述接收端的 CPE。

其中，上述方法中，所述接收端的 CPE 根据所述 TCP 请求的信息，配置所述连接链的步骤包括：

所述接收端的 CPE 在接收到所述 TCP 请求的信息后，使用所述私有协议解析；

对所述接收端的服务器的 IP 及端口发起连接，配置目标端；

将所述发起端的服务器的 IP 及端口配置为源端；

在所述目标端及所述源端之间建立连接链。

其中，上述方法中，所述发起端的服务器为分支服务器，所述接收端的服务器为总部服务器；或，

所述发起端的服务器为总部服务器，所述接收端的服务器为分支服务器。

根据本文的另一方面，提供一种配置方法，用于配置接收端的服务器与发起端的服务器之间的 SD-WAN 连接链，其中，

接收端的 CPE 接收由发起端的 CPE 发出的使用私有协议封装后的 TCP 请求的信息，并使用所述私有化协议对所述 TCP 请求的信息进行解析；

所述接收端的 CPE 对接收端的服务器的 IP 及端口发起连接，配置为目标端；

所述接收端的 CPE 将发起端的服务器的 IP 及端口配置为源端；

所述接收端的 CPE 在所述目标端与所述源端之间建立连接链。

根据本文的另一方面，提供一种虚拟内网加速系统，至少包括软件定义广域网 SD-WAN 连接的发起端的服务器、接收端的服务器、发起端的客户端设备 CPE 和接收端的 CPE；

所述发起端的 CPE，用于在接收到所述发起端的服务器向所述接收端的服务器发送的 TCP 请求时，将所述 TCP 请求的信息传输至所述接收端的 CPE；

所述接收端的 CPE，用于根据所述 TCP 请求的信息，配置所述发起端的服务器与所述接收端的服务器之间的连接链；

所述发起端的服务器与所述接收端的服务器，用于通过所述连接链，传输 TCP 请求和/或 TCP 响应数据。

其中，上述系统中，所述发起端的 CPE，用于检测 TCP 请求；

将分支服务器发送的 TCP 请求的信息使用私有协议封装后，通过与所述 TCP 请求对应的端口向所述接收端的 CPE 发送，所述 TCP 请求的信息至少包含如下信息：

请求数据、作为目标的接收端的服务器的 IP 及端口、作为请求来源的发起

端的服务器的 IP 及端口。

其中，上述系统中，所述连接链承载于所述发起端的 CPE 与所述接收端的 CPE 之间的 SD-WAN 可靠传输通道上。

其中，上述系统中，所述接收端的 CPE，用于在接收到所述 TCP 请求的信息后，使用所述私有协议解析，对所述接收端的服务器的 IP 及端口发起连接，配置目标端，将所述发起端的服务器的 IP 及端口配置为源端，在所述目标端及源端之间建立连接链。

根据本文的另一方面，提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被执行时实现如上所述的虚拟内网加速方法的步骤。

根据本文的另一方面，提供一种计算机装置，包括处理器、存储器和存储于所述存储器上的计算机程序，所述处理器执行所述计算机程序时实现如上所述的虚拟内网加速方法的步骤。

本文实现了发起端与接收端之间的 TCP 连接透明加速，对 TCP 连接传输进行了加速，有效的避免了丢包的发生，解决了现有预防丢包处理方式资源消耗量大且效果欠佳的问题。

附图说明

构成本文的一部分的附图用来提供对本文的进一步理解，本文的示意性实施例及其说明用于解释本文，并不构成对本文的不当限定。在附图中：

图 1 是根据一示例性实施例示出的一种 SD-WAN 基本架构示意图。

图 2 是根据一示例性实施例示出的一种虚拟内网加速方法的流程图。

图 3 是图 2 所示流程中步骤 201 的具体流程图。

图 4 是图 3 所示流程中步骤 202 的具体流程图。

图 5 是根据一示例性实施例示出的一种虚拟内网加速方法的实现原理示意

图。

图 6 是根据一示例性实施例示出的一种虚拟内网加速系统的架构框图。

图 7 是根据一示例性实施例示出的一种计算机设备的框图。

具体实施方式

为使本文实施例的目的、技术方案和优点更加清楚，下面将结合本文实施例中的附图，对本文实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本文一部分实施例，而不是全部的实施例。基于本文中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本文保护的范围。需要说明的是，在不冲突的情况下，本文中的实施例及实施例中的特征可以相互任意组合。

