(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 101026531 B
(45)授权公告日 2010.12.08

(21)申请号 200610168771.7

(22)申请日 2006.12.18

(30)优先权数据
2006-047316 2006.02.23 JP

(73)专利权人 株式会社日立制作所
地址 日本东京都

(72)发明人 小川佑纪雄 小桧山智久
安江利一

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静

(51)Int.Cl.
H04L 12/46(2006.01)
H04L 29/06(2006.01)
H04L 12/66(2006.01)
G06F 15/177(2006.01)

(56)对比文件
CN 1629846 A,2005.06.22, 全文.
CN 1703047 A,2005.11.30, 说明书第3-4页,第5页第5-13行、图1.
US 6678835 B1,2004.01.13, 全文.

审查员 阎洁

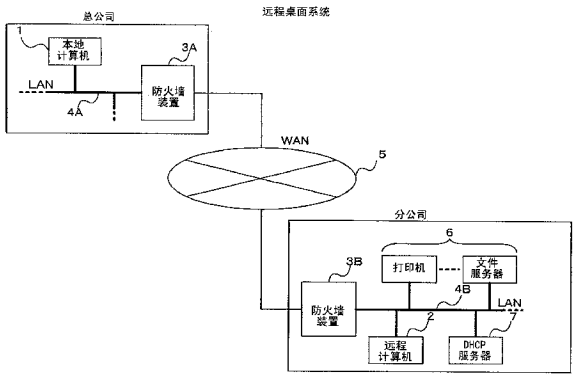
权利要求书 2 页 说明书 10 页 附图 10 页

(54)发明名称

信息处理系统

(57)摘要

本发明提供一种信息处理系统。即使不针对和网络设备的通信中所使用的每个协议进行防火墙装置的设定,信息处理装置也可以越过防火墙、使用网络设备。通过VPN连接本地计算机(1)和远程计算机(2),使远程计算机(2)具有VPN网关功能,从而使本地计算机(1)属于远程计算机(2)侧的网络。由此,在本地计算机(1)和远程计算机(2)之间存在防火墙装置(3A、3B)的情况下,为使本地计算机(1)和远程计算机(2)可以通过VPN相连,而仅对防火墙装置(3A、3B)进行设定,本地计算机(1)就可以通过各种协议,和连接在远程计算机(2)侧的LAN(4B)上的各种网络设备(6)进行通信。



CN 101026531 B

1. 一种信息处理系统，具有第 1 信息处理装置和第 2 信息处理装置，其特征在于，

所述第 1 信息处理装置，具有与 VPN 相连的 VPN 接口部、以及从所述第 2 信息处理装置接收所述 VPN 的连接请求的 VPN 连接请求接收部，

所述第 2 信息处理装置，是作为所述第 1 信息处理装置的输入输出装置而工作的操作终端，具有与所述 VPN 以及不同于所述 VPN 的网络相连的 VPN 网关部、以及向所述第 1 信息处理装置发送所述 VPN 的连接请求的 VPN 连接请求发送部，

所述 VPN 网关部，当通过所述 VPN 或所述网络接收到的数据包的目的地是分配给所述第 1 信息处理装置的所述网络的地址时，将该数据包转发至所述 VPN，当所述目的地是分配给所述第 1 信息处理装置的所述网络的地址以外的地址时，将该数据包转发至所述网络，

所述 VPN 接口部，在所述 VPN 连接请求接收部接收到所述 VPN 的连接请求时，通过所述 VPN，与所述 VPN 网关部相连。

2. 根据权利要求 1 所述的信息处理系统，其特征在于，

所述 VPN 接口部，在满足规定条件的情况下，通过所述 VPN，与所述 VPN 网关部相连。

3. 根据权利要求 2 所述的信息处理系统，其特征在于，

所述规定条件是 ：与所述 VPN 网关部的连接时刻属于规定的时间段。

4. 根据权利要求 2 所述的信息处理系统，其特征在于，

所述规定条件是 ：所述第 2 信息处理装置属于规定的网络。

5. 根据权利要求 2 所述的信息处理系统，其特征在于，

所述规定条件是 ：所述第 2 信息处理装置的用户是规定的用户。

6. 根据权利要求 1 所述的信息处理系统，其特征在于，

所述第 1 信息处理装置还具有 ：对所述 VPN 接口部和所述 VPN 网关部收发的通信数据包进行控制的通信控制部。

7. 根据权利要求 1 所述的信息处理系统，其特征在于，

所述第 1 信息处理装置还具有 ：对通过所述 VPN 接口收发通信数据的应用程序进行控制的应用程序控制部。

8. 根据权利要求 1 所述的信息处理系统，其特征在于，

所述第 1 信息处理装置，利用所述 VPN 接口部，与连接在所述网络上的网络设备进行通信。

9. 根据权利要求 8 所述的信息处理系统，其特征在于，

所述网络设备是文件服务器。

10. 根据权利要求 8 所述的信息处理系统，其特征在于，

所述网络设备是打印机。

11. 根据权利要求 8 所述的信息处理系统，其特征在于，

所述第 1 信息处理装置还具有 ：记录应用程序和所述网络设备间的通信履历的记录部。

12. 一种虚拟办公室系统，其特征在于，

具有多个权利要求 1 至 11 中任意一项中所记载的信息处理系统，所述各信息处理系统的所述第 2 信息处理装置，连接到一个网络中。

13. 一种通信方法，用于第 1 信息处理装置与在第 2 信息处理装置上网络连接的网络设

备进行通信，其特征在于，

所述第 1 信息处理装置，通过 VPN 与所述第 2 信息处理装置相连，从所述第 2 信息处理装置接收所述 VPN 的连接请求，

所述第 2 信息处理装置，作为所述第 1 信息处理装置的输入输出装置而工作，向所述第 1 信息处理装置发送所述 VPN 的连接请求，

在通过所述 VPN 或所述网络接收到的数据包的目的地是分配给所述第 1 信息处理装置的所述网络的地址时，将所述数据包转发至所述 VPN，在所述目的地是分配给所述第 1 信息处理装置的所述网络的地址以外的地址时，将该数据包转发至所述网络，

所述第 1 信息处理装置，在接收到所述 VPN 的连接请求时，通过所述 VPN，与所述第 2 信息处理装置相连。

信息处理系统

技术领域

[0001] 本发明涉及信息处理系统的网络连接技术，特别涉及，在瘦客户机型信息处理系统中将本地计算机和远程计算机侧的网络设备相连接的技术。

背景技术

[0002] 近年来，所谓的瘦客户机型（thin client type）信息处理系统受到关注。在瘦客户机型信息处理系统中，通过使用身边的远程计算机（remote machine），对位于自己家中或公司中的本地计算机（local machine）的桌面进行远程操作，可以利用在本地计算机上安装的各种应用程序和数据。在本地计算机中，除了台式PC（Desktop Personal Computer）以外，还使用了不具备本地连接的输入输出装置（键盘、鼠标和显示器）的刀片PC（刀片计算机（blade computer））等（例如，参照特开2003-337672号公报）。

发明内容

[0003] 在这种瘦客户机型信息处理系统中，在利用与远程计算机侧的网络相连的网络设备（打印机、扫描仪、文件服务器等）时，为了在本地计算机和网络设备间可以进行通信，需要对本地计算机和网络设备间存在的防火墙装置进行设定。例如，在网络设备为打印机，本地计算机使用LPR（Line PrinterDeamon Protocol）向打印机发送打印命令的情况下，为使LPR的数据包从本地计算机到达打印机，需要设定地址和端口。另外，在网络设备是文件服务器，本地计算机使用FTP（File Transfer Protocol）访问文件服务器的情况下，为使FTP的数据包从本地计算机到达打印机，需要设定地址和端口。

[0004] 这样，目前对于与网络设备的通信中使用的每个协议，必须对存在于本地计算机和网络设备间的防火墙装置进行设定，工作的负担很大。

[0005] 因此，本发明的目的是，即使不针对和网络设备的通信中使用的每个协议进行防火墙装置的设定，信息处理装置也可以越过防火墙，利用网络设备。

[0006] 为了解决上述问题，在本发明中，通过VPN（Virtual Private Network）将第1信息处理装置和第2信息处理装置相连，使第2信息处理装置具有VPN网关功能，由此，使第1信息处理装置属于第2信息处理装置侧的网络。

[0007] 例如，在具有第1信息处理装置和第2信息处理装置的信息处理系统中，所述第1信息处理装置具有与VPN（Virtual Private Network）相连的VPN接口单元，所述第2信息处理装置具有与所述VPN以及不同于所述VPN的网络相连的VPN网关单元，所述VPN网关单元在通过所述VPN或所述网络而接收到的数据包的目的地是分配给规定的网络设备的所述网络的地址时，将该数据包转发至所述VPN，当所述目的地是分配给所述规定网络设备的所述网络的地址以外的地址时，将该数据包转发至所述网络。

[0008] 在此，所述第2信息处理装置可以是作为所述第1信息处理装置的输入输出装置而工作的操作终端。

[0009] 另外，所述第2信息处理装置还具有：向所述第1信息处理装置发送VPN的连接请

求的VPN连接请求发送单元，所述第1信息处理装置还具有：从所述第2信息处理装置接收所述VPN的连接请求的VPN连接请求接收单元，并且，所述VPN接口单元在所述VPN连接请求接收单元接收到所述VPN的连接请求时，也可以通过所述VPN与所述VPN网关单元相连。

[0010] 这样，在第1信息处理装置和第2信息处理装置间存在防火墙装置时，为了可以通过VPN连接第1信息处理装置和第2信息处理装置而仅进行防火墙的设定，第1信息处理装置就可以通过各种协议与属于第2信息处理装置侧的网络的各种网络设备通信。

附图说明

[0011] 图1是表示应用了第1实施方式的远程桌面系统（瘦客户机型的信息处理系统）的概略结构的一例的图。

[0012] 图2是表示本地计算机1的概略结构例的图。

[0013] 图3是用于说明本地计算机1的动作例的图。

[0014] 图4是表示本地计算机2的概略结构例的图。

[0015] 图5是用于说明远程计算机2的动作例的图。

[0016] 图6是表示应用了第1实施方式的远程桌面系统的概略动作例的图。

[0017] 图7是用于说明本地计算机1的动作例的图。

[0018] 图8是用于说明远程计算机2的动作例的图。

[0019] 图9是表示应用了实施方式2的远程桌面系统的概略动作例的图。

[0020] 图10是表示应用了实施方式3的虚拟办公室系统的概略结构例的图。

具体实施方式

[0021] （第1实施方式）

[0022] 图1是表示应用了第1实施方式的远程桌面系统（瘦客户机型信息处理系统）的概略结构的一例的图。

[0023] 如图所示，本实施方式的远程桌面系统具有：本地计算机1、远程计算机2、打印机（打印机服务器）、扫描仪（扫描仪服务器）、文件服务器等网络设备6和DHCP(Dynamic Host Configuration Protocol)服务器7。本地计算机1例如与在总公司中构建的LAN(Local Area Network)4A相连。LAN4A通过防火墙装置3A与WAN(Wide Area Network)5相连。另外，远程计算机2、网络设备6以及DHCP服务器7，例如与在分公司中构建的LAN4B相连。LAN4B通过防火墙装置3B与WAN5相连。

