

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200580030928.3

[43] 公开日 2008 年 6 月 11 日

[51] Int. Cl.  
*H04L 29/08 (2006.01 )*  
*H04L 29/06 (2006.01 )*

[11] 公开号 CN 101199187A

[22] 申请日 2005.7.22

[21] 申请号 200580030928.3

[30] 优先权

[32] 2004.7.23 [33] US [31] 60/590,837

[32] 2004.8.13 [33] US [31] 60/601,431

[32] 2004.9.3 [33] US [31] 60/607,420

[32] 2004.9.10 [33] US [31] 60/608,814

[86] 国际申请 PCT/US2005/026296 2005.7.22

[87] 国际公布 WO2006/012610 英 2006.2.2

[85] 进入国家阶段日期 2007.3.14

[71] 申请人 茨特里克斯系统公司

地址 美国佛罗里达州

[72] 发明人 G·P·劳 E·布吕格曼  
R·罗德里格兹

[74] 专利代理机构 中国专利代理(香港)有限公司  
代理人 王 岳 王忠忠

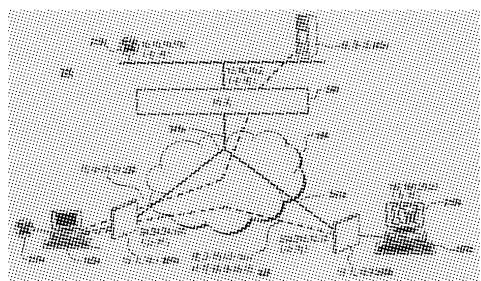
权利要求书 18 页 说明书 64 页 附图 15 页

[54] 发明名称

用于网络节点之间通信最优化的系统和方法

[57] 摘要

本发明总的针对用于提供对等通信和远程接入连接性的远程接入结构。在一个实施例中，本发明的远程接入结构提供用于经由诸如网关的第三计算设备建立对等计算设备之间的直接通信的方法。另外，本发明提供以下的使得对等通信最优化的技术：1)网络分组的接收的虚假确认允许经由无损分组协议传送对于经由有损协议传输被构建的分组，2)网络分组的有效负载移位允许经由无损分组协议传送对于经由有损协议传输被构建的分组，3)考虑由于加密造成的开销，通过调节最大传输单元(MTU)参数而减小分组分段，4)客户端网络通信的应用知道的优先化，以及5)网络中断保护，用于可靠的和持久的网络连接性与接入。



1. 一种用于建立在第一网络上的第一计算设备与第二网络上的第二计算设备之间的对等通信会话的方法，第一网络是与第二网络不连接的，并且不能路由到第二网络，该方法包括以下步骤：

(a) 由第一计算设备建立与第三计算设备的第一隧道会话，和由第二计算设备建立与第三计算设备的第二隧道会话；

(b) 由第一计算设备经由第三计算设备发起到第二计算设备的通信会话；

(c) 由服务器接收用来建立该通信会话的信号；

(d) 由服务器把第一网络地址传送到第一计算设备，该第一网络地址包括与第二隧道会话关联的第二计算设备的网络地址；

(e) 由第一计算设备通过使用第一网络地址来传送发起与第二计算设备的连接的请求；

(f) 由第三计算设备截取该请求，并为第一计算设备提供用于第二计算设备的第二网络地址，第二网络地址包括与第二计算设备关联的公共网地址；以及

(g) 由第三计算设备通过使用第二网络地址把请求传送到第二计算设备，以便允许来自第一计算设备的连接。

2. 权利要求1的方法，其中第一隧道会话或第二隧道会话之一的至少一部分包括安全套接字层或虚拟专用网络之一。

3. 权利要求1的方法，其中第三计算设备包括远程接入网关。

4. 权利要求1的方法，其中第二计算设备位于与第二网络地址关联的防火墙的后面。

5. 权利要求1的方法，包括通过把带外信号经由第一隧道会话传送到第一计算设备而由第三计算设备把第二网络地址提供给第一计算设备。

6. 权利要求1的方法，包括由第二计算设备为第一计算设备提供在防火墙中的转发口，以便使用第二网络地址与第二计算设备通信。

7. 权利要求1的方法，包括由第三计算设备把密钥传送到第一计算设备和第二计算设备。

8. 权利要求7的方法，包括由第一计算设备把密钥传送到第二计

---

算设备。

9. 权利要求8的方法，包括由第一计算设备在把数据发送到第二计算设备之前检验从第二计算设备接收的密钥与第一计算设备的密钥相匹配。

10. 权利要求7的方法，包括由第二计算设备把密钥传送到第一计算设备。

11. 权利要求10的方法，包括由第二计算设备在把数据发送到第二计算设备之前检验从第一计算设备接收的密钥与第二计算设备的密钥相匹配。

12. 权利要求1的方法，把第一电信设备与第一计算设备相关联，和把第二电信设备与第二计算设备相关联。

13. 权利要求12的方法，其中第一电信设备或第二电信设备之一包括软件部件或硬件部件之一。

14. 权利要求12的方法，包括经由连接建立在第一电信设备与第二电信设备之间的电信会话。

15. 权利要求15的方法，包括在第一电信设备和第二电信设备之间通过电信会话进行通信，而不用经过第一计算设备。

16. 权利要求1的方法，包括经由在第一计算设备和第二计算设备之间的连接，来传送远程显示协议。

17. 权利要求16的方法，其中远程桌面协议包括独立计算结构协议或远程桌面协议之一。

18. 权利要求1的方法，包括经由连接与第二计算设备共享第一计算设备的屏幕视图。

19. 在网关中，一种用于建立在第一网络上的第一计算设备与第二网络上的第二计算设备之间的对等通信会话的方法，第一网络是与第二网络不连接的，并且不能路由到第二网络，该方法包括以下步骤：

(a) 在第一网络上建立与第一计算设备的第一隧道会话；

(b) 在第二网络上建立与第二计算设备的第二隧道会话；

(c) 接收由第一计算设备发起与第二计算设备的通信会话的请求；

(d) 把用于联系第二计算设备的第一网络地址提供给第一计算设

备，第一网络地址包括与第二隧道会话关联的第二计算设备的网络地址；

(e) 通过使用第一网络地址，来接收由第一计算设备发起与第二计算设备的连接的请求；

(f) 截取发起连接的请求，并为第一计算设备提供用于第二计算设备的第二网络地址，第二网络地址包括与第二计算设备关联的公共网地址；以及

(g) 通过使用第二网络地址把请求传送到第二计算设备，以便允许从第一计算设备到第二计算设备的连接。

20. 权利要求19的方法，其中第一隧道会话或第二隧道会话之一的至少一部分包括安全套接字层或虚拟专用网络之一。

21. 权利要求19的方法，其中第二计算设备位于与第二网络地址关联的防火墙的后面。

22. 权利要求19的方法，包括通过把带外信号经由第一隧道会话传送到第一计算设备而把第二网络地址提供给第一计算设备。

23. 权利要求19的方法，包括把密钥传送到第一计算设备。

24. 权利要求19的方法，包括把密钥传送到第二计算设备。

25. 一种用于经由第三计算设备建立在第一网络上的第一计算设备与第二网络上的第二计算设备之间的对等通信会话的系统，第一网络是与第二网络不连接的，并且不能路由到第二网络，该系统包括：

在第一网络上的第一计算设备；

在第二网络上的第二计算设备；

第三计算设备，建立与第一计算设备的第一隧道会话，和与第二计算设备的第二隧道会话；

经由第三计算设备可接入的服务器；

其中：

服务器经由第三计算设备把第一网络地址传送到第一计算设备，该第一网络地址包括与第二隧道会话关联的第二计算设备的网络地址；

第一计算设备通过使用第一网络地址经由第三计算设备传送发起与第二计算设备的连接的请求；

第三计算设备截取第一请求，并为第一计算设备提供用于第二计算设备的第二网络地址，第二网络地址包括与第二计算设备关联的公共网地址；以及

第三计算设备通过使用第二网络地址传送第二请求到第二计算设备，允许来自第一计算设备的连接。

26. 权利要求25的系统，其中第一隧道会话或第二隧道会话之一的至少一部分包括安全套接字层或虚拟专用网络之一。

27. 权利要求25的系统，其中第三计算设备包括远程接入网关。

28. 权利要求25的系统，其中第二计算设备位于与第二网络地址关联的防火墙的后面。

29. 权利要求25的系统，其中第三计算设备通过经由第一隧道会话传送带外信号来把第二网络地址提供给第一计算设备。

30. 权利要求25的系统，其中第二计算设备为第一计算设备提供在防火墙中的转发口，以便使用第二网络地址与第二计算设备通信。

31. 权利要求25的系统，其中第三计算设备把密钥传送到第一计算设备和第二计算设备。

32. 权利要求31的系统，其中第一计算设备把密钥传送到第二计算设备。

33. 权利要求32的系统，其中第一计算设备在把数据发送到第二计算设备之前检验从第二计算设备接收的密钥与第一计算设备的密钥相匹配。

34. 权利要求31的系统，其中第二计算设备把密钥传送到第一计算设备。

35. 权利要求34的系统，其中第二计算设备在把数据发送到第二计算设备之前检验从第一计算设备接收的密钥与第二计算设备的密钥相匹配。

36. 权利要求25的系统，包括与第一计算设备关联的第一电信设备，和与第二计算设备关联的第二电信设备。

37. 权利要求36的系统，其中第一电信设备或第二电信设备之一包括软件部件或硬件部件之一。

38. 权利要求37的系统，其中第一电信设备经由连接建立与第二

电信设备的电信会话。

39. 权利要求38的系统，其中第一电信设备通过电信会话与第二电信设备进行通信，而不用经过第三计算设备。

40. 权利要求25的系统，第一计算设备和第二计算设备经由连接来传送远程显示协议。

41. 权利要求25的系统，其中远程桌面协议包括独立计算结构协议或远程桌面协议之一。

42. 权利要求25的系统，包括第一计算设备经由连接与第二计算设备共享屏幕视图。

43. 一种用于建立在第一网络上的第一计算设备与第二网络上的第二计算设备之间的对等通信会话的网关，第一网络是与第二网络不连接的，并且不能路由到第二网络，该网关包括：

用于在第一网络上建立与第一计算设备的第一隧道会话的装置；

用于在第二网络上建立与第二计算设备的第二隧道会话的装置；

用于接收由第一计算设备发起与第二计算设备的通信会话的请求的装置；

用于把用于联系第二计算设备的第一网络地址提供给第一计算设备的装置，第一网络地址包括与第二隧道会话关联的第二计算设备的网络地址；

用于通过使用第一网络地址，来接收由第一计算设备发起与第二计算设备的连接的请求的装置；

用于截取发起连接的请求，并为第一计算设备提供用于第二计算设备的第二网络地址的装置，第二网络地址包括与第二计算设备关联的公共网地址；以及

用于通过使用第二网络地址把请求传送到第二计算设备，以允许从第一计算设备到第二计算设备的连接的装置。

44. 权利要求43的系统，其中第一隧道会话或第二隧道会话之一的至少一部分包括安全套接字层或虚拟专用网络之一。

45. 权利要求43的系统，其中第二计算设备位于与第二网络地址关联的防火墙的后面。

46. 权利要求43的系统，包括用于通过把带外信号经由第一隧道会话传送到第一计算设备来把第二网络地址提供给第一计算设备的装置。

47. 权利要求43的系统，包括用于把密钥传送到第一计算设备的装置。

48. 权利要求43的系统，包括把密钥传送到第二计算设备的装置。

49. 一种经由无损协议传送对于经由有损协议传输被构建的分组的方法，该方法包括以下步骤：

(a) 经由无损协议建立在第一计算设备与第二计算设备之间的连接；

(b) 由第一计算设备检测无损协议分组，无损协议分组包括具有按照有损协议被构建的一个或多个分组的有效负载；

(c) 由第一计算设备把无损协议分组的接收的虚假确认传送到第一计算设备或第二计算设备之一；以及

(d) 由第一计算设备把无损协议分组传送到第二计算设备。

50. 权利要求49的方法，包括由第一计算设备使用密钥来加密一个或多个分组。

51. 权利要求50的方法，包括经由在第一计算设备与第二计算设备之间的带外传输安全层会话来提供加密密钥到第一计算设备。

52. 权利要求49的方法，包括逐个分组地加密一个或多个分组。

53. 权利要求49的方法，还包括在步骤(d)之前执行步骤(c)。

54. 权利要求49的方法，其中第二计算设备是网关。

55. 权利要求49的方法，包括响应于由第一计算设备或第二计算设备之一接收到无损协议分组的接收的虚假确认，阻止第一计算设备或第二计算设备之一的网络堆栈执行与提供无损协议的无损特性关联的操作。

56. 权利要求49的方法，其中无损协议包括传输控制协议。

57. 权利要求56的方法，包括阻止第一计算设备或第二计算设备之一的网络堆栈执行与无损协议有关的一个或多个以下的算法：重发、排序、流控制算法、nagle的算法、和滑动窗口算法。

58. 权利要求49的方法，其中有损协议包括用户数据报协议。

59. 权利要求49的方法，包括由第一计算设备经由安全套接字层或传输安全层隧道之一把无损协议分组传送到第二计算设备。

60. 权利要求49的方法，其中一个或多个分组包括实时协议。

61. 权利要求49的方法，包括由第一计算设备把实时话音、音频或数据之一经由一个或多个分组传送到第二计算设备。

62. 一种用于经由无损协议传送对于经由有损协议传输被构建的分组的系统，该系统包括：

    用于经由无损协议建立在第一计算设备与第二计算设备之间的连接的装置；

    用于由第一计算设备检测无损协议分组的装置，无损协议分组包括具有按照有损协议被构建的一个或多个分组的有效负载；

    用于由第一计算设备把无损协议分组的接收的虚假确认传送到第一计算设备或第二计算设备之一的装置；以及

    用于由第一计算设备把无损协议分组传送到第二计算设备的装置。

63. 权利要求62的系统，包括用于由第一计算设备使用密钥来加密一个或多个分组的装置。

64. 权利要求63的系统，包括用于经由在第一计算设备与第二计算设备之间的带外传输安全层会话来提供加密密钥到第一计算设备的装置。

65. 权利要求63的系统，包括用于逐个分组地加密一个或多个分组的装置。

66. 权利要求62的系统，还包括用于在传送无损协议分组之前传送无损协议分组的接收的虚假确认的装置。

67. 权利要求62的系统，其中第二计算设备是网关。

68. 权利要求62的系统，包括用于响应于由第一计算设备或第二计算设备之一接收到无损协议分组的接收的虚假确认，以阻止第一计算设备或第二计算设备之一的网络堆栈执行与提供无损协议的无损特性关联的操作的装置。

69. 权利要求62的系统，其中无损协议包括传输控制协议。

70. 权利要求69的系统，包括用于阻止第一计算设备或第二计算设备之一的网络堆栈执行与无损协议有关的一个或多个以下的算

法：重发、排序、和流控制算法的装置。

71. 权利要求62的系统，其中有损协议包括用户数据报协议。

72. 权利要求62的系统，包括用于由第一计算设备经由安全套接字层或传输安全层隧道之一把无损协议分组传送到第二计算设备的装置。

73. 权利要求62的系统，其中一个或多个分组包括实时协议。

74. 权利要求62的系统，包括用于由第一计算设备把实时话音、音频或数据之一经由一个或多个分组传送到第二计算设备的装置。

75. 一种通过使用在TCP连接上不可靠的传输协议发送来自应用的分组的方法，包括：

在第一设备处接收要使用不可靠的传输协议发送的第一分组；

创建第一TCP分组，该第一TCP分组包括接收的第一分组的第一有效负载和与在第一设备与第二设备之间建立的TCP连接关联的信息的第一TCP首部；

由第一设备把第一TCP分组发送到第二设备；

在第一设备处接收要使用不可靠的传输协议发送的第二分组；

创建第二TCP分组，该第二TCP分组包括接收的第二分组的第二有效负载和第一TCP首部信息；以及

由第一设备在接收来自第二设备的第一有效负载的接收的确认之前把第二TCP分组发送到第二设备。

76. 权利要求75的方法，包括建立与一个端口号的TCP连接，该端口号与不可靠的传输协议相关联。

77. 权利要求75的方法，包括由第一设备动态地确定包括不可靠的传输协议的第一TCP分组与第二TCP分组。

78. 权利要求75的方法，其中不可靠的传输协议是UDP。

79. 权利要求75的方法，还包括：

在第一设备上通过使用分组捕获机构截取第一TCP分组与第二TCP分组来接收第一TCP分组与第二TCP分组。

80. 权利要求75的方法，包括由第一设备建立与VPN网关设备的TCP连接。

81. 权利要求75的方法，包括经由TCP连接建立在第一设备与第二设备之间的对等通信。

82. 权利要求75的方法，包括由第一设备加密第一与第二TCP分组，和由第二设备解密该加密的第一与第二TCP分组。

83. 一种通过使用在TCP连接上的不可靠的传输协议发送来自应用的分组的方法，包括：

在第二设备处截取在第一设备处创建的和在第二设备处接收的第一TCP分组，第一TCP分组包括由应用通过使用不可靠的传输协议生成的第一分组的第一有效负载和与在第一设备与第二设备之间建立的TCP连接关联的信息的第一TCP首部，截取在第一TCP分组被提供给第二设备的TCP堆栈之前发生；