当前预防传输过程中丢包的通常做法是对同一数据包进行多份传输，通过多份传输的方式尽量降低丢包的几率。比如内网用户的一个 TCP 包，在 SD-WAN 网络内网使用发送两到三份相同的数据，走不同路径。多份传输占用不同路径，在传输数据量较大的情况下会增加对网络资源的消耗，且不能完全避免丢包的发生。

针对上述问题，本文实施例提供了一种虚拟内网加速方法及系统、配置方法、存储介质和计算机设备。

本文的一实施例提供了一种虚拟内网加速方法，使用该方法完成 SD-WAN 中数据传输的流程如图 2 所示，包括：

步骤 201、发起端的 CPE 在接收到发起端的服务器发送的 TCP 请求时，将该 TCP 请求的信息传输至接收端的 CPE。

步骤 202、接收端的 CPE 根据 TCP 请求的信息，配置发起端的服务器与接收端的服务器之间的连接链。

步骤 203、通过连接链，在源端和目标端之间传输 TCP 请求和/或 TCP 响应数据。

本文实施例中，发送端至少包括有服务器和 CPE。接收端至少也包括有服

务器和 CPE。

发起端的服务器可以为分支服务器，接收端的服务器可以为总部服务器；或者，

发起端的服务器为总部服务器，接收端的服务器为分支服务器。

其中，假设发起端的服务器为分支服务器，接收端的服务器为总部服务器时，上述步骤 201 的执行过程如图 3 所示，可以分为如下操作步骤 301 至 302：

步骤 301、发起端的 CPE 检测到 TCP 请求；

步骤 302、发起端的 CPE 将分支服务器发送的 TCP 请求的信息使用私有协议封装后，通过与 TCP 请求对应的端口发送给接收端的 CPE；

其中，本文中涉及的 TCP 请求的信息至少包含如下信息：

请求数据、作为请求目标的接收端的服务器的 IP 及端口、作为请求来源的发起端的服务器的 IP 及端口。

本文中，与 TCP 请求对应的端口指，预先为发起该 TCP 请求的用户分配的端口。即可以预先为不同的用户分别分配对应的端口，以传输该用户所请求的数据。其中，发起该 TCP 请求的用户可以是个人用户，也可以是业务服务商。

在向接收端的 CPE 发送数据时，发起端的 CPE 可以通过 SD-WAN 的可靠传输方式将 TCP 请求的信息传输至接收端的 CPE。

其中，本文实施例中，发起端的 CPE 与接收端的 CPE 还可以通过 SD-WAN 的可靠传输方式传输非 TCP 数据。

上述步骤 202 的执行过程如图 4 所示，可以分为以下步骤 401 至步骤 404：

步骤 401、接收端的 CPE 在接收到 TCP 请求的信息后，使用私有协议解析 TCP 请求的信息，获取请求数据、作为请求目标的接收端的服务器的 IP 及端口、作为请求来源的发起端的服务器的 IP 及端口；

步骤 402、对所获取的接收端的服务器的 IP 及端口发起连接，并将接收端的服务器的 IP 及端口配置为目标端；

步骤 403、将发起端的服务器的 IP 及端口配置为源端；

步骤 404、在目标端及源端之间建立连接链。

SD-WAN 虚拟网络通道传输的包都是 IP 包，主要分为 UDP 和 TCP 两种，其中 UDP 是无连接模式，而 TCP 是基于连接的可靠传输方式，TCP 会对传输过程丢失的数据包进行重传以确保传输可靠。

为确保不出现 TCP over TCP 的问题，通常 SD-WAN 网络底层传输都是使用普通 UDP 传输方式，不做可靠传输。SD-WAN 网络探测到 POP，认为网络出现丢包，则使用动态路由切换功能切换到另外的良好链路上去。采用这种做法，内网用户的 TCP 连接可以感知短暂丢包，出现丢包后，由用户的 TCP 连接发起重传。另外，内网用户的 UDP 连接也会出现传输丢包的情况，此时，可能需要内网用户手动重传。

本文实施例提供的虚拟内网加速方法，能够高效、可靠的传输 TCP 及非 TCP 包，成功的消除了网络抖动对传输产生的影响，极大的节约了网络资源并提升了用户体验。

本文的一实施例还提供了一种虚拟内网通信方法，可以解决虚拟通道传输在网络抖动情况下存在丢包的问题。

本文实施例中使用透明代理的方式实现 TCP 透明传输。在两个子网络之间，SD-WAN 网络使用可靠传输方式实现传输加速及规避丢包。

下面以一个常规分支内网到总部内网请求和响应的过程为例，来描述虚拟内网通信的过程，该过程的原理如图 5 所示。

当图 5 中所示的企业分支的服务器向企业总部的服务器发起一个 TCP 请求时，该 TCP 请求被转发到企业分支的 CPE 上，企业分支的 CPE 通过 iptables 转发实现将请求数据转发到与该 TCP 请求对应的端口上，实现了透明代理。