[0024] 本地计算机1向远程计算机2提供终端服务。即，接收并处理从远程计算机2发送来的输入信息（输入装置的操作内容），并且将表示处理结果的图像信息（显示装置的桌面画面）发送至远程计算机2。另外，本地计算机1具有VPN(Virtual Private Network)接口功能，通过VPN和远程计算机2相连。并且，利用远程计算机2的后述VPN网关功能，与远程计算机2侧的网络4B相连。在该本地计算机1中，可以使用台式PC(Personal Computer)以及不具备本地连接的输入输出装置（键盘、鼠标以及显示器）的刀片PC（刀片计算机）等。

[0025] 图2是表示本地计算机1的概略结构例的图。

[0026] 如图所示，本地计算机1具有：CPU(Central Processing Unit)101、作为CPU101

的工作区而工作的 RAM(Random Access Memory)102、用于与 LAN4A 相连的 NIC(Network Interface Card)103、HDD(Hard Disk Drive)104、快速 ROM(Flash Read Only Memory)105、生成桌面图像信息的视频卡 106、对与以上各部 101 ～ 106 相连的总线 BUS 等内部线路进行中继的网桥 107、电源 108。

[0027] 在快速 ROM105 中存储有 BIOS(Basic Input/Output System)1 050。CPU101，在接通电源 108 后，首先访问快速 ROM105，执行 BIOS1050，由此识别本地计算机 1 的系统结构。

[0028] HDD104 中至少存储有 :OS(Operating System)1041、VPN 接口程序 1042、远程服务器程序 1043、VPN 控制程序 1044、通信控制程序 1045、应用程序控制程序 1046、通信日志程序 1047、多个应用程序 1048、用户数据 1049。

[0029] OS1041 是 CPU101 用来总体控制本地计算机的各部 102 ～ 108、执行后述各程序 1042 ～ 1048 的程序。CPU101 遵从 BIOS1050 将 OS1041 从 HDD104 载入 RAM102 并执行。由此，CPU101 总体控制本地计算机 1 的各部 102 ～ 108。

[0030] VPN 接口程序 1042 是用于在与远程计算机 2 之间构建 VPN 的程序，例如是使用了 IPsec(Security Architecture for the Internet Protocol) 的通信程序。CPU101，遵从 OS1041，将 VPN 接口程序 1042 从 HDD104 载入 RAM102 并执行。由此，CPU101 通过 VPN 与远程计算机 2 相连。

[0031] 远程服务器程序 1043 是用于提供终端服务、即可以从远程计算机 2 对本地计算机 1 的桌面进行远程操作的程序，例如是 AT&T 剑桥研究所开发的 VNC(Virtual Network Computing) 的服务器程序。CPU101 遵从 OS1041，将远程服务器程序 1043 从 HDD104 载入 RAM102 并执行。由此，CPU101 接收并处理从远程计算机 2 送来的输入信息（键盘和鼠标的操作内容），并且将表示处理结果的图像信息（显示器的桌面画面）发送至远程计算机 2。

[0032] VPN 控制程序 1044 是用于控制基于 VPN 接口程序 1042 的 VPN 连接的程序。CPU101 遵从 OS1041，将 VPN 控制程序 1044 从 HDD104 载入 RAM102 并执行。由此，CPU101 根据通过 NIC103 从远程计算机 2 接受的 VPN 连接请求，在规定的条件下使 VPN 接口程序 1042 构建与远程计算机 2 之间的 VPN。在此，规定的条件是 :当前时刻属于规定的时间段，和 / 或，远程计算机 2 的网络地址是规定的地址，和 / 或，远程计算机 2 的用户是被许可进行 VPN 通信的用户。

[0033] 通信控制程序 1045 是用于对通过 VPN 收发的通信数据包进行控制的程序，例如是进行数据包过滤 (packet filtering) 的防火墙程序。CPU101 遵从 OS1041，将通信控制程序 1045 从 HDD104 载入 RAM102 并执行。由此，CPU101 进行过滤，以使通过 VPN 对使用规定的目的地地址、发送源或通信协议的数据包进行收发。

[0034] 应用程序控制程序 1046 是用于控制通过 VPN 与通信对象进行通信的应用程序 1048 的程序，例如是对被许可通过 VPN 进行数据收发的应用程序的启动进行许可的程序。CPU101 遵从 OS1041，将应用程序控制程序 1046 从 HDD104 载入 RAM102 并执行。由此，CPU101 进行控制，以使规定的应用程序 1048 可以使用 VPN。

[0035] 通信日志程序 1047 是用于记录利用 VPN 进行通信的应用程序 1048 的、与通信对象间的通信履历的程序。CPU101 遵从 OS1041，将通信日志程序 1047 从 HDD104 载入 RAM102 并执行。由此，CPU101 将使用 VPN 进行通信的应用程序 1048 的、与通信对象间的通信履历，记录在用户数据 1049 中。

[0036] 在应用程序 1048 中包括 :通用的 Web 浏览器、文字处理机、CAD、以及表计算等程序。CPU101 遵从 OS1041,对通过远程服务器程序 1043 从远程计算机 2 接受的指示进行应答,将希望的应用程序 1048 从 HDD104 载入 RAM102 并执行。然后,使视频卡 107 生成反映其执行结果的桌面画面的图像信息,通过远程服务器程序 1043 发送至远程计算机 2。

[0037] 用户数据 1049 是可以在应用程序 1048 中使用的数据,是用户个人使用的数据(例如,个人作成的文件数据、通信日志程序 1047 所生成的履历数据等)。

[0038] 图 3 是用于说明本地计算机 1 的动作例的图。

[0039] 本来,CPU101 根据程序执行该流程。但在此为了便于说明,将程序作为执行主体来说明流程。

[0040] OS1041,当通过 NIC103 从远程计算机 2 接收到终端服务请求时 (S101 :YES),将终端服务请求应答发送至远程计算机 2。然后,启动远程服务器程序 1043,开始对远程计算机 2 提供终端服务 (S102)。具体而言,当通过 NIC103 从远程计算机 2 接收到输入信息时,将该输入信息向在用的规定应用程序 1048 通知。接收该输入信息,应用程序 1048 执行对应于表示该输入信息的操作内容(键盘操作和鼠标操作)的处理。然后,在 RAM102 中,生成表示反映处理结果的桌面画面的图像信息(用于描绘桌面画面的颜色信息、描绘命令信息、位图信息等)。远程服务器程序 1043 通过 NIC103 将该图像信息发送至远程计算机 2。

[0041] 接下来,OS1041,当通过 NIC103 使用终端服务从远程计算机 2 接收到 VPN 连接请求时 (S103 :YES),将其向 VPN 控制程序 1044 通知。接收该 VPN 连接请求,VPN 控制程序 1044 判断是否满足规定的条件 (S104)。在本实施方式中,以如下条件为规定条件并判断是否满足这些条件 :通过未图示的内置计时器等取得到的当前时刻属于预定的时间段(例如,平日的上班时间段),以及,VPN 连接请求的发送源地址属于规定的网络(例如,规定的分公司中构建的 LAN),以及,远程计算机 2 的用户是被许可进行 VPN 通信的用户。

[0042] 在 S104 中不满足规定的条件的情况下 (S104 :NO),VPN 控制程序 1044 进行规定的错误 (error) 处理,如通过 OS1041 和 NIC103 向 VPN 连接请求的发送源发送错误消息等 (S110)。

[0043] 另一方面,在 S104 中满足了规定的条件的情况下 (S104 :YES),VPN 控制程序 1044,通过 OS1041 和 NIC103 向 VPN 连接请求的发送源发送 VPN 连接应答。然后,启动 VPN 接口程序 1042,在与作为 VPN 连接请求源的远程计算机 2 之间,使 VPN 接口程序 1042 确立 VPN(S105)。

[0044] 当与远程计算机 2 之间确立了 VPN 时,OS1041 利用后述的远程计算机 2 的网关功能,访问与远程计算机 2 侧的 LAN4B 相连的 DHCP 服务器 7,从 DHCP 服务器 7 取得网络地址(本地地址)(S106)。由此,本地计算机 1 可以与连接在 LAN4B 上的网络设备 6 进行通信。

[0045] 此后,OS1041 启动通信控制程序 1045,开始对通过 VPN 收发的通信数据包进行数据包过滤 (S107)。进行数据包过滤,例如全部拒绝来自网络设备 6 的访问,许可从本地计算机对网络设备 6 进行访问。

[0046] 另外,OS1041 启动应用程序控制程序 1046,开始应用程序控制服务 (S108)。由此进行控制,以便拒绝规定的应用程序 1048 以外的程序利用 VPN(VPN 接口程序 1042),使规定的应用程序 1048 可以利用 VPN 与通信对象进行通信。

[0047] 另外,OS1041 启动通信程序 1047。由此,通信日志程序 1047,将使用 VPN 的各个

应用程序 1048 的通信履历记录在用户数据 1049 中 (S109)。

[0048] 返回图 1 继续说明。

[0049] 远程计算机 2 从本地计算机 1 接受终端服务。即，将由用户输入的输入信息（输入装置的操作内容）发送至本地计算机 1，并且，从该本地计算机 1 接收图像信息（用于描绘显示装置的桌面画面的颜色信息、描绘命令信息、位图信息等），并在显示装置上显示。另外，远程计算机 2 具备 VPN 网关功能，通过 VPN 与本地计算机 1 相连。并且，将本地计算机 1 与远程计算机 2 侧的网络 4B 相连。此外，远程计算机 2 是所谓的无 HDD 型 PC，无法直接（不通过本地计算机 1）访问本地连接的外围设备和网络设备。即，远程计算机 2，仅可以使用与本地计算机 1 本地连接或网络连接的设备。这样，降低了由于远程计算机 2 的失窃等导致信息泄漏的可能性。