响应于信息的TCP首部来识别第一有效负载是由应用通过使用不可靠的传输协议而生成的分组；

从第一TCP分组剥离信息的TCP首部；以及

通过使用不可靠的传输协议把第一有效负载转发到应用。

84. 权利要求83的方法，其中不可靠的协议是UDP。

85. 权利要求83的方法，其中识别的步骤包括识别TCP首部信息，TCP首部信息包括与不可靠的传输协议关联的端口号。

86. 权利要求83的方法，还包括：

由第二设备通过使用分组捕获驱动器截取第一TCP分组。

87. 权利要求83的方法，其中第一设备是客户端设备并且第二设备是VPN网关。

88. 权利要求87的方法，还包括：

在把第一有效负载转发到应用之前在第二设备上执行网络地址转换（NAT）。

89. 一种用于通过使用在TCP连接上的不可靠的传输协议发送来自应用的分组的系统，该系统包括：

第一设备，第一设备包括：

生成第一和第二分组的应用，第一和第二分组打算通过使用不可靠的传输协议被发送；

过滤器进程，过滤器进程截取来自应用的第一和第二分组，并把截取的分组转发到隧道进程。

隧道进程，隧道进程请求打开在第一设备与第二设备之间的TCP连接，打开TCP连接的请求向第一和第二设备表示，TCP连接将传输

打算用不可靠的传输协议发送的分组，隧道进程把第一和第二分组作为在第一和第二TCP分组中的有效负载转发到第二设备，隧道进程在发送第一TCP分组之后并在接收对于第一TCP分组的确认之前发送第二TCP分组；以及

与第一设备进行通信的第二设备，第二设备包括：

第二隧道进程，该第二隧道进程打开由第一设备请求的TCP连接，并识别和把TCP连接的源地址转发到第二过滤器进程；以及

第二过滤器进程，该第二过滤器进程截取在第二设备处用首部中的TCP连接源地址接收的、来自应用的分组，第二过滤器进程从接收的分组剥离TCP首部，把被剥离的分组转发到打算的目的地，并绕过在第二设备上的TCP/IP堆栈。

90. 权利要求89的系统，其中在第一设备上的第一过滤器进程包括分组捕获驱动器。

91. 权利要求89的系统，其中在第二设备上的第二过滤器进程包括分组捕获驱动器。

92. 权利要求89的系统，其中第一设备是客户端设备并且第二设备是VPN网关设备。

93. 权利要求89的系统，还包括：

第三设备，剥离的分组被发送到该第三设备。

94. 权利要求93的系统，其中第二设备还包括：

网络地址转换(NAT)表，用来在把剥离的分组发送到第三设备之前执行网络地址转换。

95. 权利要求89的系统，其中不可靠的数据协议是UDP。

96. 一种用于调节安全网络通信的最大传输单元以减小网络分段的方法，该方法包括以下步骤：

(a) 建立在第一计算设备与第二计算设备之间的会话，第一计算设备具有第一网络堆栈；

(b) 由第一计算设备检测具有加密的有效负载的网络分组；

(c) 由第一计算设备确定对于第一网络堆栈的最大传输单元参数的设置，以将最大传输单元尺寸减小至少与有效负载的加密部分关联的一个尺寸；以及

(d) 把第一网络堆栈的最大传输单元(MTU)参数改变到所确定的

设置。

97. 权利要求96的方法，包括经由安全套接字层或传输层安全隧道之一把网络分组传送到第二计算设备。

98. 权利要求96的方法，其中有效负载包括实时协议。

99. 权利要求96的方法，还包括经由第一网络堆栈的网络驱动器接口技术规范水平机构来改变最大传输单元参数。

100. 权利要求96的方法，还包括对每个在第一计算设备与第二计算设备之间的会话动态地确定最大传输单元参数的设置。

101. 权利要求96的方法，包括经由网关建立在第一计算设备与第二计算设备之间的会话。

102. 权利要求96的方法，包括由第一计算设备把实时话音、音频或数据之一经由网络分组的有效负载传送到第二计算设备。

103. 权利要求96的方法，包括在传送网络分组之前把网络分组的接收的虚假确认传送到第一计算设备或第二计算设备之一。

104. 权利要求96的方法，还包括经由第一计算设备的代理建立在第一计算设备与第二计算设备之间的会话。

105. 权利要求104的方法，包括由代理经由 IOCTL 应用编程接口与第一网络堆栈通信，以便把最大传输单元参数改变到所确定的设置。

106. 一种用于调节安全网络通信的最大传输单元以减小网络分段的系统，该系统包括：

    用于建立在第一计算设备与第二计算设备之间的会话的装置，第一计算设备具有第一网络堆栈；

    用于由第一计算设备检测具有加密的有效负载的网络分组的装置；

    用于由第一计算设备确定对于第一网络堆栈的最大传输单元参数的设置，以将最大传输单元尺寸减小至少与有效负载的加密部分关联的一个尺寸的装置；以及

    用于把第一网络堆栈的最大传输单元（MTU）参数改变到所确定的设置的装置。

107. 权利要求106的系统，包括用于经由安全套接字层或传输层安全隧道之一把网络分组传送到第二计算设备的装置。

108. 权利要求106的系统，其中有效负载包括实时协议。

109. 权利要求106的系统，其中有效负载包括实时话音、音频或数据之一的表示。

110. 权利要求106的系统，还包括用于经由第一网络堆栈的网络驱动器接口技术规范水平机构来改变第一计算设备的最大传输单元参数的装置。

111. 权利要求106的系统，还包括用于对每个在第一计算设备与第二计算设备之间的会话动态地确定最大传输单元参数的设置的装置。

112. 权利要求106的系统，包括用于经由网关建立在第一计算设备与第二计算设备之间的会话的装置。

113. 权利要求106的系统，包括用于由第一计算设备把实时话音、音频或数据之一经由网络分组的有效负载传送到第二计算设备的装置。

114. 权利要求106的系统，包括用于在传送网络分组之前把网络分组的接收的虚假确认传送到第一计算设备或第二计算设备之一的装置。

115. 权利要求106的系统，其中网络分组包括无损协议分组。

116. 权利要求115的系统，其中无损协议分组包括传输控制协议。

117. 权利要求106的系统，其中有效负载包括有损协议分组。

118. 权利要求117的系统，其中有损协议分组包括用户数据报协议。

119. 权利要求106的系统，包括第一计算设备的代理，用于建立在第一计算设备与第二计算设备之间的会话。

120. 权利要求119的系统，其中代理经由 IOCTL 应用编程接口与第一网络堆栈通信，以便把最大传输单元参数改变到所确定的设置。

121. 一种为客户端优先化与客户端的应用关联的网络通信的方法，该方法包括以下步骤：

(a) 由客户端截取与客户端的一个或多个应用关联的一个或多个网络分组；

- (b) 由客户端存储该一个或多个网络分组到一个队列；
- (c) 由客户端确定与客户端的第一应用关联的排队的一个或多个网络分组；
- (d) 由客户端表示所确定的一个或多个网络分组的优先权，以便把确定的一个或多个网络分组放置在与客户端的第二应用关联的、队列中的至少一个网络分组之前；以及
- (e) 提供优先化的一个或多个网络分组以便经由客户端的网络堆栈通信。

122. 权利要求121的方法，其中由客户端确定的步骤还包括确定第一应用的排队的一个或多个网络分组包括实时数据。

123. 权利要求122的方法，其中实时数据包括以下的一项：实时协议、用户数据报协议、和话音或音频之一的表示。

124. 权利要求121的方法，包括由客户端阻止第二应用的至少一个网络分组在第一应用的一个或多个网络分组之前经由网络堆栈被传送。

125. 权利要求121的方法，包括由客户端把与第二应用关联的网络分组保存在队列中，并当在保存的网络分组之前优先化的、与第一应用关联的一个或多个网络分组被传送时释放保存的网络分组。

126. 权利要求121的方法，包括由客户端对于客户端上的一个或多个应用透明地截取一个或多个网络分组。

127. 权利要求121的方法，包括在前台运行第一应用，以及在后台运行第二应用。

128. 权利要求121的方法，包括把比与第二应用关联的优先权更高的优先权与第一应用相关联。

129. 权利要求128的方法，还包括由用户规定的第二应用之一的优先权。

130. 权利要求121的方法，包括由客户端接收来自计算设备的一个或多个网络分组。

131. 权利要求121的方法，包括由该一个或多应用提供一个或多个网络分组，用于从客户端到计算设备传送。

132. 一种客户端，用于对与客户端的应用关联的客户端网络通信进行优先化，该客户端包括：

用于截取与客户端的一个或多个应用关联的客户端的一个或多个网络分组的机构；

网络驱动器，用于存储一个或多个网络分组到一个队列，并经由客户端的网络堆栈传送该一个或多个网络分组；以及

代理，用于确定与客户端的第一应用关联的一个或多个网络分组，并向网络驱动器表示该一个或多个网络分组的优先权，以把所确定的一个或多个网络分组放置在与客户端的第二应用关联的、队列中的至少一个网络分组的前面。

133. 权利要求132的客户端，其中代理确定第一应用的一个或多个网络分组包括实时数据。

134. 权利要求132的客户端，其中实时数据包括以下的一项：实时协议、用户数据报协议、和话音或音频之一的表示。

135. 权利要求132的客户端，其中代理或网络驱动器之一阻止第二应用的至少一个网络分组在第一应用的一个或多个网络分组之前经由网络堆栈被传送。

136. 权利要求132的客户端，其中网络驱动器把与第二应用关联的网络分组保存在队列中，并当在保存的网络分组之前优先化的、与第一应用关联的一个或多个网络分组被传送后释放所保存的网络分组。

137. 权利要求132的客户端，其中机构对于客户端上的一个或多个应用透明地截取一个或多个网络分组。

138. 权利要求132的客户端，其中第一应用在前台运行，以及第二应用在后台运行。

139. 权利要求132的客户端，其中第一应用具有比客户端的第二应用更高的优先权。

140. 权利要求132的客户端，包括用于由用户规定优先权的配置机构。

141. 权利要求132的客户端，其中客户端接收来自计算设备的一个或多个网络分组。

142. 权利要求132的客户端，其中该一个或多个应用提供一个或多个网络分组以便从客户端到计算设备的传送。

143. 权利要求132的客户端，其中网络驱动器包括网络驱动器接

口技术规范 (NDIS) 驱动器。

144. 权利要求132的客户端，其中网络驱动器在客户端的操作系统的内核模式下工作。

145. 权利要求132的客户端，其中代理在客户端的操作系统的用户模式下工作。

146. 权利要求132的客户端，其中代理或网络驱动器之一包括用于截取客户端的一个或多个网络分组的机构。

147. 一种用于保护经由第一协议建立的会话免受网络中断的方法，该方法包括以下步骤：

(a) 经由客户端的代理建立在客户端与设备之间的网络连接上经由第一协议的会话的步骤，网络连接与网络堆栈相关联，网络堆栈的第一部分包括在第一协议的层下面的网络堆栈的一个或多个层，b 并且网络堆栈的第二部分包括用于第一协议的层和在第一协议上面的网络堆栈的一个或多个层；

(b) 检测造成网络堆栈的第一部分被解除的、在网络连接中的中断；

(c) 在中断期间由代理保持会话和网络堆栈的第二部分；以及

(d) 重新建立网络堆栈的第二部分和网络连接，同时保持会话和网络堆栈的第二部分。

148. 权利要求147的方法，还包括以下步骤：

(e) 用网络堆栈的保持的第二部分和网络堆栈的重新建立的第一部分继续进行会话。

149. 权利要求147的方法，还包括以下步骤：

(e) 由网络堆栈的第二部分丢弃在中断期间接收的任何网络分组。

150. 权利要求147的方法，其中设备包括远程接入网关或计算设备之一。

151. 权利要求147的方法，还包括经由以下的协议之一的第一协议建立会话：安全套接字层 (SSL) 协议、传输层安全 (TLS) 协议、和隧道协议。

152. 权利要求147的方法，包括由代理经由在客户端与设备之间的会话传送实时数据。

153. 权利要求152的方法，其中实时数据包括实时协议。

154. 权利要求152的方法，其中实时数据包括话音或音频之一的表示。

155. 权利要求147的方法，包括代理在客户端的操作系统的用户模式下操作。

156. 权利要求147的方法，其中网络的第一部分包括传输控制协议或互联网协议之一。

157. 权利要求147的方法，其中网络堆栈的第二部分包括互联网协议、用户数据报协议、或通过互联网的话音协议之一。

158. 权利要求147的方法，包括客户端经由远程显示协议与设备通信。

159. 权利要求158的方法，其中远程显示协议包括独立计算结构协议或远程桌面协议之一。

160. 权利要求147的方法，包括对于经由网络连接通信的客户端的应用透明地执行步骤(b)、(c)和(d)之一。

161. 权利要求147的方法，包括由代理对于客户端的应用透明地截取与应用关联的一个或多个网络分组。

162. 权利要求147的方法，包括由与堆栈的第二部分关联的网络驱动器对于客户端上的应用透明地截取与应用关联的一个或多个网络分组。

163. 一种用于保护经由第一协议建立的会话免受网络中断的系统，该系统包括：

客户端的代理，经由第一协议通过网络连接建立在客户端与设备之间的会话；

网络堆栈，具有第一部分和第二部分，网络堆栈的第一部分包括在第一协议的层下面的网络堆栈的一个或多个层，并且网络堆栈的第二部分包括用于第一协议的层和在第一协议上面的网络堆栈的一个或多个层；以及

检测器，用于检测造成网络堆栈的第一部分被解除的、在网络连接中的中断；

其中：

在由检测器检测中断时，代理在中断期间保持会话和网络堆栈的

## 第二部分；

客户端重新建立网络堆栈的第一部分和网络连接，同时代理保持会话和网络堆栈的第二部分。

164. 权利要求163的系统，其中代理用网络堆栈的保持的第二部分和网络堆栈的重建的第一部分继续进行会话。

165. 权利要求163的系统，其中网络堆栈的第一或第二部分之一丢弃在中断期间接收的任何网络分组。

166. 权利要求163的系统，其中设备包括远程接入网关或计算设备之一。

167. 权利要求163的系统，其中第一协议包括以下的协议之一：安全套接字层（SSL）协议、传输层安全（TLS）协议、和隧道协议。

168. 权利要求163的系统，其中代理经由在客户端与设备之间的会话传送实时数据。

169. 权利要求168的系统，其中实时数据包括实时协议之一。

170. 权利要求168的系统，其中实时数据包括语音或音频之一的表示。

171. 权利要求163的系统，其中代理在客户端的操作系统的用户模式下操作。

172. 权利要求163的系统，其中网络堆栈的第一部分包括传输控制协议或互联网协议之一。

173. 权利要求163的系统，其中网络堆栈的第二部分包括互联网协议、用户数据报协议、或通过互联网的话音协议之一。

174. 权利要求163的系统，其中第一协议包括远程显示协议。

175. 权利要求174的系统，其中远程显示协议包括独立计算结构协议或远程桌面协议之一。

176. 权利要求163的系统，其中代理对于客户端的应用透明地截取与该应用关联的一个或多个网络分组。

177. 权利要求163的系统，包括与网络堆栈的第二部分关联的网络驱动器，网络驱动器对于客户端的应用透明地截取与该应用关联的一个或多个网络分组，并经由会话把该一个或多个分组提供给代理。