本文实施例中，CPE 包含有 iptables、代理模块和转发模块。企业分支的服务器发出的全部请求都会先经过 CPE 的 iptables，由 iptables 过滤区分为 TCP 请求及非 TCP 请求，之后将区分出的 TCP 请求经由代理模块后，通过转发模块发送给企业总部。

其中，企业分支的 CPE 获取到请求数据、作为目标的总部服务器的 IP 及端

口、作为请求来源的分支服务器的 IP 及端口。将这些信息通过私有协议封装，转发到 SD-WAN 网络。

SD-WAN 通过可靠传输方式（包括 TCP、可靠 UDP 等）将收到的数据快速传输到企业总部的 CPE 设备上。

企业总部的 CPE 解析私有协议，获取到请求数据、请求目标 IP 及端口、请求来源 IP 及端口，对目标 IP 及端口发起连接，通过系统所支持的 TCP 参数来实现源目标地址伪装。例如，可以使用 socket 的 ip_transparent 选项，设置请求来源 IP 及端口为连接源 IP 地址和端口。这样企业总部的目标服务器看到的客户端 IP 及端口就是企业分支的服务器的地址。对于非 TCP 请求，一般不做特别处理。

后续请求及响应数据都可以在上述传输数据所使用的连接链里传输，实现 TCP 请求传输加速。

从上述描述可以看出，与相关技术中的多份发送方案，带宽浪费较大，无法根本解决网络抖动丢包问题相比，本文实施例提供的技术方案实现了对客户无感知，可以优先解决 TCP 连接传输加速的问题，可以解决网络抖动导致丢包的问题。

对于总部内网到分支内网的请求和响应的连接链建立过程，其实现原理与上述原理相同，只是传输数据的方向与图 5 所示的场景相反，本文实施例对此不再赘述。

本文的一实施例提供了一种配置方法，用于配置接收端的服务器与发起端的服务器之间的 SD-WAN 连接链，其中，

接收端的 CPE 接收由发起端的 CPE 发出的使用私有协议封装后的 TCP 请求的信息，并使用所述私有化协议对所述 TCP 请求的信息进行解析；

所述接收端的 CPE 对接收端的服务器的 IP 及端口发起连接，配置为目标端；

所述接收端的 CPE 将发起端的服务器的 IP 及端口配置为源端；

所述接收端的 CPE 在所述目标端与所述源端之间建立连接链。

其中，TCP 请求的信息至少包含如下信息：

请求数据、作为请求目标的接收端的服务器的 IP 及端口、作为请求来源的发起端的服务器的 IP 及端口。

实际应用中，本实施例提供的配置方法的操作可参见图 4 所示的虚拟内网加速方法中步骤 202 的执行过程，在此不再赘述。

本文的一实施例还提供了一种虚拟内网加速系统，其结构如图 6 所示，至少包括 SD-WAN 连接的发起端的服务器、接收端的服务器、发起端的客户端设备 CPE 和接收端的 CPE。

其中，发起端的 CPE，用于在接收到发起端的服务器向接收端的服务器发送的 TCP 请求时，将该 TCP 请求的信息传输至接收端的 CPE；

接收端的 CPE，用于根据接收到的 TCP 请求的信息，配置发起端的服务器与接收端的服务器之间的连接链；

发起端的服务器与接收端的服务器，用于通过上述连接链，传输 TCP 请求和/或 TCP 响应数据。

其中，发起端的 CPE，可以用于检测 TCP 请求，将分支服务器发送的 TCP 请求的信息使用私有协议封装后，发送给接收端的 CPE。

本文中，TCP 请求的信息至少包含如下信息：

请求数据、作为目标的接收端的服务器的 IP 及端口、作为请求来源的发起端的服务器的 IP 及端口。

其中，连接链承载于发起端的 CPE 与接收端的 CPE 之间的 SD-WAN 可靠传输通道上。

其中，接收端的 CPE，可以用于在接收到 TCP 请求的信息后，使用私有协议解析，对接收端的服务器的 IP 及端口发起连接，配置目标端，将发起端的服务器的 IP 及端口配置为源端，在目标端及源端之间建立连接链。