[0050] 图 4 是表示远程计算机 2 的概略构成例的图。

[0051] 如图所示，远程计算机 2 具有 :CPU201、作为 CPU201 的工作区而工作的 RAM202、用于与 LAN4B 相连的 NIC203、用于连接键盘和鼠标的 I/O 连接器 204、快速 ROM205、用于连接显示器的视频卡 206、对连接以上各部 201 ～ 206 的总线 BUS 等内部线路进行中继的网桥 207、电源 208。

[0052] 在快速 ROM205 中至少存储有 :BIOS2050、OS2051、VPN 网关程序 2052、远程客户机程序 2053、VPN 控制程序 2054、以及通信控制程序 2055。

[0053] CPU201 在接通电源 208 后首先访问快速 ROM205、执行 BIOS2050，由此识别远程计算机 2 的系统结构。

[0054] OS2051 是用于 CPU201 总体控制远程计算机 2 的各部 202 ～ 208、执行后述的各程序 2052 ～ 2055 的程序。CPU201 遵从 BIOS2050，将 OS205 1 从快速 ROM205 载入 RAM202 并执行。由此，CPU201 总体控制远程计算机 2 的各部 202 ～ 208。此外，在本实施方式的 OS2051 中，使用内部 OS 等可以存储在快速 ROM205 中的较小的 OS。

[0055] VPN 网关程序 2052 是用于在与本地计算机 1 之间构建 VPN 的程序，例如是使用了 IPsec 或 HTTPS 的通信程序。CPU101 遵从 OS1041 将 VPN 网关程序 2052 从快速 ROM 205 载入 RAM202 并执行。由此，CPU201 在与本地计算机 1 之间构建 VPN，将该 VPN 和 LAN4B 相连。

[0056] 远程客户机程序 2053 是用于接受终端服务、即用于远程计算机 2 远程访问本地计算机 1 的桌面的程序，例如是 VNC 的客户机（查看器 (viewer)）程序。CPU201 遵从 OS2051 将远程客户机程序 2053 从快速 ROM205 载入 RAM202 并执行。由此，CPU201 将 I/O 连接器 206 的输入信息（键盘和鼠标的操作内容）向本地计算机 1 发送，并且，接收从本地计算机 1 发送来的图像信息（用于描绘显示器的桌面画面的颜色信息、描绘命令信息、位图信息等），对其进行处理，在与视频卡 206 相连的显示装置（未图示）上显示。

[0057] VPN 控制程序 2054 是用于对基于 VPN 网关程序 2052 的 VPN 连接进行控制的程序。CPU201 遵从 OS2051 将 VPN 控制程序 2054 从快速 ROM205 载入 RAM202 并执行。由此，CPU201 根据经由 IO 连接器 204 从输入装置接受的 VPN 的连接指示，通过 NIC203 向本地计算机 1 发送 VPN 的连接请求。另外，根据经由 NIC203 从本地计算机接受的 VPN 的连接应答，在规定条件下，使 VPN 网关程序 2052 构建与本地计算机 1 之间的 VPN。在此，规定的条件是指 : 当前时刻属于规定的时间段，和 / 或，本地计算机 1 的网络地址是规定的地址，和 / 或，远程计算机 2 的用户是被许可进行 VPN 通信的用户。

[0058] 通信控制程序 2055 是用于对通过 VPN 收发的通信数据包进行控制的程序，例如是进行数据包过滤的防火墙程序。CPU201 遵从 OS2051 将通信控制程序 2055 从快速 ROM205 载入 RAM202 并执行。由此，CPU201 进行过滤，以便让使用了规定的目的地地址、发送源或通信协议的数据包可以在 VPN 和 LAN4B 之间往来。

[0059] 图 5 是用于说明远程计算机 2 的动作例的图。

[0060] 本来，CPU201 根据程序执行该流程。但在此为了便于说明，以程序为执行主体来说明流程。

[0061] 首先，OS2051 启动远程客户机程序 2053。启动后，远程客户机程序 2053 通过 NIC203 向本地计算机 1 发送终端服务请求 (S201)。然后，若从本地计算机 1 接收到终端服务请求应答，则开始利用由本地计算机 1 提供的终端服务 (S202)。具体而言，通过 IO 连接器 204 从输入装置接收输入信息时，通过 NIC203 向本地计算机 1 发送该输入信息。另外，通过 NIC203 从本地计算机 1 接收用于描绘本地计算机 1 桌面画面的图像信息，对其进行处理，并在与视频卡 206 相连的显示装置上显示。

[0062] 接下来，OS2051，当通过 IO 连接器 204 从输入装置接受 VPN 连接指示时 (S203 ：YES)，使用终端服务，通过 NIC203 向本地计算机 1 发送 VPN 连接请求 (S204)。然后，OS2051，当通过 NIC203 从本地计算机 1 接收 VPN 连接应答时 (S205 ：YES)，将其向 VPN 控制程序 2054 通知。接受该 VPN 连接应答，VPN 控制程序 2054 判断是否满足规定的条件 (S206)。在本实施方式中，以如下条件为规定条件并判断是否满足这些条件 ：通过未图示的内置计时器等取得的当前时刻属于预定的时间段 (例如，平日的上班时间段)，以及，VPN 连接应答的发送源地址属于规定的网络 (例如，构建在总公司中的 LAN)，以及，远程计算机 2 的用户是被许可进行 VPN 通信的用户。

[0063] 在 S206 中不满足规定条件的情况下 (S206 ：NO)，VPN 控制程序 2054 进行规定的错误处理，如通过 OS2051 和 NIC203，向 VPN 连接应答的发送源发送错误消息等 (S210)。

[0064] 另一方面，在 S206 中满足规定条件的情况下 (S206 ：YES)，VPN 控制程序 2054 启动 VPN 网关程序 2052。启动后，VPN 网关程序 2052 在与作为 VPN 连接应答源的本地计算机 1 之间确立 VPN(S207)。

[0065] 另外，VPN 网关程序 2052，将该确立的 VPN 和 LAN4B 相连，开始 VPN 网关服务 (S208)。

[0066] 具体而言，通过 NIC203 从 LAN4B 接收通信数据包，在该通信数据包是发往本远程计算机 2 的 VPN 数据包时，取出该 VPN 数据包中所存储的通信数据包，发送至网络 4B。另外，在该通信数据包是 VPN 数据包以外的、发往本远程计算机 2 的数据包时，将该通信数据包向 OS2051，或通过 OS2051 向远程客户机程序 2053 转移。另外，在该通信数据包是发往由 DHCP 服务器 7 分配给本地计算机 1 的数据包时，将该通信数据包存储在 VPN 数据包中，发送至本地计算机 1。由此，本地计算机 1 可以使用网络设备 6。

[0067] 当在与本地计算机 1 之间确立 VPN 时，OS2051 启动通信控制程序 2055，开始对通过 VPN 收发的通信数据包进行数据包过滤 (S209)。进行数据包过滤，例如全部拒绝从网络设备 6 对本地计算机 1 的访问，许可从本地计算机 1 对网络设备 6 访问。

[0068] 图 6 是表示应用了第 1 实施方式的远程桌面系统的概略动作例的图。

[0069] 首先，远程计算机 2 向本地计算机 1 发送终端访问请求 (S31)。本地计算机 1，当从

远程计算机 2 接收到终端访问请求时，返回终端服务应答 (S41)，开始提供终端服务 (S42)。

[0070] 接着，远程计算机 2，当通过输入装置从用户接受 VPN 的连接指示时 (S32)，利用终端服务，将其操作内容 (VPN 连接请求）向本地计算机 1 发送 (S33)。本地计算机 1，当从远程计算机 2 接收 VPN 连接请求时，通过调查是否满足规定的条件，来判断可否连接 (S43)。并且，若可以连接，则返回 VPN 连接应答 (S44)，在与远程计算机 2 之间确立 VPN(S45)。

[0071] 本地计算机 1，若在与远程计算机 2 之间确立了 VPN，则利用远程计算机 2 的 VPN 网关功能，访问 DHCP 服务器 7，从 DHCP 服务器 7 取得在 LAN4B 中的地址 (S46)。另外，开始数据包过滤服务和应用程序控制服务。另一方面，远程计算机 2 开始数据包过滤服务。

[0072] 远程计算机 2，当通过输入装置从用户接受打印指示时，利用终端服务，将其操作内容（打印指示）向本地计算机 1 发送 (S34)。本地计算机 1，当从远程计算机 2 接收打印指示时，生成打印命令，利用远程计算机 2 的 VPN 网关功能，将其发送至打印机 6A(S47)。打印机 6A，根据经由远程计算机 2 从本地计算机 1 接收到的打印命令，打印希望的文件 (S51)。

[0073] 另外，远程计算机 2，当通过输入装置从用户接受下载指示时，利用终端服务，将其操作内容（下载指示）向本地计算机 1 发送 (S35)。本地计算机 1，当从远程计算机 2 接收下载指示时，利用远程计算机 2 的 VPN 网关功能，访问文件服务器 6B，从文件服务器 6B 下载希望的文件 (S48)。

[0074] 以上，对第 1 实施方式进行了说明。

[0075] 在本实施方式中，通过 VPN 将本地计算机 1 和远程计算机 2 相连，使远程计算机 2 具有 VPN 网关功能，由此，使本地计算机 1 属于远程计算机 2 侧的网络。因此，在本地计算机 1 和远程计算机 2 之间存在防火墙装置 3A、3B 的情况下，为使本地计算机 1 和远程计算机 2 可以通过 VPN 相接而仅对防火墙装置 3A、3B 进行设定，本地计算机 1 就可以通过 LPR、FTP 等各种协议与属于远程计算机 2 侧的网络 4B 的打印机、文件服务器等各种网络设备 6 进行通信。即，不需要针对每个协议，对防火墙装置 3A、3B 进行设定。

[0076] 另外，用户可以如同使用与本地计算机 1 本地连接或网络连接的各种设备那样、在外出目的地中使用连接有远程计算机 2 的 LAN4B 上连接的各种网络设备 6。

[0077] （第 2 实施方式）

[0078] 在上述的第 1 实施方式中，以在终端服务中不利用 VPN 的情况为例进行了说明。在本实施方式中，以在终端服务中利用终端服务的情况为例进行说明。此外，本实施方式的远程桌面系统的概略结构，以及构成远程桌面的各设备的概略结构，和上述的第 1 实施方式中所示的结构相同。

[0079] 图 7 是用于说明本地计算机 1 的动作例的图。

[0080] OS1041，当通过 NIC103 从远程计算机 2 接收 VPN 连接请求时 (S121 :YES)，将其向 VPN 控制程序 1044 通知。接受该 VPN 连接请求，VPN 控制程序 1044，和第 1 实施方式的情况相同地，判断是否满足规定的条件 (S122)。