178. 权利要求177的系统，其中网络驱动器包括网络驱动器接口

技术规范（NDIS）驱动器。

179. 权利要求177的系统，其中网络驱动器在客户端的操作系统的内核模式下操作。

---

## 用于网络节点之间通信最优化的系统和方法

### 相关专利申请

本专利申请要求 2004 年 6 月 23 日提交的、题目为“Ad Hoc Distributed Network and Remote Access Architecture”的美国临时专利申请号 60/590,837、2004 年 8 月 13 日提交的、题目为“System and Method For Assuring Redundancy in Remote Access Solution”的美国临时专利申请号 60/601,431、2004 年 9 月 3 日提交的、题目为“Virtual Network Bridging”的美国临时专利申请号 60/607,420、和 2004 年 9 月 10 日提交的、题目为“System and Method For Assuring Redundancy in Remote Access Solution”的美国临时专利申请号 60/608,814 的优先权，这些专利申请在此引用以供参考。

### 技术领域

本发明总的涉及最优化网络的节点之间的网络通信。

### 背景信息

虚拟专用网络（VPN）是利用诸如互联网那样的公共电信基础结构，以便通过使用隧道和安全机构而保持专用性的专用数据网。这样，VPN 提供数据加密和为通过公共网的共同的数据提供安全性。除了解决经由公共网安全接入共同的数据以外，VPN 还针对从两个断开连接的、或不能路由的网络路由网络业务。例如，具有在 10.0.0.0-10.255.255.255 的范围的专用互联网协议地址的第一专用网经由 VPN 与具有在 192.168.0.0-192.168.255.255 的范围的专用互联网协议地址的第二专用网通信。VPN 允许在第一专用网上的远程机通过隧道传送来自远程机的网络业务和使得网络业务出现在第二专用网上而与在第二专用网上的内部机通信。这对于客户端-服务器协议是可以行得通，其中远程计算机与位于远程网络的企业服务器进行协商。

然而，传统的 VPN 在其中两个远程计算机诸如在对等协议下经由

VPN 网关隧道传送互相直接通信的情形下不能很好地工作。VPN 通过平整不接连的专用网地址空间而达到这种对等计算，在所述地址空间中由两个远程计算机经由 VPN 网关隧道传送所有的对等通信的。结果，来自一方的网络业务流到网关，并切换内部网上的隧道，通过互联网流回到对等计算机。在对等计算机之间的网络业务可以行进或长或短的最佳路由，即使对等计算机可以在它们之间具有较短的直接路径。允许远程计算机从由 VPN 提供的安全性获益而不引起较长的数据路径的缺点是有用的。

在两个计算机之间通过网络的直接通信存在其它低效性。例如，网络连接容易断开。例如，在客户端与服务器之间的无线连接常常是不可靠的。另外，网络连接是间歇的。当人们进入电梯或隧道时，连接会丢失，并且仅仅在人们从电梯或隧道中出来后连接才恢复。在另一个例子中，当移动计算设备诸如在无线网络拓扑中从网络接入点移动到另一个网络接入点时，连接会中断。

如果在客户端与服务器计算机之间的建立的连接会话异常地终结，则客户端通常必须通过启动新的通信会话重新建立连接。为了开始新的通信会话，用户典型地必须重新发送鉴权证书，诸如登录/密码对，到服务器计算机，这样，服务器计算机可以授权用户新的通信会话。这种通过多个通信会话的用户的鉴权证书的重发使得该用户的鉴权证书重复地暴露给潜在的攻击者，由此降低鉴权证书的安全水平。另外，这常常是缓慢的过程，也导致用户受挫和低效率。而且，在建立新的通信会话时，网络可能需要客户端得到新的网络标识符，诸如互联网协议地址。因为客户端标识符的改变，客户端的应用或程序可能需要重新启动。因此，希望保护计算设备免受网络中断。

与对等计算设备之间的直接通信关联的另一个低效率在于，用于通信的协议可能不是如想要的那样有效或安全。举例来说，网络通信可包括诸如通过 IP 的话音 (VoIP) 通信那样的实时数据通信。实时数据通信可以经由诸如用户数据报协议那样的不可靠的协议被传送，以便减小电话呼叫的等待时间。然而，VoIP 通信可能经过 TCP/IP 网络或安全 SSL 网关，它提供可靠的协议给 VoIP 通信。这会增加不可靠的协议打算减小的电话呼叫的等待时间。需要经由打算用于通

---

过使用有损协议的通信的无损协议来传输数据的技术。

直接通信中的另一个低效率是由于使用加密而造成的。诸如 SSL 的加密可用来提供安全网络通信。虽然通信是安全的，但网络业务的加密增加了网络分组的尺寸，这会导致对于单个分组，分组有效负载变为太大。这会导致分组分段，造成用于通信处理的更多的开销。用于解决加密开销而调节分组的最大值的技术是有用的。

另一个低效率是由于以下事实造成的：客户端典型地在用户的活动和客户端的应用生成网络通信时发送网络通信，并在网络通信被接收时，处理进入的网络通信。例如，在一种情形下，虽然应用在前台运行，并且当前正在由用户使用，但对于在后台运行的应用生成或接收的网络分组可能在对于前台运行的应用生成或接收的网络分组之前被处理。在另一个例子中，客户端可能正在运行 VoIP 应用，以提供电话呼接到远程计算设备。与 VoIP 的实时数据通信无关的客户端的一个或多个应用可能正在运行。用于这些应用的网络分组可能在 VoIP 电话的实时网络分组之前被处理，由此增加等待时间和减小语音应用的质量。所以希望提供对分组业务的应用知道的、客户端特定的优先化。

## 发明内容

本发明总的针对用于提供对等通信和远程接入连接性的远程接入结构。在一个实施例中，本发明的远程接入结构提供用于经由诸如网关的第三计算设备建立对等计算设备之间的直接通信的方法。另外，本发明提供用于对等通信最优化的各种技术，包括实时通信，诸如通过互联网协议的话音(VoIP)信令，以及媒体、视频、和其它实时数据应用，诸如 web 合作、屏幕或桌面共享、和即时消息。本发明提供以下的对等最优化技术：1) 网络分组的接收的虚假确认允许经由无损分组协议传送对于经由有损协议传输被构建的分组，2) 网络分组的有效负载移位允许经由无损分组协议传送对于经由有损协议传输被构建的分组，3) 考虑由于加密造成的开销，通过调节最大传输单元(MTU)参数而减小分组分段，4) 客户端侧网络通信的应用知道的优先化，以及 5) 网络中断保护，用于可靠的和持久的网络连接性与接入，诸如用于移动计算。

一方面，本发明涉及用于建立在第一网络上的第一计算设备与第二网络上的第二计算设备之间的对等通信会话的方法。第一网络可以是与第二网络不连接的，并且不能路由到第二网络。该方法包括由第一计算设备建立与第三计算设备的第一隧道会话，和由第二计算设备建立与第三计算设备的第二隧道会话。第三计算设备可以是网关，诸如 SSL VPN 网关。第一计算设备经由第三计算设备，诸如经由信令协议发起到第二计算设备的通信会话。服务器接收一个信号，用来建立发起的通信会话，并且服务器把第一网络地址传送到第一网络的第一计算设备，第一网络地址包括与第二隧道会话关联的第二计算设备。第一计算设备通过使用第一网络地址传送发起与第二计算设备的连接的请求。方法还包括通过第三计算设备截取请求，并为第一计算设备提供用于第二计算设备的第二网络地址。第二网络地址识别与第二计算设备关联的公共网地址。第三计算设备通过使用第二网络地址，诸如经由横穿防火墙的浮筒会话（swimmer session）把请求传送到第二计算设备，以允许来自第一计算设备的连接。

在本发明的一个实施例中，通过使用安全套接字层或虚拟专用网络建立第一隧道会话或第二隧道会话。第三计算设备可以是远程接入网关。在另一个实施例中，第二计算设备位于与第二网络地址关联的防火墙的后面。

在另一个实施例中，本发明的方法包括通过把带外信号经由第一隧道会话传送到第一计算设备而由第三计算设备把第二网络地址提供给第一计算设备。在附加实施例中，该方法包括由第二计算设备为第一计算设备提供在防火墙中的转发口，以便使用第二网络地址与第二计算设备通信。

在本发明的再一个实施例中，第三计算设备把密钥传送到第一计算设备和第二计算设备。第一计算设备和第二计算设备可以交换密钥。另外，第一和第二计算设备可以在发送数据到其它计算设备之前检验从其它计算设备接收的密钥是否匹配。

在本发明的一些实施例中，该方法把第一电信设备与第一计算设备相关联，和把第二电信设备与第二计算设备相关联。第一电信设备或第二电信设备可包括软件部件或硬件部件，诸如硬或软 VoIP 电

话。在一个实施例中，本发明的方法包括经由在第一和第二计算设备之间的连接建立在第一电信设备与第二电信设备之间的电信会话。第一电信设备和第二电信设备可以通过电信会话通信而不用经过第三计算设备。

在本发明的另一个实施例中，该方法经由在第一计算设备和第二计算设备之间的连接传送远程显示协议。远程桌面协议可包括独立计算结构协议或远程桌面协议。在再一个实施例中，该方法可包括经由连接与第二计算设备共享第一计算设备的屏幕视图或屏幕数据。

一方面，本发明涉及在网关中执行的、用于建立在第一网络上的第一计算设备与第二网络上的第二计算设备之间的对等通信会话的方法。第一网络可以是与第二网络不连接的，并且不能路由到第二网络。该方法包括建立与第一网络上的第一计算设备的第一隧道会话，和建立与第二网络上的第二计算设备的第二隧道会话。网关接收由第一计算设备发起与第二计算设备的通信会话的请求。第一计算设备提供用于联系第二计算设备的第一网络地址。第一网络地址识别与第二隧道会话关联的、第二计算设备的网络地址。网关接收由第一计算设备发起通过使用第一网络地址与第二计算设备连接的请求，截取发起连接的请求，并为第一计算设备提供用于第二计算设备的第二网络地址。第二网络地址识别与第二计算设备关联的公共网地址。网关通过使用第二网络地址，诸如经由横穿防火墙的浮筒会话把允许从第一计算设备到第二计算设备的连接的请求传送到第二计算设备。

在一个实施例中，经由网关的第一隧道会话或第二隧道会话包括安全套接字层或虚拟专用网络。在另一个实施例中，第二计算设备位于与第二网络地址关联的防火墙的后面。在再一个实施例中，本发明的方法通过把带外信号经由第一隧道会话传送到第一计算设备而把第二网络地址提供给第一计算设备。另外，网关可以把密钥传送到第一计算设备和第二计算设备。

另一方面，本发明涉及用于经由第三计算设备建立在第一网络上的第一计算设备与第二网络上的第二计算设备之间的对等通信会话的系统。第一网络可以是与第二网络不连接的，并且不能路由到第

二网络。该系统包括在第一网络上的第一计算设备与第二网络上的第二计算设备。第三计算设备建立与第一计算设备的第一隧道会话，和与第二计算设备的第二隧道会话。系统还包括经由第三计算设备可接入的服务器。在系统操作中，服务器经由第三计算设备把第一网络地址传送到第一计算设备，该第一网络地址识别与第二隧道会话关联的第二计算设备的网络地址。第一计算设备通过使用第一网络地址经由第三计算设备传送发起与第二计算设备的连接的请求。第三计算设备截取第一请求，并为第一计算设备提供用于第二计算设备的第二网络地址。第二网络地址识别与第二计算设备关联的公共网地址。第三计算设备通过使用第二网络地址传送第二请求到第二计算设备，以允许来自第一计算设备的连接。

在该系统的一个实施例中，第一隧道会话或第二隧道会话包括安全套接字层或虚拟专用网络。而且，第三计算设备可以是远程接入网关，诸如 SSL VPN 网关。在系统的另一个实施例中，第二计算设备位于与第二网络地址关联的防火墙的后面。

在本发明的另外的实施例中，第三计算设备通过经由第一隧道会话，诸如经由带外 TLS 会话，传送带外信号而把第二网络地址提供给第一计算设备。在一个实施例中，由第二计算设备为第一计算设备提供在防火墙中的转发口，以便使用第二网络地址与第二计算设备通信。

在本发明的再一个实施例中，第三计算设备把密钥传送到第一计算设备和第二计算设备。第一计算设备和第二计算设备可以交换密钥。另外，第一和第二计算设备可以在发送数据之前检验从其它计算设备接收的密钥是否匹配。

在本发明的一些实施例中，系统包括与第一计算设备关联的第一电信设备，和与第二计算设备关联的第二电信设备。第一电信设备或第二电信设备可包括软件部件或硬件部件，诸如硬或软 VoIP 电话。在一个实施例中，本发明的系统包括经由在第一和第二计算设备之间的连接建立在第一电信设备与第二电信设备之间的电信会话。第一电信设备和第二电信设备可以通过电信会话通信而不用经过第三计算设备。

在本发明的另一个实施例中，第一计算设备和第二计算设备经由

连接传送远程显示协议。远程桌面协议可包括独立计算结构协议或远程桌面协议。在再一个实施例中，第一计算设备可以经由连接与第二计算设备共享屏幕视图或屏幕数据。

另一方面，本发明涉及经由无损协议传送对于经由有损协议传输被构建的分组的方法。该方法可以在一个或多个电子设备，诸如在系统中，并通过任何适当的装置和机构被执行。该方法包括经由无损协议建立在第一计算设备与第二计算设备之间的连接。在一些实施例中，第二计算设备可以是网关，诸如 SSL VPN 网关。第一计算设备检测无损协议分组，无损协议分组包括具有按照有损协议被构建的一个或多个分组的有效负载。第一计算设备把无损协议分组的接收的虚假确认传送到第一计算设备和/或第二计算设备。无损协议分组的接收的虚假确认阻止利用用于无损协议的可靠性算法和机构。第一计算设备把无损协议分组传送到第二计算设备。在一些实施例中，无损协议分组的接收的虚假确认在传送无损协议分组之前被传送。

在一个实施例中，本发明的方法包括由第一计算设备使用密钥来加密一个或多个分组。在一些实施例中，加密密钥可以经由在第一计算设备与第二计算设备之间的带外传输安全层会话被提供给第一计算设备。在另一个实施例中，方法逐个分组地加密一个或多个分组。

在本发明的方法的另一个实施例中，响应于由第一计算设备和/或第二计算设备接收到无损协议分组的接收的虚假确认，第一计算设备和/或第二计算设备阻止执行与提供无损协议的无损特性关联的操作。在一个实施例中，无损协议是传输控制协议。

在再一个实施例中，本发明的方法阻止第一计算设备和/或第二计算设备的网络堆栈执行与无损协议有关的一个或多个以下的算法：1) 重发，2) 排序，3) 流控制算法，4) nagle 算法，和 5) 滑动窗口算法。

在一个实施例中，有损协议包括用户数据报协议。在另一个实施例中，该方法包括由第一计算设备经由安全套接字层或传输安全层隧道把无损协议分组传送到第二计算设备。

在另一个实施例中，有效负载的一个或多个分组包括实时协议。

在附加实施例中，该方法包括由第一计算设备把实时话音、音频或数据之一经由一个或多个分组传送到第二计算设备。

一方面，本发明涉及通过使用在 TCP 连接上不可靠的传输协议发送来自应用的分组的方法。该方法包括在第一设备接收要使用不可靠的传输协议发送的第一分组，和创建第一 TCP 分组，该第一 TCP 分组包括接收的第一分组的第一有效负载和与在第一设备与第二设备之间建立的 TCP 连接关联的信息的第一 TCP 首部。第一设备把第一 TCP 分组发送到第二设备。该方法还包括在第一设备处接收要使用不可靠的传输协议发送的第二分组，和创建第二 TCP 分组，该第二 TCP 分组包括接收的第二分组的第二有效负载和第一 TCP 首部信息。在接收来自第二设备的第一有效负载的接收的确认之前，第一设备把第二 TCP 分组发送到第二设备。