本文实施例还提供了一种计算机存储介质，其上存储有计算机程序，所述程序被处理器执行时实现本文的实施例提供的一种虚拟内网通信方法的步骤。

本文实施例还提供了一种计算机设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述程序时实现本文的实施例提供的一种虚拟内网通信方法的步骤。

本文的实施例提供了一种虚拟内网加速方法及系统、配置方法、存储介质和计算机设备，发起端的 CPE 在接收到发起端的服务器向接收端的服务器发送的 TCP 请求时，将 TCP 请求的信息传输至接收端的 CPE。接收端的 CPE 根据接收到的 TCP 请求的信息，配置发起端的服务器与接收端的服务器之间的连接链，然后通过该连接链，传输 TCP 请求和/或 TCP 响应数据。其中，在 SD-WAN 的发起端的服务器和接收端的服务器之间建立连接链，通过所述连接链，传输 TCP 请求和/或 TCP 响应数据时还可以将该连接链承载于可靠传输通道上。从而实现发起端与接收端之间的 TCP 连接透明加速，对 TCP 连接传输进行了加速，有效的避免了丢包的发生，解决了现有预防丢包处理方式资源消耗量大且效果欠佳的问题。

在基于 WAN 的虚拟内网加速 TCP 连接，加速方式对客户无感知，有效的解决了虚拟 WAN 网络丢包带来应用层感知丢包的问题。

图7是根据一示例性实施例示出的一种用于虚拟内网加速的计算机设备700的框图。例如，计算机设备700可以被提供为一服务器。参照图7，计算机设备700包括处理器701，处理器的个数可以根据需要设置为一个或者多个。计算机设备700还包括存储器702，用于存储可由处理器701的执行的指令，例如应用程序。存储器的个数可以根据需要设置一个或者多个。其存储的应用程序可以作为一个或者多个。处理器701被配置为执行指令，以执行上述虚拟内网加速方法，包括：

发起端的客户端设备 CPE 在接收到发起端的服务器向接收端的服务器发送的 TCP 请求时，将所述 TCP 请求的信息传输至接收端的 CPE；

所述接收端的 CPE 根据所述 TCP 请求的信息，配置所述发起端的服务器与所述接收端的服务器之间的连接链；

通过所述连接链，传输 TCP 请求和/或 TCP 响应数据。

本领域技术人员应明白，本文的实施例可提供为方法、装置（设备）、或计算机程序产品。因此，本文可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本文可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质上实施的计算机程序产品的形式。计算机存储介质包括在用于存储信息（诸如计算机可读指令、数据结构、程序模块或其他数据）的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质，包括但不限于 RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘（DVD）或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质等。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

本文是参照根据本文实施例的方法、装置（设备）和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的物品或者设备不仅包括那些要素，而且

还包括没有明确列出的其他要素，或者是还包括为这种物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的物品或者设备中还存在另外的相同要素。

尽管已描述了本文的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本文范围的所有变更和修改。

显然，本领域的技术人员可以对本文进行各种改动和变型而不脱离本文的精神和范围。这样，倘若本文的这些修改和变型属于本文权利要求及其等同技术的范围之内，则本文的意图也包含这些改动和变型在内。

工业实用性

本文中技术方案，在发起端的 CPE 接收到发起端的服务器向接收端的服务器发送的 TCP 请求时，将该 TCP 请求的信息传输至接收端的 CPE。接收端的 CPE 根据收到的 TCP 请求的信息，配置发起端的服务器与接收端的服务器之间的连接链，然后通过该连接链，传输 TCP 请求和/或 TCP 响应数据。在 SD-WAN 的发起端的服务器和接收端的服务器之间建立连接链，通过该连接链，传输 TCP 请求和/或 TCP 响应数据。还可以将该连接链承载于可靠传输通道上。实现了发起端与接收端之间的 TCP 连接透明加速，对 TCP 连接传输进行了加速，有效的避免了丢包的发生，解决了现有预防丢包处理方式资源消耗量大且效果欠佳的问题。在基于 WAN 的虚拟内网加速 TCP 连接，加速方式对客户无感知，有效的解决了虚拟 WAN 网络丢包带来应用层感知丢包的问题。