[0081] 在 S122 中不满足规定的条件的情况下 (S122 :NO)，VPN 控制程序 1044 进行规定的错误处理，如通过 OS1041 和 NIC103，向 VPN 连接请求的发送源发送错误消息等 (S130)。

[0082] 另一方面，在 S122 中满足规定的条件的情况下 (S122 :YES)，VPN 控制程序 1044，通过 OS1041 和 NIC103，向 VPN 连接请求的发送源发送 VPN 连接请求应答。然后，启动 VPN 接口程序 1042，在和作为 VPN 连接请求源的远程计算机 2 之间，使 VPN 接口程序 1042 确立

VPN(S123)。

[0083] 在与远程计算机 2 之间确立 VPN 时，OS1041 利用远程计算机 2 的网关功能，访问与远程计算机 2 侧的 LAN4B 相连的 DHCP 服务器 7，从 DHCP 服务器 7 取得网络地址（本地地址）(S124)。由此，本地计算机 1 可以和连接在 LAN4B 上的网络设备 6 通信。

[0084] 然后，OS1041 启动通信控制程序 1045，和第 1 实施方式的情况相同地，开始对通过 VPN 收发的通信数据包进行数据包过滤 (S125)。另外，OS1041 启动应用程序控制程序 1046，和第 1 实施方式的情况相同地，开始应用程序控制服务 (S126)。另外，OS1041 启动通信日志程序 1047，开始记录利用 VPN 的各个应用程序 1048 的通信履历 (S127)。

[0085] 然后，OS1041，当通过 VPN 从远程计算机 2 接收终端服务请求时 (S128 :YES)，通过 VPN 向远程计算机 2 发送终端服务请求应答。然后，启动远程服务器程序 1043，经由 VPN，开始提供对远程计算机 2 的终端服务 (S129)。

[0086] 图 8 是用于说明远程计算机 2 的动作例的图。

[0087] 首先，OS2051 利用终端服务，通过 NIC203 向本地计算机 1 发送 VPN 连接请求 (S211)。然后，OS2051，当通过 NIC203 从本地计算机 1 接收到 VPN 连接应答时 (S222 :YES)，将其向 VPN 控制程序 2054 通知。接受该 VPN 连接应答，VPN 控制程序 2054，和上述的第 1 实施方式相同地，判断是否满足规定的条件 (S223)。

[0088] 在 S223 中不满足规定的条件的情况下 (S223 :NO)，VPN 控制程序 2054 进行规定的错误处理，如通过 OS2051 和 NIC203，向 VPN 连接应答的发送源发送错误消息等 (S229)。

[0089] 另一方面，在 S223 中满足规定的条件的情况下 (S223 :YES)，VPN 控制程序 2054 启动 VPN 网关程序 2052。VPN 网关程序 2052，在与作为 VPN 连接应答源的本地计算机 1 之间确立 VPN(S224)。另外，VPN 网关程序 2052，将该确立的 VPN 与 LAN4B 相连，开始 VPN 网关服务 (S225)。

[0090] 具体而言，通过 NIC203 从 LAN4B 接收通信数据包，在该通信数据包是发往本远程计算机 2 的 VPN 数据包的情况下，取出该 VPN 数据包中存储的通信数据包，确认其发送目的地。若其发送目的地是本远程计算机 2 的地址，则将该存储的数据包向 OS2051，或通过 OS2051 向远程客户机程序 2053 转移。另一方面，若其发送目的地不是本远程计算机 2 的地址，则将其发送至网络 4B。另外，在通过 NIC203 从 LAN4B 接收到的通信数据包是 VPN 数据包以外的、发往本远程计算机 2 的数据包的情况下，将该通信数据包向 OS2051，或通过 OS2051 向远程客户机程序 2053 转移。另外，当通过 NIC203 从 LAN4B 接收到的通信数据包是发往由 DHCP 服务器 7 分配给本地计算机 1 的地址的数据包的情况下，将该通信数据包存储在 VPN 数据包中，发送至本地计算机 1。由此，本地计算机 1 可以使用网络设备 6。

[0091] 在与本地计算机 1 之间确立 VPN 时，OS2051 启动通信控制程序 2055，和上述的第 1 实施方式的情况相同地，开始对通过 VPN 收发的通信数据包进行数据包过滤 (S226)。

[0092] 然后，OS2051 启动远程客户机程序 2053。远程客户机程序 2053，通过 VPN 向本地计算机 1 发送终端服务请求 (S227)。然后，若通过 VPN 从本地计算机 1 接收到终端服务请求应答，则开始利用由本地计算机通过 VPN 提供的终端服务 (S228)。

[0093] 图 9 是表示应用了第 2 实施方式的远程桌面系统的概略动作例的图。

[0094] 首先，远程计算机 2 向本地计算机 1 发送 VPN 连接请求 (S61)。本地计算机 1，当从远程计算机 2 接收 VPN 连接请求时，通过调查是否满足规定的条件，来判断可否连接 (S71)。

并且，若可以连接，则返回 VPN 连接应答 (S72)，在与远程计算机 2 之间确立 VPN(S73)。

[0095] 本地计算机 1，若在与远程计算机 2 之间确立了 VPN，则利用远程计算机 2 的 VPN 网关功能，访问 DHCP 服务器 7，从 DHCP 服务器 7 取得在 LAN4B 中的地址 (S74)。另外，开始数据包过滤服务和应用程序控制服务。另一方面，远程计算机 2 开始数据包过滤服务。

[0096] 然后，远程计算机 2 通过 VPN 向本地计算机 1 发送终端服务请求 (S62)。本地计算机 1，当通过 VPN 从远程计算机 2 接收到终端服务请求时，返回终端服务应答 (S75)，开始提供利用了 VPN 的终端服务 (S76)。

[0097] 远程计算机 2，当通过输入装置从用户接受打印指示时，利用 VPN 上的终端服务，将其操作内容（打印指示）发送至本地计算机 1(S63)。本地计算机 1，当从远程计算机 2 接收打印指示时，生成打印命令，利用远程计算机 2 的 VPN 网关功能，将其发送至打印机 6A(S77)。打印机 6A，根据经由远程计算机 2 从本地计算机 1 取得的打印命令，打印希望的文件 (S81)。

[0098] 另外，远程计算机 2，当通过输入装置从用户接受下载指示时，利用 VPN 上的终端服务，将其操作内容（下载指示）发送至本地计算机 1(S64)。本地计算机 1，当从远程计算机 2 接收下载指示时，利用远程计算机 2 的 VPN 网关功能，访问文件服务器 6B，从文件服务器 6B 下载希望的文件 (S78)。

[0099] 以上，对第 2 实施方式进行了说明。

[0100] 在本实施方式中，在终端服务中利用了 VPN。因此，除了上述的第 1 实施方式的效果以外，在本地计算机 1 和远程计算机 2 之间存在防火墙装置 3A、3B 的情况下，为使本地计算机 1 和远程计算机 2 可以通过 VPN 相连而仅对防火墙装置 3A、3B 进行设定，就可以实现本地计算机 1 和远程计算机 2 之间的终端服务。

[0101] （第 3 实施方式）

[0102] 对使用了上述的第 1 和 / 或第 2 实施方式的远程桌面系统的虚拟办公室系统进行说明。

[0103] 图 10 是表示应用了第 3 实施方式的虚拟办公室系统的概略结构例的图。

[0104] 如图所示，本实施方式的虚拟办公室系统具有 ：多台本地计算机 1A ～ 1N ；多台远程计算机 2A ～ 2N ；打印机（打印机服务器）、扫描仪（扫描仪服务器）、文件服务器等网络设备 6 ；DHCP 服务器 7。

[0105] 本地计算机 1A ～ 1N，分别与作为不同的 ASP(Application ServiceProvider) 的中心 1 ～中心 N 的 LAN4A 相连。LAN4B 通过防火墙装置 3B 与 WAN5 相连。

[0106] 远程计算机 2A ～ 2N，与网络设备 6 和 DHCP 服务器 7 一起，与构建在相同办公室中的 LAN4B 相连。LAN4B，通过防火墙装置 3B 与 WAN5 相连。

[0107] 本地计算机 1A ～ 1N，分别向对应于本地计算机 1A ～ 1N 的远程计算机 2A ～ 2N 提供终端服务。即，接收并处理从对应的远程计算机 2A ～ 2N 发送来的输入信息（输入装置的操作内容），同时将表示处理结果的图像信息（用于描绘显示装置的桌面画面的颜色信息、描绘命令信息、位图信息等）发送至远程计算机 2A ～ 2N。另外，本地计算机 1A ～ 1N 具备 VPN 接口功能，通过 VPN 和对应于该本地计算机 1A ～ 1N 的远程计算机 2 相连。另一方面，远程计算机 2A ～ 2N 具备 VPN 网关功能，将在与对应于该远程计算机 2A ～ 2N 的本地计算机 1A ～ 1N 之间所构建的 VPN，和 LAN4B 相连。

[0108] 由此，本地计算机 1A ～ 1N，利用对应于该本地计算机 1A ～ 1N 的远程计算机 2A ～ 2N 的 VPN 网关功能，与办公室的网络 4B 相连。本地计算机 1A ～ 1N，也可以通过对应的远程计算机 2A ～ 2N 相互连接。本地计算机 1A ～ 1N 和远程计算机 2A ～ 2N，可以使用在上述的第 1 和 / 或第 2 实施方式的远程桌面系统中所使用的本地计算机 1 和远程计算机 2。

[0109] 以上，对第 3 实施方式进行了说明。

[0110] 根据本实施方式，远程计算机 2A ～ 2N 与相同办公室的 LAN4B 相连，因此，本地计算机 1A ～ 1N 可以利用与该 LAN4B 相连的网络设备 6。从而，可以实现将本地计算机 1A ～ 1N 配置在相同的办公室中，可以使用相同网络设备的环境，即，虚拟办公室环境。

[0111] 此外，本发明实施方式不限于上述实施方式，在其主旨范围内，可以进行多种变更。

[0112] 例如，在上述的各实施方式中，以本地计算机 1 向远程计算机 2 提供终端服务的远程桌面系统为例进行了说明，但不限于此。也可以通过 VPN，将具有 VPN 接口功能的第 1 计算机和具有 VPN 网关功能的第 2 计算机相连，第 1 计算机利用第 2 计算机的 VPN 网关功能，与第 2 计算机连接在同一网络中。