在一个实施例中，本发明的方法建立与一个端口号的 TCP 连接，该端口号与不可靠的传输协议相关联。在另一个实施例中，该方法包括由第一设备动态地确定包括不可靠的传输协议的第一 TCP 分组与第二 TCP 分组。在一些实施例中，不可靠的传输协议是 UDP。

在另外的实施例中，该方法包括在第一设备上通过使用分组捕获机构截取第一 TCP 分组与第二 TCP 分组来接收第一 TCP 分组与第二 TCP 分组。在一些实施例中，该方法包括由第一设备建立与 VPN 网关设备的 TCP 连接。在其它的实施例中，该方法包括经由 TCP 连接建立在第一设备与第二设备之间的对等通信。在本发明的另一个实施例中，该方法包括由第一设备加密第一与第二 TCP 分组，和由第二设备解密该加密的第一与第二 TCP 分组。

另一方面，本发明涉及通过使用在 TCP 连接上的不可靠的传输协议发送来自应用的分组的方法。该方法包括在第二设备处截取在第一设备处创建的和在第二设备处接收的第一 TCP 分组。第一 TCP 分组包括由应用通过使用不可靠的传输协议生成的第一分组的第一有效负载和与在第一设备与第二设备之间建立的 TCP 连接关联的信息的第一 TCP 首部。该方法的截取在第一 TCP 分组被提供给第二设备的 TCP 堆栈之前发生。该方法包括响应于信息的 TCP 首部来识别第一有效负载是由应用通过使用不可靠的传输协议而生成的分组，从第一 TCP 分组剥离信息的 TCP 首部，和通过使用不可靠的传输协议

把第一有效负载转发到应用。

在一个实施例中，不可靠的协议是 UDP。在另一个实施例中，识别的步骤包括识别 TCP 首部信息，包括与不可靠的传输协议关联的端口号。在一些实施例中，该方法包括由第二设备通过使用分组捕获驱动器来截取第一 TCP 分组。

在一些实施例中，第一设备是客户端设备并且第二设备是 VPN 网关。另外，本发明的方法包括把第一有效负载转发到应用之前在第二设备上执行网络地址转换 (NAT)。

再一方面，本发明涉及用于通过使用在 TCP 连接上的不可靠的传输协议发送来自应用的分组的系统。系统包括第一和第二设备。第一设备具有生成第一和第二分组的应用。第一和第二分组打算通过使用不可靠的传输协议被发送。第一设备还具有过滤器进程和隧道进程。过滤器进程截取来自应用的第一和第二分组，并把截取的分组转发到隧道进程。隧道进程请求打开在第一设备与第二设备之间的 TCP 连接。打开 TCP 连接的请求向第一和第二设备表示，TCP 连接将传输打算用不可靠的传输协议发送的分组。隧道进程把第一和第二分组作为在第一和第二 TCP 分组中的有效负载转发到第二设备。隧道进程在发送 TCP 分组之后和在接收对于第一 TCP 分组的确认之前发送第二 TCP 分组。

本发明的系统的第二设备与第一设备进行通信。第二设备具有第二过滤器进程和隧道进程。第二隧道进程打开由第一设备请求的 TCP 连接，并识别并把 TCP 连接的源地址转发到第二过滤器进程。第二过滤器进程截取在第二设备处用首部中的 TCP 连接源地址接收的、来自应用的分组。第二过滤器进程从接收的分组剥离 TCP 首部，把被剥离的分组转发到打算的目的地，并绕开在第二设备上的 TCP/IP 堆栈。

在本发明的系统的一个实施例中，在第一设备上的第一过滤器进程和/或在第二设备上的第二过滤器进程是分组捕获驱动器。在一些实施例中，第一设备是客户端设备并且第二设备是 VPN 网关设备。在一个实施例中，不可靠的数据协议是 UDP。

在另一个实施例中，系统还包括第三设备，剥离的分组被发送到该第三设备。另外，第二设备还可包括网络地址转换 (NAT) 表，用来

---

在把剥离的分组发送到第三设备之前执行网络地址转换。

再一方面，本发明涉及用于调节安全网络通信的最大传输单元以减小网络分段的方法。方法可以在一个或多个电子设备，诸如在系统中，并通过任何适当的装置和机构被执行。该方法包括建立在第一计算设备与第二计算设备之间的会话。会话可以由第一计算设备的代理建立。第一计算设备具有第一网络堆栈。该方法由第一计算设备检测具有加密的有效负载的网络分组，并确定对于第一网络堆栈的最大传输单元参数的设置，以将最大传输单元尺寸减小至少与有效负载的加密部分关联的一个尺寸。该方法把第一网络堆栈的最大传输单元（MTU）参数改变到所确定的设置。这样，报告的 MTU 参数被减小，以便考虑加密。

在一个实施例中，本发明的方法包括经由安全套接字层或传输层安全隧道把网络分组传送到第二计算设备。第二计算设备可以是网关，诸如 SSL VPN 网关。在另一个实施例中有效负载包括实时协议。

另外，在一个实施例中，方法还可包括经由第一网络堆栈的网络驱动器接口技术规范（NDIS）水平机构来改变最大传输单元参数。在另一个实施例中，该方法对每个在第一计算设备与第二计算设备之间的会话动态地确定最大传输单元参数的设置。在一个实施例中，第一计算设备的代理经由 IOCTL 应用编程接口与第一网络堆栈通信，以便把最大传输单元参数改变为所确定的设置。

在一些实施例中，本发明的方法经由网关建立在第一计算设备与第二计算设备之间的会话。在其它实施例中，该方法包括由第一计算设备把实时语音、音频或数据经由一个或多个网络分组的有效负载传送到第二计算设备。在再一个实施例中，该方法可包括在传送网络分组之前把网络分组的接收的虚假确认传送到第一计算设备和/或第二计算设备。在一个实施例中，网络分组包括无损协议分组，诸如传输控制协议。在另一个实施例中，有效负载包括有损协议分组，诸如用户数据报协议。

另一方面，本发明涉及对客户端优先化与客户端的应用关联的、客户端的网络通信的方法。该方法包括由客户端截取与客户端的一个或多个应用关联的一个或多个网络分组，并存储该一个或多个网络分组到一个队列。客户端确定与客户端的第一应用关联的排队的

一个或多个网络分组。客户端表示所确定的一个或多个网络分组的优先权，把确定的一个或多个网络分组放置在与客户端的第二应用关联的、队列中的至少一个网络分组之前。客户端提供优先化的一个或多个网络分组以便经由客户端的网络堆栈通信。

在一个实施例中，本发明的方法包括由客户端确定第一应用的排队的一个或多个网络分组包括实时数据。实时数据可包括以下的一项：1) 实时协议，2) 用户数据报协议，和3) 语音或音频的表示。

在另一个实施例中，该方法包括由客户端阻止第二应用的至少一个网络分组在第一应用的一个或多个网络分组之前经由网络堆栈被传送。在再一个实施例中，该方法包括由客户端把与第二应用关联的网络分组保存在队列中，并当在保存的网络分组之前优先化的、与第一应用关联的一个或多个网络分组被传送时释放保存的网络分组。

在本发明的又一个实施例中，该方法包括由客户端对于客户端上的一个或多个应用透明地截取一个或多个网络分组。在一些实施例中，第一应用在前台运行，以及第二应用在后台运行。

在本发明的一个实施例中，该方法包括把比与第二应用关联的优先权更高的优先权与第一应用相关联。在另一个实施例中，用户可以规定第一应用或第二应用的优先权。在再一个实施例中，客户端接收来自计算设备的一个或多个网络分组。另外，该一个或多应用可提供一个或多个网络分组，以便从客户端到计算设备的传送。

另一方面，本发明涉及对于与客户端的应用关联的客户端网络通信进行优先化的客户端。客户端包括用于截取与客户端的一个或多个应用关联的客户端的一个或多个网络分组的机构。客户端还包括网络驱动器，用于存储一个或多个网络分组到一个队列，并经由客户端的网络堆栈传送该一个或多个网络分组。客户端还包括代理，用于确定与客户端的第一应用关联的一个或多个网络分组，并向网络驱动器表示该一个或多个网络分组的优先权，以把所确定的一个或多个网络分组放置在与客户端的第二应用关联的、队列中的至少一个网络分组的前面。

在一个实施例中，本发明的代理确定第一应用的一个或多个网络分组，包括实时数据。实时数据包括以下的一项：1) 实时协议，2)

用户数据报协议，和 3) 语音或音频的表示。

在另一个实施例中，本发明的代理或网络驱动器阻止第二应用的至少一个网络分组在第一应用的一个或多个网络分组之前经由网络堆栈被传送。在一个实施例中，网络驱动器把与第二应用关联的网络分组保存在队列中，并当在保存的网络分组之前的、与第一应用关联的一个或多个网络分组被传送时释放所保存的网络分组。

在另一个实施例中，本发明经由机构对于客户端上的一个或多个应用透明地截取一个或多个网络分组。在一些实施例中，第一应用在前台运行，以及第二应用在后台运行。另外，第一应用可能具有比客户端的第二应用更高的优先权。而且，客户端可包括用于用户规定优先权的配置机构。在一些实施例中，客户端接收来自计算设备的一个或多个网络分组。在其它实施例中，该一个或多个应用提供一个或多个网络分组以便从客户端到计算设备的传送。

在另外的实施例中，网络驱动器包括网络驱动器接口技术规范(NDIS)驱动器。另外，网络驱动器可以在客户端的操作系统的内核模式下工作。在某些情形下，代理在客户端的操作系统的用户模式下工作。而且，网络驱动器的代理包括用于截取客户端的一个或多个网络分组的机构。

再一方面，本发明涉及用于保护经由第一协议建立的会话免受网络中断的方法。该方法包括经由客户端的代理建立在客户端与设备之间的网络连接上经由第一协议的会话的步骤。网络连接与网络堆栈相关联。网络堆栈的第一部分包括在第一协议的层下面的网络堆栈的一个或多个层，并且网络堆栈的第二部分包括用于第一协议的层和在第一协议上面的网络堆栈的一个或多个层。该方法包括检测造成网络堆栈的第二部分被解除的、在网络连接中的中断，和在中断期间由代理保持会话和网络堆栈的第二部分。该方法还包括重新建立网络堆栈的第一部分和网络连接，而同时保持会话和网络堆栈的第二部分。

在一个实施例中，该方法包括用网络堆栈的保持的第二部分和网络堆栈的重新建立的第一部分继续进行会话。在一些实施例中，该方法还包括由网络堆栈的第一和/或第二部分丢弃在中断期间接收的任何网络分组。

在另一个实施例中，设备包括远程接入网关或另一个计算设备。在某些情形下，该方法包括经由以下的协议的第一协议建立会话：1)安全套接字层(SSL)协议，2)传输层安全(TLS)协议，以及3)隧道协议。另外，本发明的方法可包括由代理经由在客户端与设备之间的会话传送实时数据。实时数据可包括实时协议，或实时数据可表示话音或音频。

在一些实施例中，代理在客户端的操作系统的用户模式下工作。在一个实施例中，网络的第一部分包括传输控制协议或互联网协议之一。在另一个实施例中，网络堆栈的第二部分包括以下的一个协议：1)互联网协议，2)用户数据报协议，或3)通过互联网的话音协议。另外，客户端可以经由远程显示协议与设备通信。远程显示协议可以是独立的计算结构(ICA)协议或远程桌面协议(RDP)。

在另一个实施例中，本发明的方法对于经由网络连接通信的客户端的应用透明地执行。在一个实施例中，该方法包括由代理对于客户端的应用透明地截取与应用关联的一个或多个网络分组。在一个实施例中，该方法包括由与堆栈的第一部分关联的网络驱动器对于客户端的应用透明地截取与应用关联的一个或多个网络分组。

另一方面，本发明涉及用于保护经由第一协议建立的会话免受网络中断的系统。系统具有客户端的代理经由第一协议通过网络连接建立在客户端与设备之间的会话。该系统包括具有第一部分和第二部分的网络堆栈，诸如客户端的网络堆栈。网络堆栈的第二部分包括用于第一协议的层和在第一协议上面的、网络堆栈的一个或多个层，以及网络堆栈的第一部分包括在第一协议的层下面的、网络堆栈的一个或多个层。该系统包括检测器，用于检测造成网络堆栈的第一部分被解除的、在网络连接中的中断。在系统操作中和在由检测器检测中断时，代理在中断期间保持会话和网络堆栈的第二部分。客户端重建网络堆栈的第一部分和网络连接，同时代理保持会话和网络堆栈的第二部分。

在本发明的系统的一个实施例中，代理用网络堆栈的保持的第二部分和网络堆栈的重建的第一部分继续进行会话。在一些实施例中，网络堆栈的第一和/或第二部分丢弃在中断期间接收的任何网络分组。

在一个实施例中，系统的设备是远程接入网关或另一个计算设备。由本发明的系统所使用的第一协议可包括以下的一个：1)安全套接字层（SSL）协议，2)传输层安全（TLS）协议，以及3)隧道协议。在另一个实施例中，本发明的代理经由在客户端与设备之间的会话传送实时数据。实时数据可包括实时协议，或语音或音频的表示。

在系统的一些实施例中，代理在客户端的操作系统的用户模式下工作。在一个系统实施例中，网络的第一部分包括传输控制协议和/或互联网协议。在另一个实施例中，网络堆栈的第二部分包括以下的一个协议：1)互联网协议，2)用户数据报协议，或3)通过互联网的话音协议。另外，客户端可以经由远程显示协议与设备通信，它可以是独立的计算结构（ICA）协议或远程桌面协议（RDP）。

在另一个实施例中，本发明的系统保持网络堆栈的第二部分和对于经由网络连接通信的客户端的应用透明地重建网络堆栈的第一部分。在一个实施例中，代理对于客户端的应用透明地截取与应用关联的一个或多个网络分组。在一个实施例中，系统还包括由与堆栈的第二部分关联的网络驱动器对于客户端的应用透明地截取与应用关联的一个或多个网络分组。

下面在附图和说明中阐述本发明的各种实施例的细节。

#### 附图说明

通过参考结合附图作出的以下的说明，本发明的上述的和其它的目的、方面、特性和优点将变得更明白和可以更好地了解，其中：

图1A是显示用于在网络环境下经由网关实施本发明的操作的实施例的框图；

图1B是显示用于在对等网络环境下实施本发明的操作的另一个实施例的框图；

图1C是显示用于网络通信的、本发明的远程接入客户端的实施例的框图；

图1D和1E是显示在实施本发明的实施例中有用的计算设备的实施例的框图；

图2A是显示用于实施用于建立对等通信路由的本发明的技术的

实施例的对等网络环境的实施例的框图；

图 2B 是显示对于使得本发明的对等路由最优化技术最优化执行的步骤的实施例的流程图；

图 3A 是显示在图 1A 到 1C 上所示的说明性实施例的任何计算设备的网络堆栈的实施例的框图；

图 3B 是显示对于使用网络分组的接收的虚假确认经由对于经由有损协议传输被构建的无损协议分组进行通信所执行的步骤的实施例的流程图；

图 3C 是显示对于经由有损协议传输被构建的无损协议分组进行通信所执行的步骤的实施例的流程图；

图 4 是显示对于调节最大传输单元参数执行的步骤的一个实施例的流程图；

图 5A 是显示用于提供客户端侧应用知道的优先化技术的客户端的环境的框图；

图 5B 是对于提供客户端侧应用知道的优先化执行的步骤的一个实施例的流程图；

图 6A 是显示用于保护来自设备的网络中断的设备的实施例的框图；以及

图 6B 是在保护来自设备的网络中断时执行的步骤的一个实施例的流程图。

### 具体实施方式

下面描述本发明的某些说明性实施例。然而，应当直接指出，本发明不限于这些实施例，而是打算把对于这里直接描述的内容的添加和修改包括在本发明的范围内。而且，可以看到，这里描述的各种实施例的特性不是互相不相容的，而是可以存在于各种组合和置换，即使这样的组合或置换在这里没有直接作出，而不背离本发明的精神和范围。