权利要求

1、一种虚拟内网加速方法，包括：

发起端的客户端设备 CPE 在接收到发起端的服务器向接收端的服务器发送的 TCP 请求时，将所述 TCP 请求的信息传输至接收端的 CPE；

所述接收端的 CPE 根据所述 TCP 请求的信息，配置所述发起端的服务器与所述接收端的服务器之间的连接链；

通过所述连接链，传输 TCP 请求和/或 TCP 响应数据。

2、根据权利要求 1 所述的虚拟内网加速方法，其中，所述发起端的 CPE 在接收到发起端的服务器向接收端的服务器发送的 TCP 请求时，将所述 TCP 请求的信息传输至接收端的 CPE 的步骤包括：

所述发起端的 CPE 检测到 TCP 请求；

所述发起端的 CPE 将分支服务器发送的 TCP 请求的信息使用私有协议封装后，通过与所述 TCP 请求对应的端口向所述接收端的 CPE 发送，所述 TCP 请求的信息至少包含如下信息：

请求数据、作为目标的接收端的服务器的 IP 及端口、作为请求来源的发起端的服务器的 IP 及端口。

3、根据权利要求 2 所述的虚拟内网加速方法，其中，所述发起端的 CPE 通过 SD-WAN 的可靠传输方式将所述 TCP 请求的信息传输至所述接收端的 CPE。

4、根据权利要求 2 所述的虚拟内网加速方法，其中，所述接收端的 CPE 根据所述 TCP 请求的信息，配置所述连接链的步骤包括：

所述接收端的 CPE 在接收到所述 TCP 请求的信息后，使用所述私有协议解析；

对所述接收端的服务器的 IP 及端口发起连接，配置目标端；

将所述发起端的服务器的 IP 及端口配置为源端；

在所述目标端及所述源端之间建立连接链。

5、根据权利要求1所述的虚拟内网加速方法，其中，

所述发起端的服务器为分支服务器，所述接收端的服务器为总部服务器；

或，

所述发起端的服务器为总部服务器，所述接收端的服务器为分支服务器。

6、一种配置方法，用于配置接收端的服务器与发起端的服务器之间的SD-WAN连接链，其中，

接收端的客户端设备CPE接收由发起端的CPE发出的使用私有协议封装后的TCP请求的信息，并使用所述私有化协议对所述TCP请求的信息进行解析；

所述接收端的CPE对接收端的服务器的IP及端口发起连接，配置为目标端；

所述接收端的CPE将发起端的服务器的IP及端口配置为源端；

所述接收端的CPE在所述目标端与所述源端之间建立连接链。

7、一种虚拟内网加速系统，至少包括软件定义广域网SD-WAN连接的发起端的服务器、接收端的服务器、发起端的客户端设备CPE和接收端的CPE；

所述发起端的CPE，用于在接收到所述发起端的服务器向所述接收端的服务器发送的TCP请求时，将所述TCP请求的信息传输至所述接收端的CPE；

所述接收端的CPE，用于根据所述TCP请求的信息，配置所述发起端的服务器与所述接收端的服务器之间的连接链；

所述发起端的服务器与所述接收端的服务器，用于通过所述连接链，传输TCP请求和/或TCP响应数据。

8、根据权利要求7所述的虚拟内网加速系统，其中，

所述发起端的CPE，用于检测TCP请求；

将分支服务器发送的TCP请求的信息使用私有协议封装后，通过与所述TCP请求对应的端口向所述接收端的CPE发送，所述TCP请求的信息至少包含如下信息：

请求数据、作为目标的接收端的服务器的 IP 及端口、作为请求来源的发起端的服务器的 IP 及端口。

9、根据权利要求 8 所述的虚拟内网加速系统，其中，所述连接链承载于所述发起端的 CPE 与所述接收端的 CPE 之间的 SD-WAN 可靠传输通道上。

10、根据权利要求 7 所述的虚拟内网加速系统，其中，

所述接收端的 CPE，用于在接收到所述 TCP 请求的信息后，使用所述私有协议解析，对所述接收端的服务器的 IP 及端口发起连接，配置目标端，将所述发起端的服务器的 IP 及端口配置为源端，在所述目标端及源端之间建立连接链。

11、一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被执行时实现如权利要求 1—5 中任意一项所述方法的步骤，或者所述计算机程序被执行时实现如权利要求 6 所述方法的步骤。

12、一种计算机设备，包括处理器、存储器和存储于所述存储器上的计算机程序，所述处理器执行所述计算机程序时实现如权利要求 1—5 中任意一项所述方法的步骤，或者所述处理器执行所述计算机程序时实现如权利要求 6 所述方法的步骤。