[0113] 另外，在上述的各实施方式中，各程序可以从 CD-ROM、DVD-ROM 等移动存储介质安装到计算机（本地计算机 1、远程计算机 2）中。或者，也可以通过数字信号、载波、网络等通信介质，下载到计算机并安装。另外，也可以将上述各实施方式组合起来。

[0114] 根据本说明书，即使不针对与网络设备的通信中所使用的每个协议进行防火墙装置的设定，信息处理装置也可以越过防火墙、利用网络设备。

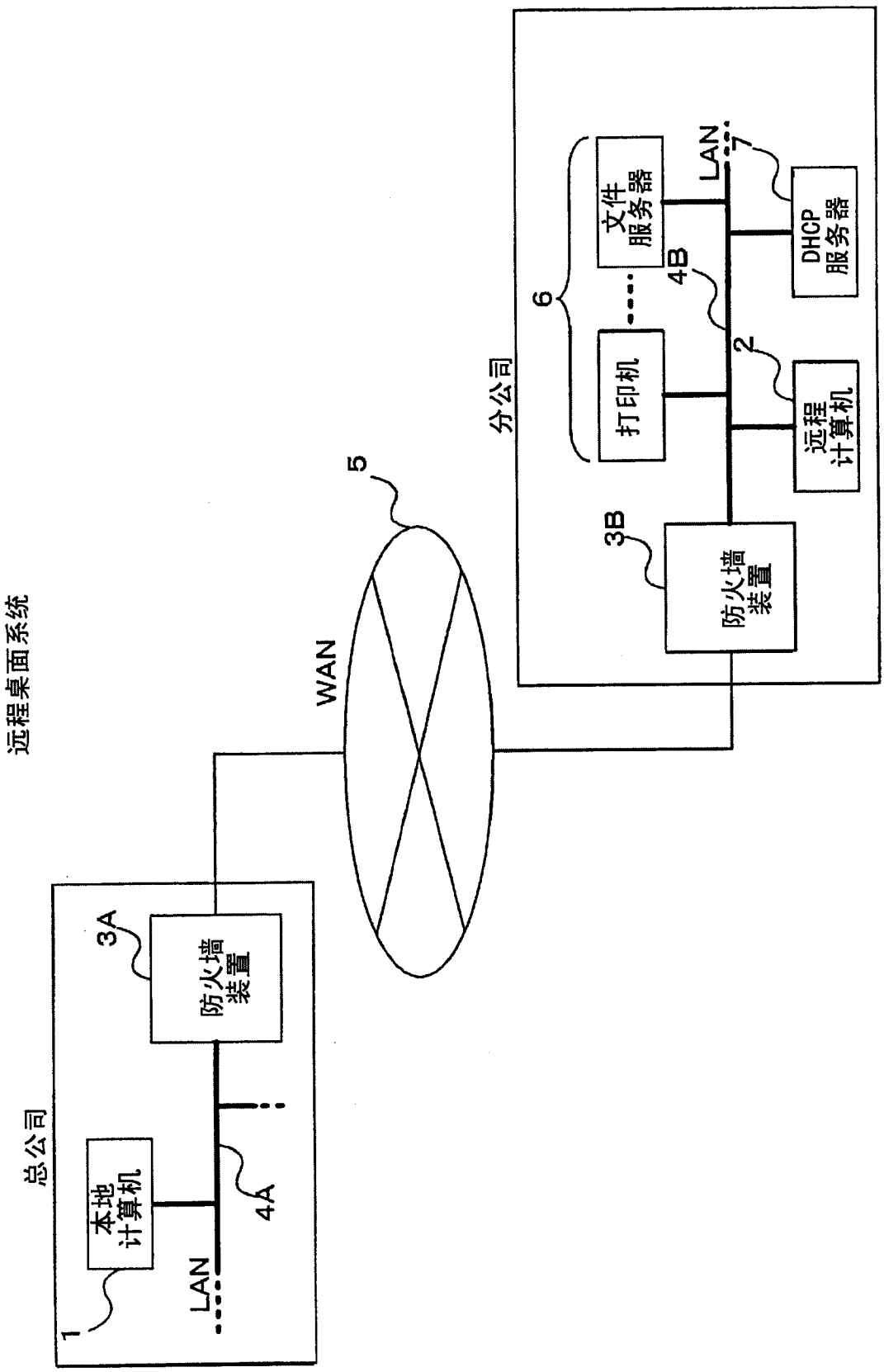

远程桌面系统
总公司
本地计算机
1
LAN
4A
3A
防火墙装置
WAN
5
分公司
6
打印机
文件服务器
4B
LAN
7
DHCP服务器
2
远程计算机
3B
防火墙装置

图 1

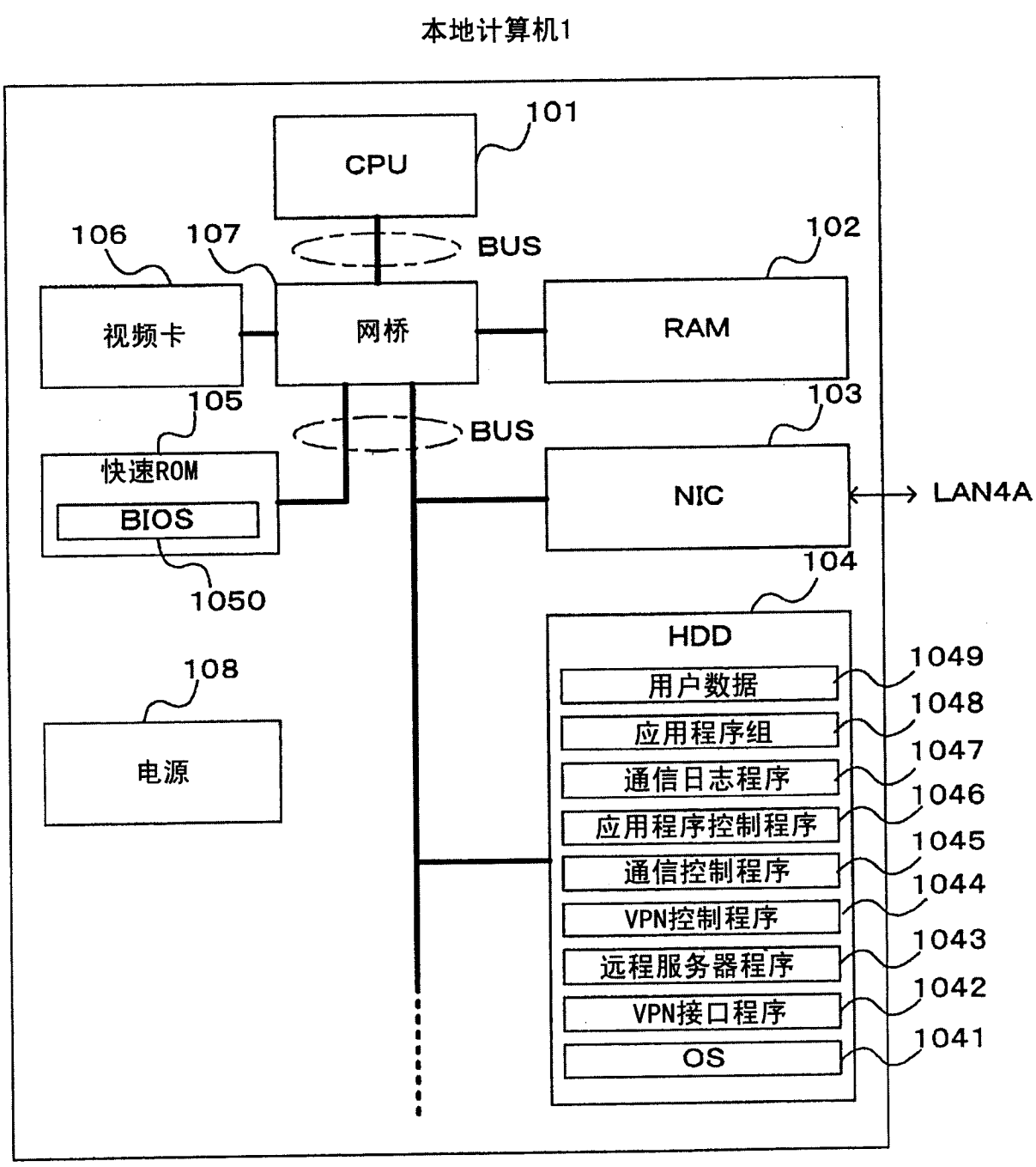

本地计算机1
CPU
101
BUS
106
107
102
视频卡
网桥
RAM
105
BUS
103
快速ROM
BIOS
NIC
LAN4A
1050
104
HDD
108
电源
用户数据
1049
应用程序组
1048
通信日志程序
1047
应用程序控制程序
1046
通信控制程序
1045
VPN控制程序
1044
远程服务器程序
1043
VPN接口程序
1042
OS
1041