本发明的说明性实施例总的针对用于提供对等通信和远程接入连接性的远程接入结构。在一个说明性实施例中，本发明的远程接入结构提供用于经由第三计算设备，诸如网关，建立在各个计算设备之间的直接连接的方法。本发明还提供用于使通过或不通过网关

建立的对等通信最优化的各种技术。对等通信可包括实时通信，诸如通过互联网协议的话音(VoIP)信令和媒体、视频和其它实时数据应用，诸如 web 合作、屏幕或桌面共享、以及立即消息。除了经由网关建立对等通信以外，本发明还提供使对等通信最优化的以下技术：1) 网络分组的接收的虚假确认允许经由无损分组协议传送对于经由有损协议传输被构建的分组，2) 网络分组的有效负载移位允许经由无损分组协议传送对于经由有损协议传输被构建的分组，3) 考虑由于加密造成的开销，通过调节最大传输单元(MTU)参数而减小分组分段，4) 客户端侧网络通信的应用知道的优先化，以及5) 网络中断保护，用于可靠的和持久的网络连接与接入，诸如用于移动客户端。这些技术在一些实施例中可在两个客户端之间的对等通信中被实施，或在其它实施例中在客户端与网关之间，或在一个计算设备经由网关与另一个计算设备之间的通信中被实施，诸如经由本发明的说明性实施例的 SSL VPN 网关。

在本发明的说明性实施例中，对等路由最优化技术确定客户端可以尝试经由网关接入的、到资源的更加优化的路由。客户端和由客户端接入的资源，诸如服务器或各个计算机，可以具有比具有网关更直接的路由。例如，客户端和服务器可以互相靠近，但远离网关，因此比起网关来说互相更接近。而且，使用网关使得在客户端与服务器之间的对等网络通信中至少一个附加的跳。代替客户端与服务器通过使用它们的虚拟专用网络(VPN)指定的互联网协议(IP)网络地址经由网关进行通信，本发明的网关与远程接入结构便于客户端和服务器以对等的方式经由直接路由互相通信而不使用网关。然而，在某些情形下，客户端和服务器可能互相之间没有直接路径，因为客户端和/或服务器可能处在防火墙后面，诸如网络地址转换(NAT)防火墙。本发明的对等路由最优化技术和远程接入结构还提供客户端与服务器经由穿过防火墙直接通信的技术。这样，本发明的对等路由最优化技术，比起经由网关，提供在对等计算机之间的更短的更优化的路由。

在本发明的说明性实施例中，本发明的实施例的虚假确认技术使得对于经由有损协议发送被构建的分组能够经由无损协议被传送。例如，实时协议(RTP)可以在用户数据报协议(UDP)上实施，用

于 IP (VoIP) 通信。有损的或不可靠的协议，诸如 UDP，可用于语音通信，因为在某些实时话音应用中对于接收者更重要的是及时得到网络分组，而不是按照顺序得到网络分组或保证网络分组的传递。然而，借助于使用诸如诸如安全套接字层 (SSL) 或传输层安全性 (TLS) 那样的安全通信和/或隧道协议的虚拟专用网络和远程接入解决方案，对于经由诸如 UDP 那样的有损协议发送而被构建的实时应用可以经由诸如传输控制协议 (TCP) 的无损的或可靠的协议被传送。本发明的技术允许诸如 UDP 上的 RTP 那样的有损协议经由诸如 TCP 那样的无损协议进行通信，同时避免无损协议的一个或多个无损特性被应用到通信。在本发明的说明性实施例中，这个技术把无损协议网络分组的接收的虚假确认传送到相应的网络堆栈，以避免无损协议执行提供协议的可靠性的算法。通过使用这种技术，有损协议可以在诸如 TCP, SSL 那样的无损协议上，或经由网关的隧道协议被传送，例如使得通信安全，并使得有损协议网络分组及时到达接收者，而不是可靠地到达接收者。在一个实施例中，这个技术可用来在对等体之间或经由网关安全地传送诸如在 SSL 或 TLS 上的 VoIP 那样的实时数据通信。

本发明的说明性实施例还提供有效负载移位的另一个技术，使得对于经由有损协议发送而被构建的分组能够经由无损协议被传送。第一计算设备接收通过使用不可靠的传输协议所发送的第一分组，并创建包括所接收的第一分组的第一有效负载的第一 TCP 分组。第一 TCP 分组用具有与在第一和第二计算设备之间建立的 TCP 连接关联的信息的 TCP 首部来创建。第一 TCP 分组被传送到第二计算设备。通过使用不可靠传输协议被传送的第二分组由第一计算设备接收，第一计算设备转而创建包括接收的第二分组的有效负载的、但具有第一 TCP 分组的 TCP 首部信息的第二 TCP 分组。第二 TCP 分组在从第二设备接收对于第一 TCP 分组的接收的确认之前被发送到第二计算设备。这样，有效负载移位技术在 TCP 首部下传送多个不可靠传输协议有效负载，直至接收到对于接收的确认为止。

在本发明的说明性实施例中，最大传输单元调节技术考虑到由于有效负载的加密造成的网络分组尺寸的影响，以减小客户端的网络堆栈的最大传输单元 (MTU) 参数的报告尺寸。网络分组的有效负载

的加密增加要传送到客户端的或由客户端传送的网络分组的尺寸，并可能使得网络分组被分段。例如，服务器可以经由 SSL 网关把网络分组传送到客户端。虽然服务器发送应当满足客户端的网络堆栈可以处理的 MTU 尺寸的网络分组，但由网关提供的加密在网络分组到达客户端之前增加网络分组的尺寸。这可能使得从服务器经由网关到客户端的网络分组被分段，因为由于加密造成的增加的分组尺寸对于客户端的 MTU 尺寸可能太大。本发明的技术考虑到加密的开销调节客户端的报告的 MTU 尺寸，以便报告较小的尺寸。这个技术减小网络分段或否则避免非最优分段。

在本发明的说明性实施例中，优先化技术提供网络通信的客户端侧和应用知道的优先化。即，本发明的远程接入客户端管理和控制按客户端上的网络通信优先化。优先化是基于客户端上的应用的属性的。远程接入客户端透明地截取与在客户端上执行的应用关联的网络通信，检测与应用关联的网络通信，以及根据应用的优先权确定网络通信的优先权。例如，在客户端端的应用可以把诸如 VoIP 那样的实时数据通信传送到对等客户端，或经由网关传送。远程接入客户端可以截取网络分组，并且检测例如包含实时数据或来自 VoIP 应用的网络分组。远程接入客户端可以表示对于这个网络分组的优先权，这样，网络分组可以在非实时数据通信之前或在来自其它应用的网络通信之前被传送。这样，本发明的优先化技术可以根据在客户端端运行的应用来改进或提高在客户端端的性能、工作特性、和用户的体验。

在本发明的说明性实施例中，网络中断保护技术提供客户端到网络的持久的和可靠的连接，诸如对等通信会话或到网关的连接。例如，移动客户端，诸如具有基于软件的 IP 电话的笔记本电脑，可以连接到网络，用于 VoIP 通信。当移动客户端在同一个网络中不同的接入点之间漫游时或当客户端在网络之间交换（例如从有线网到无线网）时在网络连接中可能发生临时中断。这使到客户端的网络服务中断并可能丢弃 VoIP 电话呼叫。另外，当移动客户端在接入点之间移动时，移动客户端可以得到不同的 IP 网络地址，诸如来自新的动态主配置协议 (DHCP) 租用。这也会使得网络连接和 VoIP 电话通信中断。本发明的技术检测网络的中断，并保护一部分网络堆栈免受

网络中断的影响。网络堆栈的保护的部分被保持，而同时网络堆栈的其它部分被重建和重新连接到网络。一旦网络可用，本发明就继续客户端的网络通信。在一些实施例中，在网络中断期间网络通信被排队，并且一旦网络可用，就被发送。在其它实施例中，诸如对于实时数据通信，网络分组在中断期间被丢弃，避免网络分组排队可能造成诸如 VoIP 电话呼叫那样的实时通信的等待时间。

虽然本发明的说明性实施例总是结合基于互联网协议 (IP) 的协议，诸如传输控制协议 (TCP) 或用户数据报协议 (UDP) 来描述的，但本发明的技术可用于具有其它联网协议的任何其它类型的联网环境，诸如使用顺序分组交换 (SPX) 协议的、基于任何网间分组交换 (IPX) 协议的网络。另外，虽然诸如 UDP 那样的有损或不可靠协议或诸如 TCP 那样的无损或可靠的协议可用来说明本发明的实施例，但本领域技术人员已知的、任何无损/可靠的和有损/不可靠的协议可用来实施这里描述的本发明的操作。而且，虽然本发明的某些说明性实施例可以在下面相对于诸如 VoIP 那样的实时数据通信被描述，但本发明的技术可被应用于非实时数据通信，正如本领域技术人员也将认识和看到的。

另外，有时，本发明的说明性实施例可以对于对等通信被描述。一方面，对等模型包括其中任何计算机可以通过给其它计算机提供接入到它的资源而用作为服务器和可以通过接入来自其它计算机的共享的资源而用作为客户端的那种网络。另一方面，虽然对等模型可能不包括客户端和服务器的概念，但客户端和服务器可以提供对等通信以及客户端到客户端、服务器到服务器、或客户端/服务器到诸如网关的计算设备。再一方面，对等通信包括一个处理过程，由此计算机可以互相之间直接交换信息，而不用第三方网络或诸如网关的设备的帮助。虽然对等通信通常可被描述为在计算机之间的直接通信，但在计算设备之间可以有其它网络单元，诸如，例如网络集线器，以便于实行传输和/或通信。

而且，虽然本发明的说明性实施例可以是对于对等、点对点、客户端对服务器通信等等描述的，但本领域技术人员将会有认识和看到，本发明可以以任何方式经由任何网络拓扑在计算设备之间被实施，以及对于对等、客户端服务器等等的任何参考无论如何不打算

限制本发明。

一方面，本发明涉及具有远程接入客户端的远程接入结构，用于经由网关或对等使网络与另一个远程接入客户端或另一个计算设备通信。本发明的远程接入结构提供用于把在网关后面在专用网之间传送的网络业务安全地传送到诸如公网的外部网络上的客户端的系统和方法。本发明的远程接入结构通过在网关上提供网络地址转换(NAT)功能而使得客户端能够与专用网分开。使用网络地址转换(NAT)的网关提供客户端的IP地址的伪装(masquerading)，以便保护专用网不被客户端直接第2层接入。

现在参照图1A，环境180描绘在本发明的说明性实施例中用于部署远程接入结构的系统。概略地，环境180包括多个计算设备102a-102c(这里也称为客户端105a-105c)，经由一个或多个网络连接341a-341n连接到网络104。一个或多个客户端105a-105c可以经由网关350连接到服务器102a、服务器场102e、或各个计算设备102d。

每个客户端105a-105n包括远程接入客户端120a-120c，这将结合图1C更详细地描述，和一个或多个应用338a-338n。每个客户端105a-105n在网络104上通过使用任何类型和/或形式的适当隧道或网关协议经由隧道或网关连接341a-341n与网关340通信。在一些实施例中，网关连接341a-341n可用于安全地通信，诸如经由打包和加密，或否则可以使用任何其它协议，诸如任何实时、无损、或有损协议。在其它实施例中，网关340提供在一个或多个客户端105a-105n与任何的计算设备102d-102n之间的虚拟专用网络连接。

客户端105可以是任何类型和/或形式的计算设备102，它可以运行接入诸如网络104那样的网络的一个或多个应用38。应用338可以是任何类型和/或形式的应用，诸如任何类型和/或形式的web浏览器、基于web的客户端、客户端服务器应用、瘦客户端计算的客户端、ActiveX控制、或Java小应用程序、或任何类型和/或形式的能够在客户端105处执行的或经由网络104传送的可执行指令。应用338可以使用任何类型的协议，并且它可以是例如HTTP客户端、FTP客户端、Oscar客户端、或Telnet客户端。在一些实施例中，应用338使用远程显示或呈现级别协议。在一个实施例中，应

用 338 是由 Fort Lauderdale, Florida 的 Citrix Systems, Inc. 公司开发的 ICA 客户端。在其它的实施例中，应用 338 包括由 Redmond, Washington 的微软公司开发的远程桌面 (RDP) 客户端。在其它实施例中，应用 338 包括与诸如软 IP 电话那样的 VoIP 通信关联的任何类型的软件。在另外的实施例中，应用 338 包括诸如用于流视频和/或音频的应用那样的、与实时数据通信关联的任何应用。

客户端 105a-105n 可以接入经由可以在同一个网络 104 上的或可以在诸如专用网的分离网络上的通信设备 102 提供的任何资源。在一些实施例中，计算设备 102a-102n 可以是在断开连接的网络上，并且是不能从客户端 105a-105n 的网络路由的。在一个实施例中，任何客户端 105a-105n 可以与具有远程接入客户端 102n 和应用 338d 的各个计算设备 102d 通信。例如，应用 338d 可包括对应于在客户端 105a-105n 处的任何应用 338a-338c 的一部分客户端/服务器或分布式应用。在一些实施例中，任何远程接入客户端 120a-120n 可以经由网关 340 与远程接入客户端 120n 通信。

在另一个实施例中，任何客户端 105a 可以经由网关 340 与运行应用 338e 的服务器 102e 通信，例如，该服务器可以是提供诸如由 Redmond, Washington 的微软公司制造的微软交换机的电子邮件的应用服务器、web 或互联网服务器、或桌面共享服务器、或合作服务器。在一些实施例中，任何应用 338e 可包括任何类型的主机服务，诸如由 Fort Lauderdale, Florida 的 Citrix Systems, Inc. 公司提供的 GoToMeeting.com，由 Santa Clara, California 的 WebEx, Inc. 公司提供的 WebEx.com，或由 Redmond, Washington 的微软公司提供的 LiveMeeting.com。

在另一个实施例中，任何客户端 105a 可以经由网关 340 与服务器场 102n 或服务器网络通信，服务器场 102n 或服务器网络是作为单个实体被管理的一个或多个服务器的逻辑组。服务器场 102n 可以运行一个或多个应用 338N，诸如提供瘦客户端计算或远程显示呈现应用的应用 338f。在一个实施例中，服务器 102e 或服务器场 102n 执行 Citrix Systems, Inc. 的 Citrix Access Suite<sup>TM</sup>，诸如 MetaFrame 或 Citrix Presentation Server<sup>TM</sup>，和/或由微软公司制造的微软视窗终端服务的任何部分作为应用 338c-338n。

仍旧参照图 1A，网关 340 可包括任何类型和/或形式的网关，诸如远程接入服务器，它可用来把一个网络上的一个或多个计算设备连接到其它网络。另一方面，网关 340 可用来提供虚拟专用网络连接，使得客户端 105a-105c 接入到专用网。再一方面，网关 340 可以是在两个不同的协议或者分开或断开的网络或系统之间进行转换的硬件或软件装置。网关 340 可包括专门化的硬件或联网设备，或可以是被配置成用作为网关的计算设备。这样，网关 340 可包括软件、硬件、或软件和硬件的任何组合。在一个实施例中，客户端 105 和网关 340 经由任何类型和/或形式的网关或隧道协议 341a-341n，诸如 SSL 或 TLS，或由 Fort Lauderdale, Florida 的 Citrix Systems, Inc. 公司制造的 Citrix Gateway Protocol。