图 2

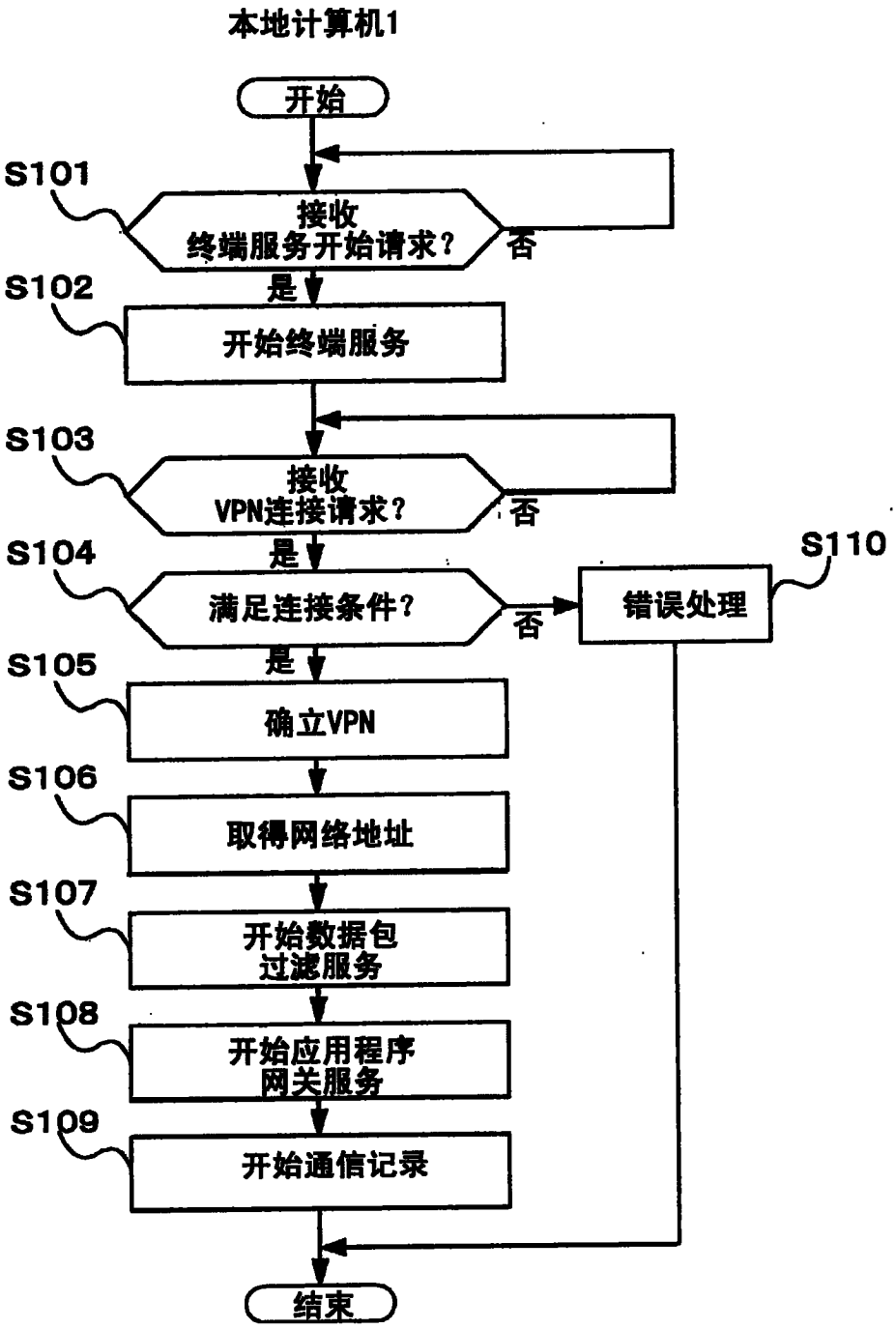

本地计算机1
开始
S101
接收
终端服务开始请求?
否
是
S102
开始终端服务
S103
接收
VPN连接请求?
否
是
S104
满足连接条件?
否
S110
错误处理
是
S105
确立VPN
S106
取得网络地址
S107
开始数据包
过滤服务
S108
开始应用程序
网关服务
S109
开始通信记录
结束

图 3

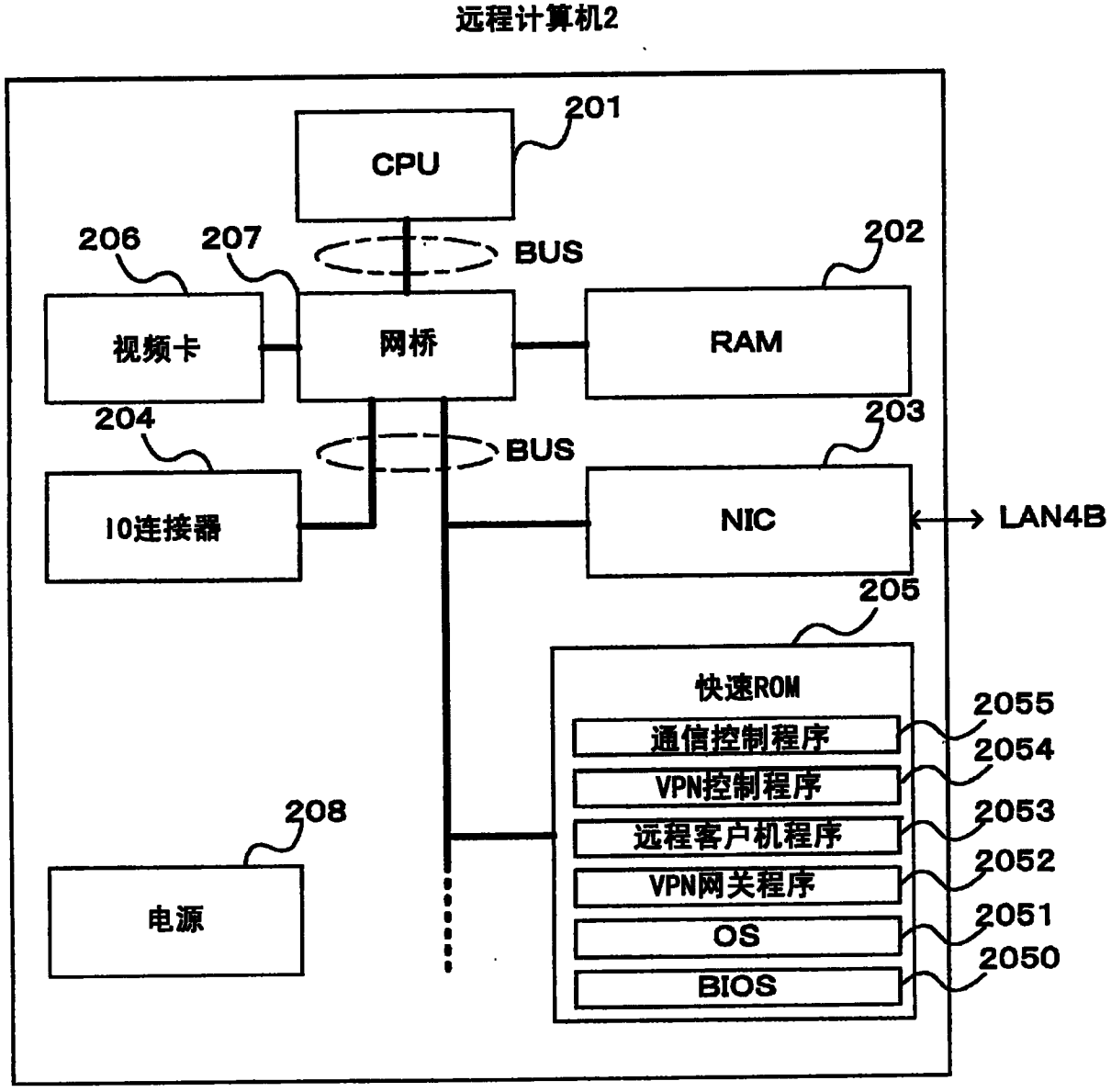

远程计算机2
CPU
201
206
207
BUS
202
视频卡
网桥
RAM
204
BUS
203
IO连接器
NIC
LAN4B
205
快速ROM
2055
通信控制程序
2054
VPN控制程序
208
2053
远程客户机程序
2052
VPN网关程序
电源
2051
OS
2050
BIOS

图 4

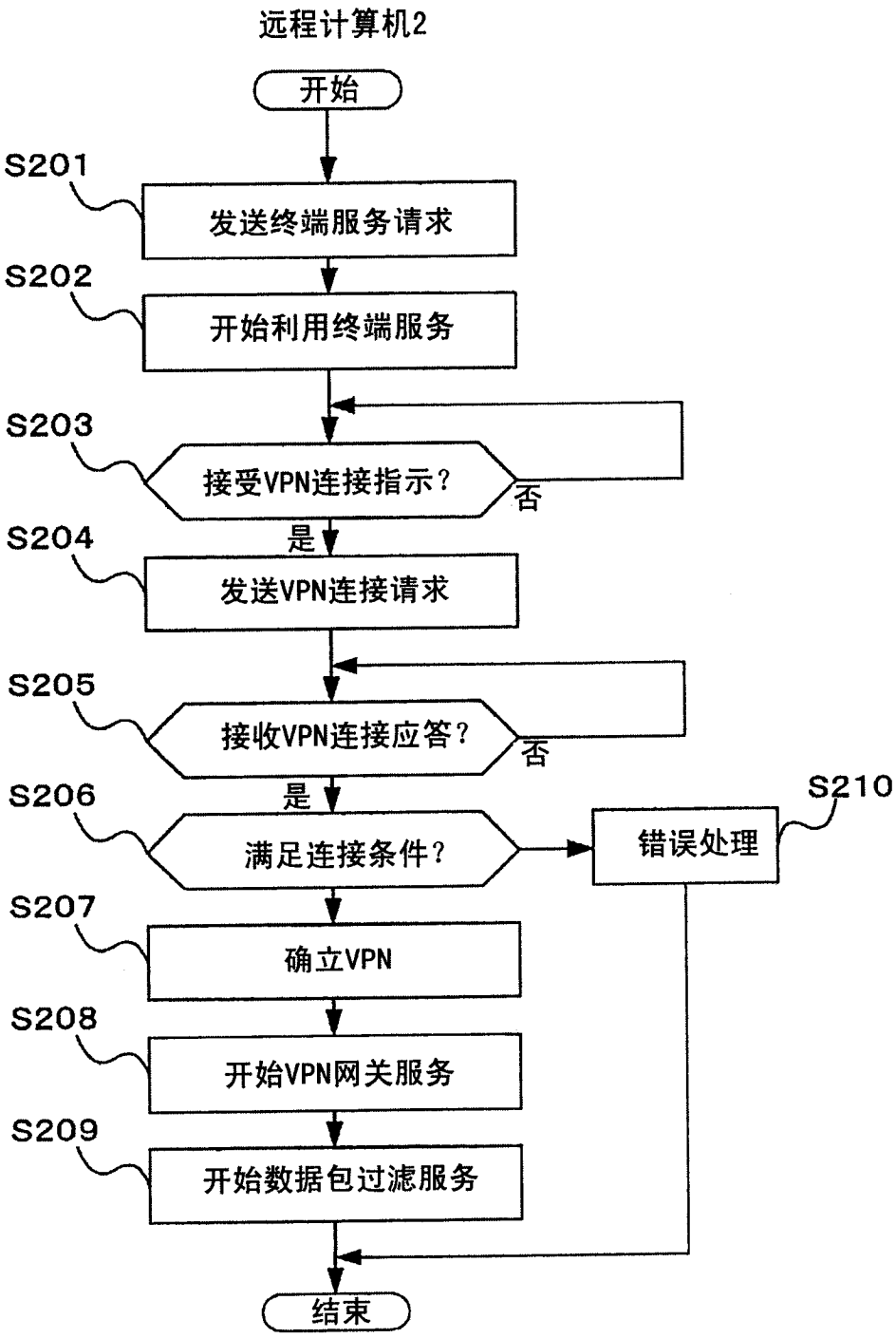

远程计算机2
开始
S201
发送终端服务请求
S202
开始利用终端服务
S203
接受VPN连接指示？
否
是
S204
发送VPN连接请求
S205
接收VPN连接应答？
否
是
S206
满足连接条件？
S210
错误处理
S207
确立VPN
S208
开始VPN网关服务
S209
开始数据包过滤服务
结束