在一些实施例中，网关 340 可以解密从客户端 105a-105c 接收的加密的分组，并可以加密要传送到客户端 105a-105n 的分组。网关 340 可用来保护诸如网络 104 那样的专用网。在一些实施例中，网关 340 把客户端 105a-105c 与专用 IP 地址或专用网的 IP 地址相关联。在这些实施例的一个实施例中，当网关 340 从客户端 105a-105c 接收分组时，网关 340 把分组的 IP 地址转换成与用于专用网的、与客户端 105a-105c 关联的 IP 地址。在一些实施例中，网关 340 可以把接入控制策略应用于到和/或来自客户端 105a-105c 的网络业务。例如，接入控制策略可以在把分组路由到最后的目的地之前被应用于从客户端接收的分组。

在网关 340 的一个实施例中，一旦帧经由 SSL 隧道进入网关 340，分组和它的有效负载就经由回叫被分派到在用户模式下执行的操控器，其提供 SSL 解密的功能。在另一个实施例中，使用硬件加速器。在其它实施例中，使用硬件减速器。在再一个实施例中，网关 340 包括一个或多个刀形开关，用于提供远程接入。一旦分组被解密，就把它注入到 HTTP 网络堆栈，在其中首部被组装和被传送到远程接入刀形开关。在远程接入刀形开关中，分组由包含在分组内的数据类型被分类。在一个实施例中，分组包含请求登录和登记的 HTTP 首部。在另一个实施例中，分组寻求 TCP/UDP/R raw/OTHER 连接建立。在又一个实施例中，分组包含连接特定的数据。在再一个实施例中，分组包含专门的特性请求，诸如与其它用户合作、获取用

户目录和存在、或请求电话功能，诸如会议和 web 播放。远程接入模块把分组适当地分派到对应的子操控器。例如，客户端 105 可以请求，在网关 340 后面的专用网上建立到特定的机器的连接。远程接入模块可以咨询接入控制模块，如果返回肯定的确认，则远程接入模块可以准许请求。在一些实施例中，远程接入模块 120 可以通过使用利用 NAT/PAT 的帧转发模块在专用网上注入随后的帧来准许把进入的帧与对应于客户端 105a-105c 的 SSL 隧道 341a-341n 进行相关的请求。

如图 1A 所示的网络 104 可以是任何类型的网络。网络 104 可以是诸如公司内部网那样的局域网 (LAN)、城域网 (MAN)、或诸如互联网或万联网那样的广域网 (WAN)。网络 104 的拓扑可以是总线、星形或环形网络拓扑。网络 104 和网络拓扑可以是能够支持这里描述的本发明的操作的任何这样的网络或网络拓扑。客户端 108 和网关 340 可以通过包括标准电话线、LAN、或 WAN 链路 (例如，T1, T3, 56kb, X.25, SNA, DECNET)、宽带连接 (ISDN, 帧中继, ATM, Gigabit 以太网, 通过 SONET 的以太网)、和无线连接或它们的组合的各种各样的连接，连接到一个或多个网络 104。连接可以通过使用各种各样的通信协议 (例如，TCP/IP, SPX, NetBIOS, 以太网, ARCNET, 光纤分布式数据接口 (FDDI), RS232, IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, 和直接异步连接) 被建立。

在本发明的一个实施例中，图 1A 所示的网关 340 用来实行在计算设备 102a-102n 之间的对等连接。例如，客户端 105a 可以建立与网关 340 的隧道会话，以便接入各个计算设备 102d。网关 340 与客户端 105a 的远程接入客户端 120a 和计算设备 102d 的远程接入客户端 120a 协商，使得客户端 105a 能够直接连接到计算设备 102d，而不用经过网关 340。一旦在客户端 105a 与计算设备 102d 之间的网络连接被建立，客户端 105a 就可以以对等方式与计算设备 102d 通信。本发明的网关 340 可以实行在环境 180 所示的、任何计算设备 102a-102n 之间的直接对等通信。在一个实施例中，网关 340 可以实行在任何的客户端 105a-105n 之间，例如在客户端 105a 与客户端 105b 之间或在客户端 105b 与客户端 105c 之间的对等通信。在另一个实施例中，网关 340 实行在计算设备 102a-102n 之间，例如在计

算设备 102d 与服务器 102e 或服务器场 102n 之间的对等通信。在其它实施例中，网关 340 实行在客户端 105a-105n 之一与计算设备 102a-102n 之一之间的对等通信。经由网关 340 实行对等通信的技术将在下面结合图 2A 和 2B 更详细地讨论。

现在参照图 1B，本发明的远程接入客户端 120 可以在不用网关 304 的对等连接的说明性实施例中被使用。例如，网关 340 可以实行在图 1 所示的、任何计算设备 102a-102n 之间的对等连接，此后，计算设备 102a-102n 以对等方式互相直接通信。在其它实施例中，任何计算设备 102a 可以不用实行连接的网关 340 经由网络 104 直接与另一个计算设备 102b 或 102c 通信。

在图 1B 的概略图上，远程接入客户端 120a 可被部署在运行一个或多个应用 338a 的客户端 102a 上。计算设备 102a 可以通过网络 104 连接到计算设备 102b 和/或计算设备 102c。计算设备 102b 可以是也包括远程接入客户端 120b 的各个或客户端计算设备。在一些实施例中，远程接入客户端 120a 和 120b 可以经由网络 104 互相通信，和可以对于应用 338a 互相结合地工作以便与应用 338b，诸如用于基于 web 的或客户端/服务器应用进行通信。在其它实施例中，远程接入客户端 120a 可以与计算设备 102c 通信，该计算设备可以是不执行远程接入客户端 120 的服务器。

图 1C 描绘了显示具有用于把网络分组从客户端 105 路由到网络 104 的远程接入客户端 120 的系统的框图。在概略图上，系统包括具有操作系统的计算设备 102（这里称为客户端 105），操作系统包括用户模式 332，也被称为应用或用户空间，和内核模式 334，也被称为内核或系统级空间。客户端 105 运行一个代理 326，在一个实施例中，它可以在用户模式 332 下运行。客户端 105 还运行滤波器 322，在一个实施例中，它可以在内核模式或内核空间 334 下运行。在一个实施例中，滤波器 322 和代理 326 形成远程接入客户端 120，用于经由网络路由分组，或用于按照这里描述的本发明的操作提供远程接入连接性。远程接入客户端 120 或它的任何部分，诸如代理 326 或滤波器 322，可以在用户模式 332 或内核模式 334 下运行。

客户端 105 还可以具有网络堆栈 310，它可包括一个或多个网络层，诸如开放系统互联（OSI）通信模型的任何网络层，正如本领域

技术人员认识和理解的。网络堆栈 310 可包括一个或多个协议，诸如在以太网上的 TCP/IP 协议或无线协议，诸如 IEEE 802.11，正如本领域技术人员认识和理解的。而且，网络堆栈 310 可包括支持该一个或多个层的一个或多个网络驱动器，诸如 TCP 驱动器或网络层驱动器。网络驱动器可被包括作为计算设备 102 的操作系统的一部分，或作为任何网络接口卡的一部分或计算设备 102 的其它网络接入部件。另外，网络堆栈 310 的任何网络驱动器可被定制、修改或调整，以便提供支持这里描述的本发明的任何技术的网络堆栈 310 的定制或修改部分。另外，网络堆栈 310 的某些部分可以在内核模式下工作，而其它的部分运行在用户模式 332，诸如网络堆栈 310 的应用层。

滤波器 322 可包括分组捕获机构 365，并且滤波器 322 和/或分组捕获机构 365 可包括网络驱动器，诸如工作在客户端 105 的网络堆栈 310 的任何层或部分的网络驱动器。滤波器 322 和/或分组捕获机构 365 可包括遵从网络驱动器接口技术规范 (NDIS) 的驱动器，或 NDIS 驱动器。在另一个实施例中，滤波器和/或分组捕获机构 365 可包括迷你滤波器或迷你端口驱动器。分组捕获机构 365 在一些实施例中还可以工作在内核模式 334。虽然分组捕获机构 365 被显示为滤波器 322 的一部分，但分组捕获机构 365 可以与滤波器 322 分开的。另外，滤波器 322 和分组捕获机构 365 可以工作在客户端 105 的网络堆栈 310 的不同的层或部分。

滤波器 322 可以使用滤波器表，用于滤波分组。滤波表用来确定对于诸如由分组捕获机构 365 截取的分组那样的分组采取什么动作。滤波器 322 可以检查分组的内容，诸如路由信息，根据滤波表确定所采取的动作。在一些实施例中，滤波器 322 可以根据网络分组的内容来丢弃或接收它们。在一些实施例中，滤波器 322 可以根据分组内容和/或滤波器表把网络分组路由到代理 326。滤波器表也可以用来保证不想要的分组被丢弃。滤波器 322 可用来拒绝进入到特定的协议或通过丢弃分组阻止从远程计算机授权到特定的目的地地址的未授权接入。

在一些实施例中，滤波器表包括有关专用网的信息。在其它实施例中，在客户端计算设备 102 处的滤波器 322 接收滤波器表。在这

些实施例的一个实施例中，滤波器 322 从应用 338 或在计算设备 102 处的代理 326 接收滤波器表。在这些实施例的另一个实施例中，滤波器 322 从代理 326 接收配置设置，并把配置设置存储在滤波器表。

分组捕获机构 365 可以截取客户端 105 的任何网络业务，诸如与应用 338 关联的网络分组。在一些实施例中，分组捕获机构 365 透明地截取到应用 338、代理 326、网关 340、或对于客户端 105 的网络堆栈 310 的任何部分的网络分组，所述任何部分诸如是工作在分组捕获机构 365 所工作的层的以上的或以下的层的任何其它驱动器或层。这样，本发明可用于支持这里描述的任何技术和用于任何应用与由应用使用的任何协议。在一个实施例中，分组捕获机构 365 截取出去的分组业务，诸如经由网络 104 和/或网关 340 传送的任何网络业务。分组捕获机构 365 可以把分组转发到代理 325 或代理 326 的帧监视机构 360。在一些实施例中，滤波器 322 经由异步 I/O 控制消息与代理 326 通信。在这些实施例的一个实施例中，分组捕获机构 365 可以经由异步 I/O 控制消息转发寻址到在网关 340 后面的专用网的分组。在其它实施例中，滤波器 322 经由 UDP 分组与在用户空间 334 中运行的代理 326 通信。在一个实施例中，滤波器 322 经由异步 I/O 控制消息从代理 326 接收配置设置。配置设置可包括有关哪些网络、协议、和分组的类型进行滤波的信息。在一个实施例中，滤波器 322 把配置设置存储在滤波器表。在另一个实施例中，滤波器 322 接收包括配置设置的滤波器表。

在一个实施例中，滤波器 322 截取客户端 105 的所有的外出的分组，以便检查。例如，在一些实施例中，滤波器截取由在用户模式下执行的应用 338 生成的分组，以便由客户端 105 发送。如果分组满足在滤波器表中列出的条件，则滤波器 322 可以发送分组到代理 326，而不是到分组的原先的目的地，滤波器 322 可以使用异步 I/O 控制消息，来把分组转发到代理 326。滤波器 322 可以按照或响应于路由表发送分组到代理 326。

在一些实施例中，代理 326 和滤波器 322 经由 IOCTL 应用编程接口 (API)，诸如任何的 IOCTL 库和由微软视窗操作系统族提供的功能调用，进行通信。在其它实施例中，在代理 326 与滤波器 322 之间的基于 IOCTL 的接口可以由运行在客户端 105 处的操作系统的任

何部分提供。虽然是在 I/O 控制消息和 IOCTL 接口方面讨论的，但代理 326 与滤波器 322 可以经由任何适当的机构和/或装置进行通信。

客户端 105 的内核 334 可包括 NDIS 接口。在一些实施例中，NDIS 接口包括多个中间滤波器。在一个实施例中，分组通过 NDIS 接口传送，并可以由多个中间滤波器进行检查。虽然滤波器 322 可作为 NDIS 驱动器被提供，但滤波器 322 也可以是在内核 334 中执行的进程或其它的组或类型的可执行的指令。

本发明的代理 326 可以在客户端 105 处应用空间 332 或用户模式中执行。在其它实施例中，代理 326 可以在内核模式 334 下工作。在一些实施例中，代理 326 提供用于从滤波器 322 接收分组的功能。在其它实施例中，代理 326 提供用于把策略应用到接收的分组的功能。在再一个实施例中，代理 326 提供用于管理到网关 340 的 SSL 隧道的功能。在又一个实施例中，代理 326 提供用于加密和发送分组到网关 340 的功能。代理 326 可包括帧监视器机构 360。帧监视器 360 可包括策略和用于把策略应用到接收的分组的逻辑块。代理 326 可以响应于由帧计数器 360 作出的基于策略的决定，把分组发送到网关 340。

在一些实施例中，帧监视器 360 可以应用策略来在分组发送时确定客户端 105 的条件或终点。在其它实施例中，帧监视器 360 可以识别生成分组的应用 338。在执行实施例的一些实施例中，帧监视器 360 可以响应于该识别的应用 338 作出发送分组到网关 340 的、基于策略的决定。在另一个实施例中，帧监视器 360 可以对分组执行检验和，以便验证该识别的应用实际上生成分组。

在其它实施例中，不是在滤波器 322，或除了滤波器 322 以外，分组捕获机构 365 可被包括在代理 326 中。这样，代理 326 可以截取网络业务。分组捕获机构 365 可使用任何挂钩应用编程接口 (API) 来截取、挂钩、或得到客户端 105 的进入的和/或出去的分组，诸如与应用 338 关联的网络业务。

在一个实施例中，TCP 连接由在客户端 105 处执行的应用 338 发起，以便把 IP 分组传输到目标计算设备，诸如图 1B 的计算设备 102c 或图 1A 的网关 340。远程接入客户端 120 可以截取或捕获由应用 338

生成的 IP 分组。远程接入客户端 120 可以发送 TCP 确认分组到应用 338，并终结由应用 338 发起的 TCP 连接。然后，远程接入客户端 120 创建到第二计算设备 102c 或网关 340 的第二 TCP 连接，并经由第二 TCP 连接发送捕获的 IP 分组。在一些实施例中，远程接入客户端 120 可以把捕获的 IP 分组存储在缓存器中。在这些实施例中，远程接入客户端 120 可以经由第二 TCP 连接把缓存的 IP 分组发送到第二计算设备 102c。把捕获的 IP 分组存储在缓存器中，使能在网络连接中出现中断的情形下保留分组。

在一个实施例中，在接收到捕获的 IP 分组后，网关 340 可以创建在网关 340 与目标计算设备 102d 之间的第三 TCP 连接，诸如图 1A 所示的。网关 340 可保持端口映射的网络地址转换 (NAT) 表，使得网关 340 能够把来自目标计算设备 102d 的响应分组发送到由在客户端 105 处原生成 IP 分组的应用 338 监视的端口。因为客户端 105 只与网关 340 的公共网地址通信，因此客户端 105 不知道目标计算设备 102d 的网络地址，增加了目标计算设备 102d 所处的网络的安全性。类似地，由于网关 340 发起到目标计算设备 102d 的 TCP 连接，因此目标计算设备 102d 没有接收客户端 105 的地址信息，保护了客户端 105 和该客户端所处的网络。另外，因为网关 340 接收 IP 地址，网关 340 可以响应于策略或安全性检验作出是否发送 IP 分组到目标计算设备 102d 的决定，进一步增加了对于目标计算设备 102d 所处的网络的保护。

在一个实施例中，本发明提供用于保护从网关 340 后面的专用的、安全网络发送到外部网络 104 的客户端的分组的方法。本发明通过在网关 340 上提供网络地址转换 (NAT) 功能而使能把客户端 105 与专用网分开。使用 NAT 的 VPN 网关提供客户端 105 的 IP 地址的伪装来保护专用网不被客户端 105 直接第 2 层接入。

一方面，远程接入客户端 120 的任何部分，诸如代理 326、帧监视器 360、滤波器 322、和分组捕获机构 365 或它们的任何部分可包括软件、硬件，诸如 ASIC 或 FPGA，或软件和/或硬件的任何组合。在一些实施例中，远程接入客户端 120 的任何部分，可以经由客户端 105 处的一个或多个刀形开关被提供。