图 5

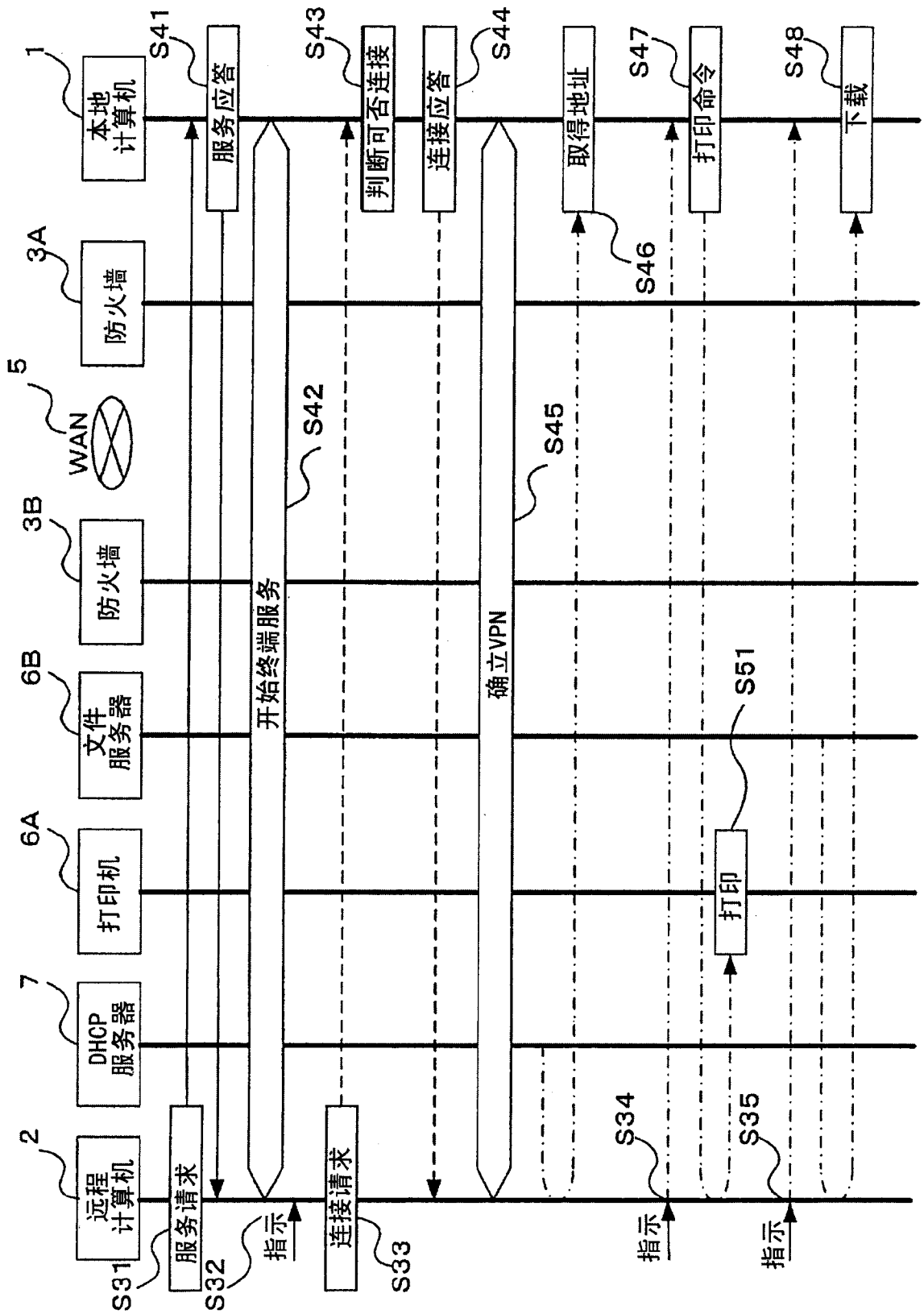

1
本地计算机
3A
防火墙
5
WAN
3B
防火墙
6B
文件服务器
6A
打印机
7
DHCP服务器
2
远程计算机
S41
服务应答
S43
判断可否连接
S44
连接应答
S46
取得地址
S47
打印命令
S48
下载
S42
开始终端服务
S45
确立VPN
S51
打印
S31
服务请求
S32
指示
S33
连接请求
S34
指示
S35
指示

图 6

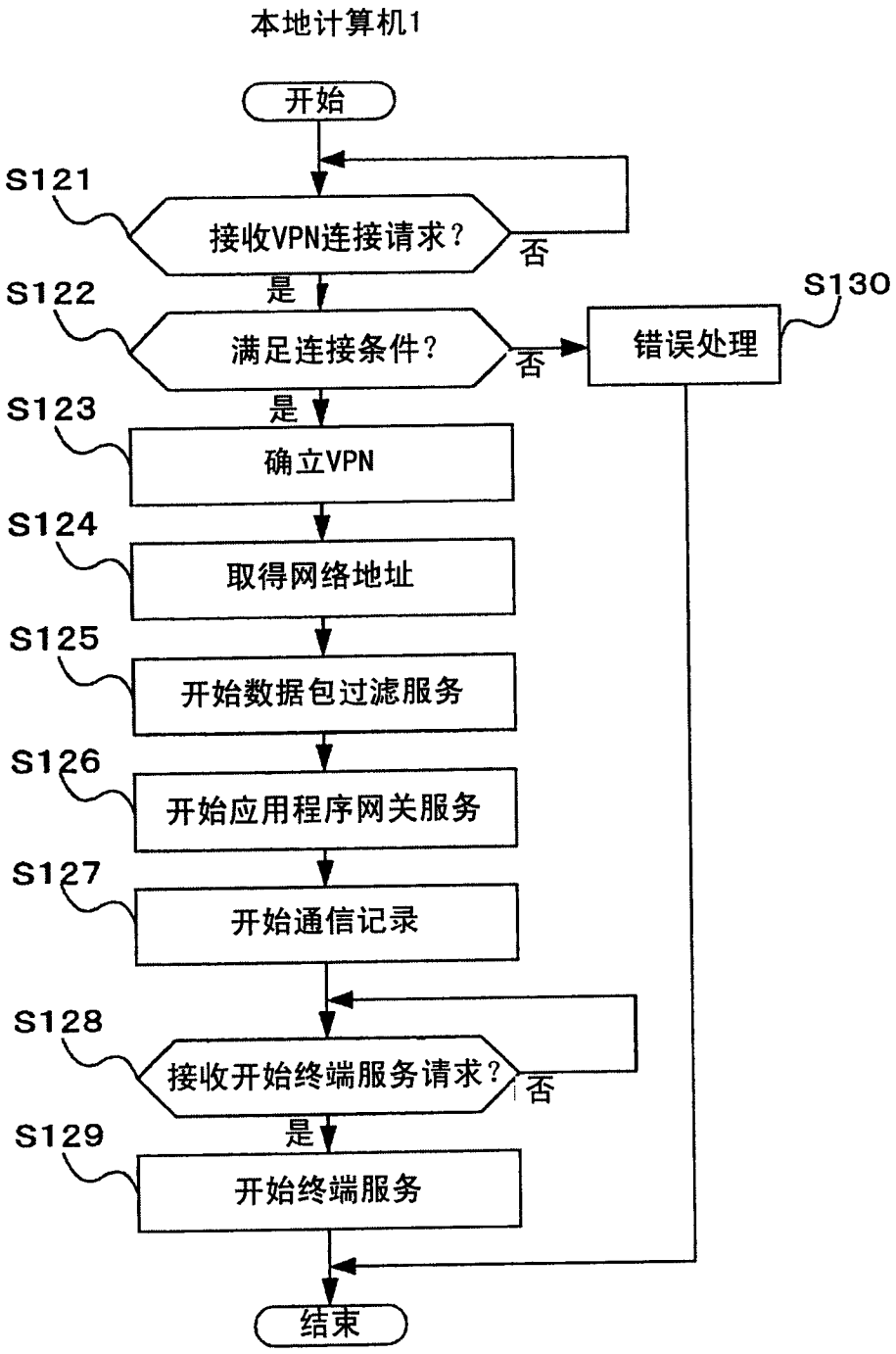

本地计算机1
开始
S121
接收VPN连接请求？
否
是
S122
满足连接条件？
否
S130
错误处理
是
S123
确立VPN
S124
取得网络地址
S125
开始数据包过滤服务
S126
开始应用程序网关服务
S127
开始通信记录
S128
接收开始终端服务请求？
否
是
S129
开始终端服务
结束

图 7

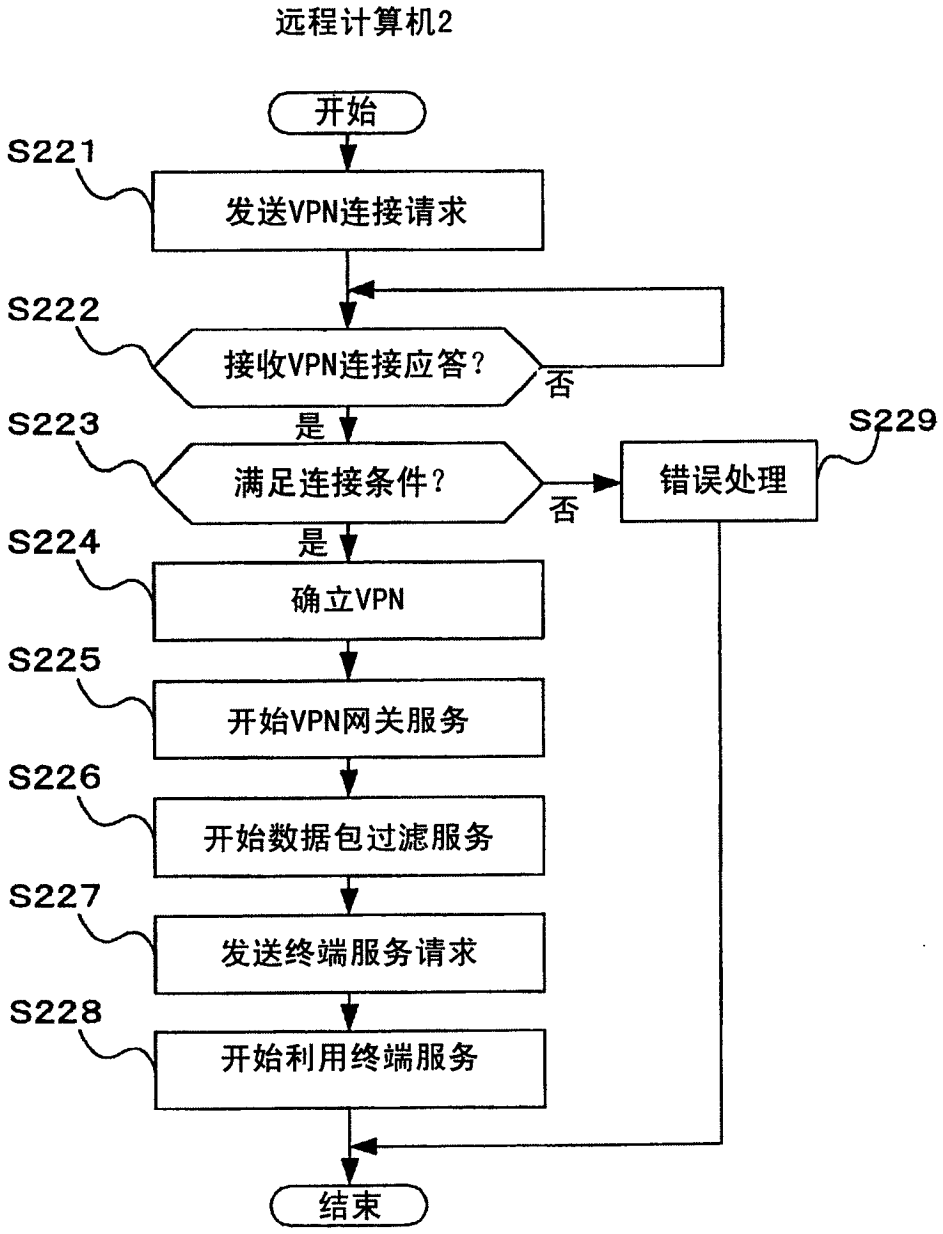

远程计算机2
开始
S221
发送VPN连接请求
S222
接收VPN连接应答？
否
是
S223
满足连接条件？
否
S229
错误处理
是
S224
确立VPN
S225
开始VPN网关服务
S226
开始数据包过滤服务
S227
发送终端服务请求
S228
开始利用终端服务
结束

图 8

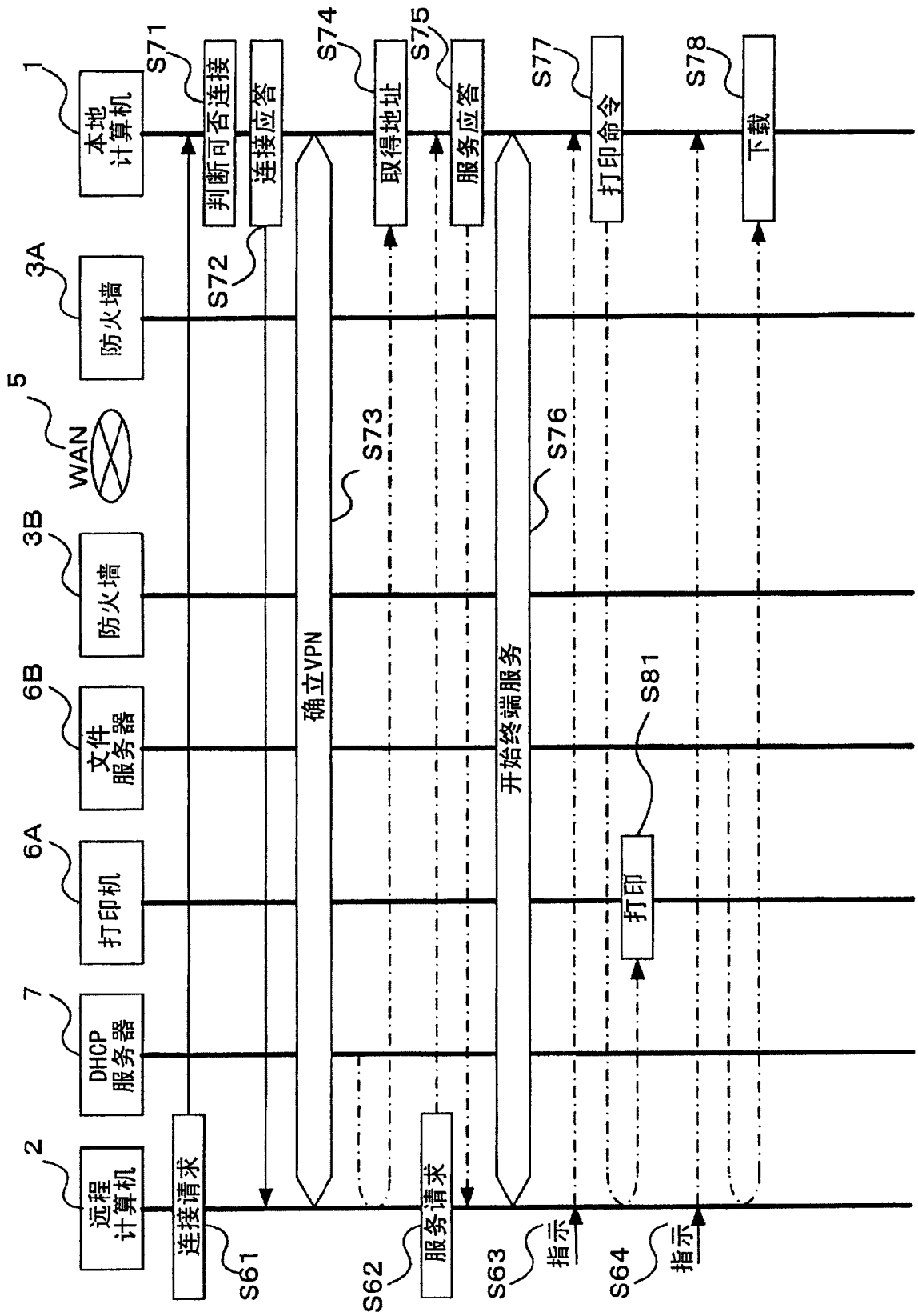

1
本地计算机
3A
防火墙
5
WAN
3B
防火墙
6B
文件服务器
6A
打印机
7
DHCP服务器
2
远程计算机
S71
判断可否连接
S72
连接应答
S73
确立VPN
S74
取得地址
S75
服务应答
S76
开始终端服务
S77
打印命令
S78
下载
S81
打印
连接请求
S61
服务请求
S62
指示
S63
指示
S64

图 9

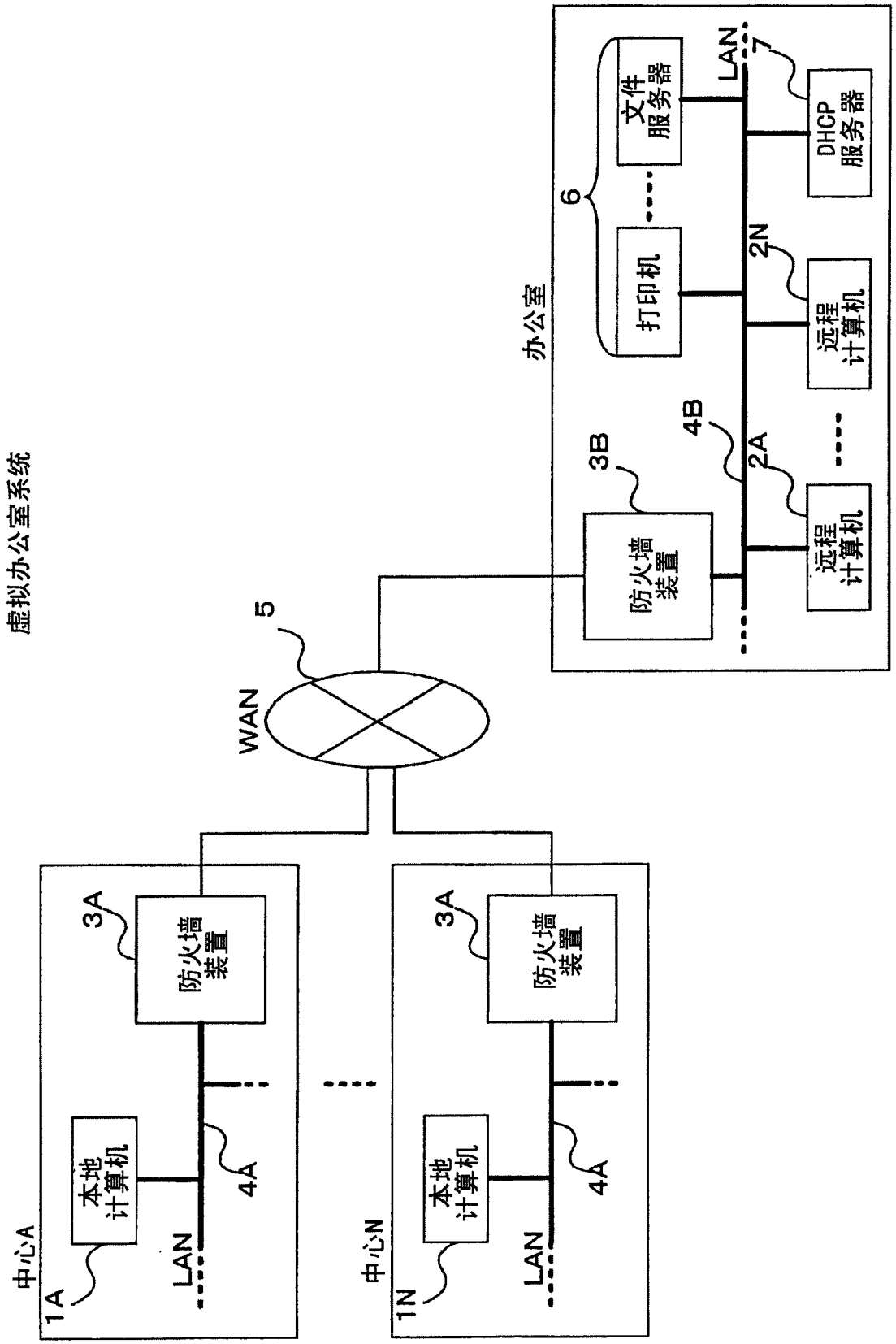

虚拟办公室系统
中心A
1A
本地计算机
LAN
4A
3A
防火墙装置
中心N
1N
本地计算机
LAN
4A
3A
防火墙装置
WAN
5
办公室
6
文件服务器
打印机
LAN
7
DHCP服务器
2N
远程计算机
4B
2A
远程计算机
3B
防火墙装置

图 10