虽然远程接入客户端 120 被显示为具有多个部件，诸如代理 326

和滤波器 322，但本领域技术人员将会认识和理解到，这里描述的远程接入客户端 120 的操作和功能可以以单个机构或单个部件被实施。例如，在一些实施例中，远程接入客户端 120 的操作和功能可被包括在应用 338 内。在一个实施例中，例如，远程接入客户端 120 的操作和功能可以仅仅被提供为代理 326，以及在另一个实施例中，仅为网络驱动器，诸如滤波器 322。

在一些实施例中，远程接入客户端 120，或它的任何部分，诸如代理 326、帧监视器 360、滤波器 322、和分组捕获机构 365，可包括应用、模块、服务、计算机程序、软件部件、web 服务、web 部件、库、功能、进程、任务、线程、或任何其它类型和/或形式的可执行指令，被设计成和能够执行这里描述的本发明的功能，以及可以在用户模式 332 和/或内核模式 334 的任何部分或组合下工作。

如图 1A-1C 所示，本发明的远程接入客户端 120 可以各种不同的方式被部署和使用，以便诸如经由网关 340 或直接地在各个计算设备之间进行通信并提供通过网络的远程接入给其它计算设备。在这些各种不同的环境下，远程接入客户端 120 可用来实施如在下面更详细地描述的、本发明的一个或多个最优化技术。例如，远程接入客户端 120 可用来使得在图 1A-1C 的任何说明性环境下的任何实时数据通信最优化，诸如 VoIP、桌面共享、或 web 会议。

在图 1A-1C 的任何说明性环境下，诸如用于客户端 105、服务器、或网关 340 的任一项的计算设备 102a-102n，可被提供为任何类型和/或形式的计算设备，诸如由 Palo Alto, California 的 HP 公司或 Round Rock, TX 的 Dell 公司制造的那种个人计算机或计算机服务器。图 1D 和 1E 描述对于实施本发明的实施例有用的计算设备 1-2 的框图。如图 1D 和 1E 所示，每个计算设备 102 包括中央处理单元 102，和主存储器单元 104。如图 1D 所示，典型的计算设备 102 可包括图像显示设备 124、键盘 126、和/或指向装置 127，诸如鼠标。每个计算设备 102 还可包括附加的任选单元，诸如一个或多个输入/输出设备 130a-130b(总的用标号 130 表示)，和与中央处理单元 102 通信的缓冲存储器 140。

中央处理单元 102 是响应于和处理从主存储器单元 104 捕获的指令的任何逻辑电路。在许多实施例中，中央处理单元由微处理器提

供，诸如：8088、80286、80386、80486、Pentium(奔腾)、Pentium Pro、Pentium II、Celeron、或Xeon处理器，所有的这些处理器由Mountain View, California 的 Intel 公司制造；68000、68010、68020、68030、68040、PowerPC601、PowerPC604、PowerPC604e、MPC603e、MPC603ei、MPC603ev、MPC603r、MPC603p、MPC740、MPC745、MPC750、MPC755、MPC7400、MPC7410、MPC7441、MPC7445、MPC7447、MPC7450、MPC7451、MPC7455、或MPC7457处理器，所有的这些处理器由 Schaumburg, Illinois 的 Motorola 公司制造；Crusoe TM5800、Crusoe TM5800、Crusoe TM5800、Crusoe TM5800、Efficeon TM8600、Efficeon TM8600、Efficeon TM8600 处理器，由 Santa Clara, California 的 Transmeta 公司制造；RS/6000 处理器、RS64、RS64 II、PS2C、POWER3、RS64 III、POWER3-II、RS64 IV、POWER4、POWER4+、POWER5、或POWER6 处理器 3，所有的这些处理器由 White Plains, New York 的 IBM 公司制造；AMD Opteron、AMD Athlon 64 FX、AMD Athlon、或 AMD Duron 处理器，由 Sunnyvale, California 的 Advanced Micro Devices 公司制造。计算设备 102 可以是基于任何上述的处理器，或能够如这里描述的那样工作的任何其它处理器。

主存储器单元 104 可以是能够存储数据和允许由微处理器 100 直接存取的任何存储单元的一个或多个存储器芯片，诸如静态随机存取存储器(SRAM)、突发 SRAM 或同步突发 SRAM(BSRAM)、动态随机存取存储器(DRAM)、快速寻呼模式 DRAM(FPM DRAM)、增强的 DRAM(EDRAM)、扩展数据输出 RAM(EDORAM)、扩展数据输出 DRAM(EDO DRAM)、突发扩展数据输出 DRAM(BEDO RAM)、增强的 DRAM(EDRAM)、同步 DRAM(SDRAM)、JEDEC SRAM、PC100 SDRAM、双数据速率 SDRAM(DDR SDRAM)、增强的 SDRAM(ESDRAM)、同步链路 DRAM(SLDRAM)、直接 Rambus DRAM(DRDRAM)、或铁电 RAM(FRAM)。主存储器 104 可以是基于任何上述的存储器芯片，或能够如这里描述的那样工作的任何其它可得到的存储器芯片。在图 1E 所示的实施例中，处理器 100 经由系统总线 150(下面更详细地描述)与主存储器 104 通信。图 1E 显示其中处理器 100 经由存储器端口 103 直接与主存储器 104 通信的计算设备 102 的实施例。例如，在图 1E 上，主存储器 104 可以是 DRDRAM。

图 1D 和 1E 显示其中主处理器 100 经由辅助总线，有时称为后段总线，直接与缓冲存储器 140 通信的实施例。在其它实施例中，主处理器 100 通过使用系统总线 150 与缓冲存储器 140 通信。缓冲存储器 140 典型地比主存储器 104 具有更快速的响应时间，它典型地由 SRAM、BSRAM 或 EDRAM 提供。

在图 1D 所示的实施例中，处理器 100 经由本地系统总线 150 与各种 I/O 设备 130 通信。各种总线可用来把中央处理单元 102 连接到任何的 I/O 设备 130，包括 VESA VL 总线、ISA 总线、EISA 总线、微信道结构 (MCA) 总线、PCI 总线、PCI-X 总线、PCI-Express 总线、或 Nu 总线。对于 I/O 设备是视频显示器 124 的实施例，处理器 100 可以使用高级图形端口 (AGP) 与显示器 124 通信。图 1E 显示其中主处理器 100 经由 HyperTransport, Rapid I/O, 或 InfiniBand 直接与 I/O 设备 130 通信的计算机 102 的实施例。图 1E 也显示其中本地总线与直接通信混合：处理器 100 通过使用本地互联总线与 I/O 设备 130a 通信而同时直接与 I/O 设备 130b 通信的实施例。

计算设备 102 可以支持任何适当的安装设备 116，诸如软盘驱动，用于接纳诸如 3.5 英寸、5.25 英寸盘的软盘或 ZIP 盘，CD-ROM 驱动、CD-R/RW 驱动、DVD-ROM 驱动、或各种格式的磁带驱动、USB 装置、硬盘驱动或适合于安装软件和程序的任何其它装置，诸如与本发明关联的远程接入客户端软件 120。

计算设备 102 还可包括存储装置 128，诸如一个或多个硬盘驱动或独立盘的冗余阵列，用于存储操作系统和其它相关的软件，和用于存储应用程序，诸如与本发明的远程接入客户端 120 关联的任何程序。任选地，任何安装设备 118 还可被用作为存储装置 128。另外，操作系统和代理软件 120 可以从可引导的媒体，例如可引导的 CD，诸如 KNOPPIX®，作为 GNU/Linux 从 knoppix.net 可得到的、用于 GNU/Linux 的可引导的 CD 被运行。

而且，计算设备 102 可包括网络接口 118，用来通过各种各样的连接，包括但不限于，标准电话线、LAN、或 WAN 链路（例如，802.11, T1, T3, 56kb, X.25）、宽带连接（例如，ISDN, 帧中继, ATM）、无线连接或以上的任何部分或全部的某些组合，接口到局域网 (LAN)、广域网 (WAN) 或互联网。网络接口 118 可包括内建的网络适配器、网络接口

卡、PCMCIA 网卡、卡总线网络适配器、无线网适配器、USB 网络适配器、调制解调器或适用于把计算设备 102 接口到能够通信和执行这里描述的操作的任何类型的网络的任何其它装置。

在计算设备 102 中可以存在各种各样的 I/O 设备 130a-130n。输入设备包括键盘、鼠标、跟踪板、跟踪球、话筒和画图板。输出设备包括视频显示器、扬声器、喷墨打印机、激光打印机、和染料升华打印机。I/O 设备可以由如图 1D 所示的 I/O 控制器 123 控制。I/O 控制器可以控制一个或多个 I/O 设备，诸如键盘 126 和打印机设备 127，例如鼠标或光笔。而且，I/O 设备还可以提供存储装置 128 和/或用于计算设备 102 的安装媒体 118。在另外其它的实施例中，计算设备 102 可提供 USB 连接，以接纳手持的 USB 存储装置，诸如由 Los Alamitos, California 的 Twintech Industry 公司制造的设备的 USB 闪速驱动线。

在再一个实施例中，I0 设备 130 可以是在系统总线 150 与诸如 USB 总线、Apple 台式总线、RS-232 串行连接、SCSI 总线、火线总线、火线 800 总线、以太网总线、AppleTalk 总线、千兆以太网总线、异步传送模式总线、HIPPI 总线、超级 HIPPI 总线、SerialPlus 总线、SCI/LAMP 总线、光纤信道总线、或串行附着小计算机系统接口总线那样的外部通信总线之间的桥路 170。

如图 1D 和 1E 所示的、那种计算设备 102 典型地在操作系统的控制下工作，该操作系统控制任务的调度和接入到系统资源。计算设备 102 可以运行任何操作系统，诸如 Microsoft® 视窗操作系统的任何版本、Unix 和 Linux 操作系统的不同版、用于 Macintosh 计算机的 MacOS® 的任何版本、任何嵌入的操作系统、任何实时操作系统、任何开放源操作系统、任何专用操作系统、用于移动计算设备的操作系统、或能够在计算设备上运行和执行这里描述的操作的任何其它操作系统。典型的操作系统包括：WINDOWS 3.x、WINDOWS 95、WINDOWS 98、WINDOWS 2000、WINDOWS NT 3.51、WINDOWS NT 4.0、WINDOWS CE、和 WINDOWS XP，所有的这些操作系统由 Redmond, Washington 的微软公司制造；MacOS，由 Cupertino, California 的 Apple 计算机公司制造；OS2，由 Armonk, New York 的 IBM 公司制造；和 Linux，一种由 Salt Lake City, Utah Caldera 公司免费提供的操

作系统，Java 或 Unix 等等。

在其它实施例中，计算设备 102 可以具有不同的处理器、操作系统、和与设备一致的输入设备。例如，在一个实施例中，计算机 102 是由 Palm 公司制造的 Zire 71 个人数字助理。在本实施例中，Zire 71 在 PalmOS 操作系统的控制下工作，它包括针阵输入设备以及五方式导航器设备。

而且，计算设备 102 可以是任何工作站、台式计算机、笔记本电脑、服务器、手持计算机、移动电话、任何其它计算机、或能够通信和具有足够的处理器功率和存储器容量来执行这里描述的操作的计算或电信设备的其它形式。

一方面，本发明涉及提供用于使得在诸如在图 1A-1C 的任何说明性环境下描绘的计算设备之间的通信最优化的各种技术。本发明提供以下的、可以单独地或任何组合地实施的技术：1) 对等路由最优化，2) 经由无损协议传送对于经由有损协议的传输被构建的分组，3) 通过考虑到加密调节最大传输单元 (MTU) 参数而减小网络分段，4) 客户端侧应用知道的网络通信优先化，以及 5) 保护设备免受网络中断。对等路由最优化技术将结合图 2A 和 2B 进行讨论，经由无损协议传送对于经由有损协议的传输被构建的分组的技术将结合图 3A 和 3B 进行讨论，MTU 调节技术将结合图 4 进行讨论，客户端侧应用知道的优先化技术将结合图 5A 和 5B 进行讨论，以及网络中断保护技术将结合图 6A 和 6B 进行讨论。

一方面，本发明涉及提供在第一计算设备经由网关，诸如图 1A 所示的网关，接入第二计算设备之间的对等路由最优化技术。对等路由技术提供在建立或试图建立经由网关的通信会话的计算设备之间的更优化和直接的通信。本发明的实施例的说明性方法 260 将对于图 2A 的说明性环境进行讨论。概述地，环境 200 包括网关 340，提供远程接入连接性给专用网，诸如具有 IP 地址范围 10.10.10.XXX 的网络。与专用网关联的网关 340 可以分配 10.10.10.2 的 IP 地址，用于在专用网上通信。这个专用网可以包括服务器 102c。另外，专用网包括电信设备 210c，诸如任何类型和/或形式的 VoIP 电话。电信设备 210c 被分配有在专用网上的 IP 地址 10.10.10.100。

在一个实施例中，服务器 102 包括信令服务器，它可以提供任何

类型和/或形式的信令服务，用于建立在计算设备，诸如第一计算设备 102a 与第二计算设备 102b 之间的通信会话。在一个实施例中，服务器 102c 支持会话发起协议，SIP，其用于发起牵涉到诸如视频、语音、聊天、游戏、和虚拟现实那样的多媒体单元的互动的用户会话的互联网工程任务组（IETF）标准协议。在一个实施例中，SIP 工作在开放系统互联（OSI）通信模型的应用层。在一些实施例中，第一计算设备 102a 经由信令，诸如经由 SIP 协议，发起经由信令路径到信令服务器 102c 的会话。在一个实施例中，信令服务器 102c 结合网关 340 用于建立在第一计算设备 102a 与第二计算设备 102b 之间的媒体路径 225，诸如用于在电话 210a 与 210b 之间的 VoIP 电信会话。

环境 200 的第一计算设备 102a 可以是网络--专用网或公共网--的一部分，通过连接 341a 经由网络 104 接入网关 340，并穿过防火墙 205a。防火墙 205a 提供接入和穿过公共网，并分配有 24.24.24.100 的 IP 地址。第一计算设备 102a 可以是与电信设备 210a 通信，或接口或耦合到该电信设备，诸如 VoIP 通信设备，或任何其它实时数据通信设备。第二计算设备 102b 可以是专用网的一部分，并分配有 192.168.20.20 的 IP 地址。另外，第二计算设备 102b 可包括基于软件的电信设备 210b，诸如基于软件的 VoIP 电信设备或程序。第二计算设备 102b 可以通过连接 341b 经由网络 104 并穿过防火墙 205b 接入网关 340，防火墙 205b 具有 216.216.10.10 的公共网 IP 地址。防火墙 205a 和 205b 可以是如本领域技术人员已知的任何类型和形式的防火墙，诸如 NAT 防火墙。

图 2A 的第一计算设备 102a 和第二计算设备 102b 包括和使用本发明的远程接入客户端 120，提供在环境 200 中 ad-hoc 对等虚拟网连接。除了保持与网关 340 的、诸如 SSL VPN 连接那样的隧道和虚拟专用连接以外，本发明的远程接入客户端 120 还具有逻辑、功能、和操作，以建立直接到它试图到达的对等体的 ad-hoc 连接，比如 SSL VPN 连接。对于图 2A，图 2B 的说明性方法 260 将用来在本发明的一个说明性实施例中讨论对于媒体路径 225 如何建立对等安全通信会话。如通过方法 200 显示的本发明的对等路由技术提供较好的语音质量和减小与 VoIP 通信以及其它实时数据通信关联的等待时间。

在说明性方法 260 的概略中，在步骤 262，计算设备 102a 和 102b 建立与网关 340 的隧道会话。在步骤 264，第一计算设备 102a 经由到信令服务器 102b 的信令路径 220 使用信令协议，来发起经由网关 340 到第二计算设备 102b 的会话。会话可以由电信设备 102a 与第一计算设备 102a 通信而被发起。在步骤 266，信令服务器 102c 建立电信会话，和在步骤 268，为第一计算设备 102a 提供第二计算设备 102c 的第一网络标识符。第一网络标识符包括第二计算设备 102b 的网络地址，比如主机名或 IP 地址，该网络地址诸如基于用网关 340 通过隧道 341b 所建立的其 IP 地址。在步骤 270，第一计算设备 102a 通过使用第一网络标识符与第二计算设备 102b 通信，以建立连接或通信会话。

在另外的概况中，在步骤 272，网关 340 通过第一计算设备 102a 截取通信，并给第一计算设备 102a 提供用于第二计算设备 102b 的第二网络标识符。第二网络标识符包括由第一计算设备 102a 直接或公开地可接入的第二计算设备 102a 的 IP 地址或主机名，诸如第二计算设备 102b 的最后得知的公共 IP 地址。在步骤 274，在一个实施例中，网关 340 与第二计算设备 102b 通信，以请求第二计算设备 102b 建立浮筒会话，由第一计算设备 102a 经由防火墙 205b 连接到第二计算设备 102b。在一些实施例中，网关 340 在步骤 276 可以协商或否则提供用于第一计算设备 102a 和第二计算设备 102b 加密密钥。在步骤 278，第一计算设备 102a 建立到第二计算设备 102b 的直接连接、通信会话、或媒体路径 225。在其它实施例中，在步骤 280，第一计算设备 102a 和/或第二计算设备 102b 在允许通信之前匹配由其它计算设备接收的加密密钥。

在说明性步骤 262 的一些实施例中，计算设备 102a 和 102b 可以通过任何适当的装置和/或机构，诸如通过任何类型和/或形式的隧道或网关协议建立与网关 340 的连接。在一些实施例中，到网关 340 的连接 341a 和 341b 可以形成虚拟专用网络连接，以及在其它实施例中，可以使用 SSL 或 TLS 提供到专用网的安全通信，诸如由在说明性图 2 上的 IP 范围 10.10.10.XXX 识别的专用网。在一个实施例中，计算设备 102a 和 102b 通过经由专用网穿过防火墙 205a-205b 而连接到网关 340，而在其它实施例中，计算设备 102a 102b 可以经

由专用网连接到网关 340，并且可以不经过防火墙 205a-205b。本领域技术人员将会认识到和看到计算设备 102a-102b 可以连接到和与网关 340 通信的各种各样方式。

在说明性步骤 264，在一个实施例中，电信设备 210a，诸如硬 IP 电话，发起到诸如软 IP 电话的电信设备 210b 的电信会话，诸如电话呼叫。在一些实施例中，电信设备 210a 通过表示电信设备 210b 的分机而发起电话呼叫。当电信设备 210a 发起电信会话时，建立电信会话或媒体会话的这个发起、表示、或请求可以经由 SIP 协议，专用信令协议，或使用于信令的任何其它类型的协议，被发送到信令服务器 102a。信号经由信令路径 220，经由隧道会话 341a 被传送到网关 230，以及经由在网关 340 后面的专用网的内部网路由到达信令服务器 102c。

虽然方法 260 的说明性实施例是对于 VoIP 或电信信令和会话讨论的，但本领域技术人员将认识和理解，本发明可用于发起任何类型和/或形式的通信会话、实时或否则诸如牵涉到多媒体单元，诸如视频、语音、闲谈、游戏、和虚拟真实性等等的互动的用户会话。这样，电信设备 210a-210b、信令/信号路径 220、和信令服务器 120a 由此且适当地包括对应于通信会话的类型和/或形式的设备、信令、协议和通信的类型和/或形式。

在说明性步骤 266 的一些实施例中，信号服务器 102c 可以设置、协商、或建立任何类型的通信会话，以及在一个实施例中，信令服务器 102c 可以建立电信会话，诸如由电信设备 210a 发起的 VoIP 电话。当建立电信或其它媒体会话时，信令服务器 102c 在步骤 270，指令、请求、通知发起的电信设备 210a 和/或第一计算设备 102a 或否则与之通信，以经由某个网络地址联系、通知、接触电信设备 210b 或否则与之通信。在一些实施例中，由信令服务器 102c 提供给发起的电信设备 210a 的网络地址包括在网关 340 后面的专用网上计算设备 102b 的网络地址，即，10.10.10.XXX。在一个实施例中，用于各个电信设备 210b 的网络地址可包括企业专用网地址。

这时，代替经由对等电信设备 210b 的 VPN 专用 IP 地址与之联系，说明性方法 260 经由远程接入客户端 120 实行电信设备 210a 和/或第一计算设备 102a 直接联系对等或目标电信设备 210b 或第二计

算设备 102b。本发明的技术不是对于任何 VoIP 特定的，它可以应用到任何其它协议，诸如在计算设备之间的任何的对等协议。本发明的技术通过客户端试图联系的资源的 IP 地址来作出决定。

在步骤 270，当电信设备 210a 用由信令服务器 120c 在步骤 268 提供的第一网络地址，诸如软 IP 电话的 VPN 专用 IP 地址，发起到电信设备 210b 的数据连接时，网关 340 截取通信，以向电信设备 210 和/或第一计算设备 102b 提供用于联系电信设备 210b 的第二网络地址。在一个实施例中，网关 340 通过相同的建立的 VPN 隧道 341a 介入并发送带外信号正在实行用于硬 IP 电话 210a 的业务的第一计算设备 102a。本领域技术人员将认识和理解，网关 340 可以直接通过任何适当的装置和/或机构把用于联系计算设备 102b 和/或电信设备 210b 的该网络地址传送到电信设备 210 和/或计算设备 102a。例如，网关 340 可以经由第二隧道会话把第二网络地址传送到第一计算设备 102a。

在一些实施例中，网关向第一计算设备 102a 表示最后的已知的公共 IP 地址，正在运行软 IP 电话 210b 的第二计算设备 102b 使用该 IP 地址来联系网关 340。在其它实施例中，这个公共 IP 可能不是第二计算设备的实际的 IP 地址，而可以是其后面是第二计算设备 102b 的防火墙 205b 的 IP 地址。如果计算设备 210a 直接联系防火墙 205b 的公共 IP 地址，则分组可以被防火墙 205b 拒绝。在这些实施例中，网关 340 指令计算设备 102b 建立到第一计算设备 102a 的、本领域技术人员称之为浮筒会话的会话。在防火墙 205b 上打开一个转发口，基于它第一计算设备 102a 可以穿过或返回。在其它实施例中，任何适当的装置和/或机构可用来允许第一计算设备 102a 穿过防火墙 205b，与第二计算设备 102b 联系和通信。

虽然说明性方法 260 是结合在防火墙 205a 后面具有第二计算设备 102n 的、图 2A 的环境 200 讨论的，但本领域技术人员将认识和理解，说明性方法 260 可用于第二计算设备 102b 是直接可接入的而不用穿过防火墙 205a 的环境。这样，说明性方法 260 可以不需要在步骤 274 指令第二计算设备 102b 为第一计算设备 102a 连接到第二计算设备 102b 提供浮筒会话或其它机构。

在一些实施例中，网关 340 在步骤 276 可以在计算设备 102a-

102b 之间协商用于安全通信的密钥。在计算设备 102a-102b 处的远程接入客户端 120 可以使用这个用于安全和加密通信的密钥，和/或鉴权或授权其它计算设备。在其它实施例中，为了保证恶意的计算设备不利用这个开孔，网关 340 在步骤 276 在两个计算设备 102a 和 102b 之间协商安全密钥，并且各个远程接入客户端 120 在允许数据通信之前保证密钥匹配。例如，在建立浮筒会话的实施例中，这个密钥保证进入到开孔的分组是来自浮筒会话所指的计算设备。

在其它实施例中，网关 340 不执行步骤 276，以提供在计算设备 102a-102b 之间的对等通信会话的安全机构。例如，计算设备 102a-102b 可能是处在同一个专用企业网络，所以可以是信任的。在另外的实施例中，不用网关 340 协商安全密钥，计算设备 102a-102b 使用任何适当的装置和/或机构，来鉴权和/或授权其它计算设备进行对等通信。在一些实施例中，计算设备 102a-102b 可以经由网关隧道会话，诸如经由路径 341a，或在步骤 280，经由在步骤 278 建立的媒体路径 225，进行鉴权和/或授权。例如，每个计算设备 102a-102b 的远程接入客户端 120 可以在允许任何数据在连接 225 上进行通信之前通过建立的媒体路径 225 检验密钥的匹配。

在步骤 278，不用经过网关 340 在计算设备 102a-102b 之间建立用于任何类型和/或形式的通信的直接媒体路径 224，并且在一些实施例中，不使用计算设备 102a-102b 的各个 VPN 分配的 IP 地址，而是代之以使用它们的公共 IP 地址或由它们驻在的网络分配给它们的 IP 地址。通过使用本发明的技术，计算设备 102a-102b 的各个远程接入客户端 120 互相用作为临时对等 SSL 网关，直接解密互相的 SSL 会话，而不用经由网关 340 通信。经由路径 225 的直接对等通信会话避免经由网关 340 的额外跳。这将减小由于采用经由网关 340 的较长路由造成的等待时间，并将改进诸如图 2A 所示的 VoIP 通信那样的实时数据通信的质量、性能和感受。

在一些实施例中，网关 340 可被配置成每当计算设备 102 试图建立对等通信会话或经由网关 340 接入资源时自动执行说明性方法 260 的技术。在一些实施例中，网关 340 可被配置成仅仅对于源 IP 地址、目的地 IP 地址、或它们的任何组合的，某些 IP 地址范围自动执行说明性方法 260 的技术。在另一个实施例中，网关 340 可以根据经

由网关 340 接入的应用和/或资源的类型执行这种技术。例如，在一个实施例中，网关 340 可以对于任何的类型的、经由网关 340 共享屏幕数据的桌面或屏幕共享应用自动执行这种技术。在其它实施例中，网关 340 可以确定根据任何类型和/或形式的商业规则、接入控制策略或其它配置、算法、和统计值执行这种技术。例如，网关 340 可以根据在对等计算设备之间的、基于 ping 的定时统计来执行这种技术。如果对等计算设备比与网关 340 互相更靠近，则网关执行对等路由技术。本领域技术人员将认识和理解本发明的网关可被适配为或否则被配置成执行本发明的对等路由技术的各种方式。

一方面，本发明涉及允许经由无损协议传送对于经由有损协议的传输被构建的分组。在图 3B 所示的一个技术中，本发明当经由无损或可靠的协议传送有损或不可靠的协议，诸如，例如经由 TCP 或 SSL/TCP 连接在 UDP 上传送 RTP 时，使用虚假确认技术。在图 3C 所示的另一个技术中，本发明使用有效负载移位，以经由无损协议传送对于经由有损协议的传输被构建的分组。在一些实施例中，本发明的这些技术帮助达到在 UDP 级别的传输层安全性（TLS），正如本领域技术人员在下面的说明中将认识和理解的。

下面鉴于图 3A 的说明性环境 300 和另外鉴于图 1A-1E，讨论用于实施虚假确认技术的本发明的实施例的说明性方法 360。概略地，环境 300 包括计算设备 102a 的客户端 105a 与计算设备 102b 的另一方客户端 105b 通信，或替换地经由网络 104 与网关 340 通信。在一些实施例中，客户端 105a 可以经过 IP 路由器 305a-305b，或网络 104 可以具有 IP 路由器 305a-305b。虽然在其它实施例中，计算设备 102a-102b 和网关 340 可以是在同一个网络 104。另外，电信设备 210a 可以与客户端 105a 相关联，以及电信设备 210b 可以与另一方客户端 105b 或网关 340a 相关联。

客户端 105a 可包括第一网络堆栈 310a，客户端 105 或网关 340 可包括第二网络堆栈 310b。网络堆栈 320a-310a 可包括一个或多个网络层，诸如开放系统互联（OSI）通信模型的任何网络层。例如，如图 3A 所示，网络堆栈 310a-310b 包括在帧层之上通信的 TCP/IP 343a-343b，它是本领域技术人员认为适用于基于 TCP/IP 的网络 104。TCP/IP 343a-343b 包括可靠的或无损协议的说明性实施例。例

如，在如本领域技术人员已知的 TCP 343a-343b 中，网络堆栈 310a-310b 或其任何驱动器或机构，诸如 TCP 驱动器，可以执行算法和操作，以及包括提供协议的一个或多个无损或可靠的特性的逻辑或功能。例如，为了支持 TCP 343a-343b，网络堆栈 310a-310b 可以执行分组排序、分组重发、分组接收的确认、流控制算法、滑动窗口算法、和/或 Nagle 的算法，以及本领域技术人员在 TCP 343a-343b 或任何其它无损协议方面将认识和看到的、任何其它可靠性关联的操作和算法。

另外，网络堆栈 310a-310b 可包括用于支持 SSL 或 SSL VPN 通信的 SSL 341a-341b 层。例如，SSL 层 341a-341b 可用于在远程接入客户端 120 之间或在远程接入客户端 120 和网关 340 之间的网关或隧道会话。如图 3A 所示，网络堆栈 310a-310b 还可提供用于诸如 UDP 那样的有损协议 342a-342b 的层，以通过诸如 TCP 那样的无损协议 343a-343b 被传送。在一些实施例中，有损或不可靠的协议 343a-343b 可包括在 UDP 上的实时协议 (RTP)，以及可包括具有诸如话音或音频的任何表示那样的任何类型和/或形式的实时数据的有效负载。在其它实施例中，有损协议 342a-342b 可以在建立的 VoIP 会话中，诸如经由以上结合图 2A 和 2B 讨论的说明性方法 260 建立的会话中，承载到和来自客户端 105a 的 VoIP 通信。诸如 UDP 342a-342b 那样的无损协议可被选择用于诸如话音的实时应用，因为对于诸如对等客户端 105b 那样的接收者，及时得到分组要比以可靠的方式，诸如经由无损协议得到分组，是更重要的。

网络堆栈 310a-310b 还包括本发明的远程接入客户端 120 的垫层 (shim) 322a-322b。垫层 322a-322b 可包括远程接入客户端 120 的任何部分，并且在一些实施例中，它包括网络驱动器、网络驱动器接口、或用于提供如这里描述的本发明的虚假确认技术的、其它网络层关联的机构。垫层 322a-322b 可包括软件、硬件、或软件与硬件的任何组合。在一个实施例中，垫层 322a-322b 可以在网络分组到达 TCP 层 343a 之前工作在网络堆栈的 IP 层。在其它实施例中，垫层 322a-322b 可以工作在 TCP 层 343a-343b。本领域技术人员将认识和看到，垫层 322a-322b 可以在网络堆栈 310a-310b 中以与无损协议的操作的层关联的任何方式工作，包括在无损协议的层中或在

其附近。

图 3B 的方法 360 所示的、本发明的虚假确认技术允许经由诸如 TCP 343a-343b 那样的无损协议传送诸如 UDP 342a-342b 那样的有损协议。通过垫层 322a-322b 发出对于 TCP 分组接收的虚假确认，本发明的技术阻止或避免诸如在 TCP 343a-343b 的例子中任何的分组排序、分组重发、流控制算法、滑动窗口算法、和/或 nagle 算法那样的无损协议的可靠性机构、操作和算法。这样，有损协议 342a-342b 可以通过无损协议 343a-343b 通信，但保持它的有损或不可靠的特性，这是诸如在实时数据通信中想要的。这个技术也使得有损协议能够安全地通信，或经由隧道协议通过网关，或仅仅经由 TCP/IP 而不把无损协议的无损特性应用到有损协议通信。

关于说明性方法 360 的概貌，在步骤 365，计算设备 102a 和 102b 或网关 340 建立基于无损协议的连接，诸如 TCP 连接，通过该连接可以传送无损协议分组。在步骤 370，本发明的远程接入客户端 120 可以检测，无损协议分组包括有损协议，诸如 RTP 或 UDP，或否则包括实时数据。在一个实施例中，在步骤 375，说明性方法 360 可以用密钥，诸如经由带外 TLS 或步骤 367 的 SSL 会话提供的密钥，加密有效负载。在步骤 380，无损协议分组的接收的虚假确认可以诸如通过垫层 322a-322b 被传送到或否则提供给网络堆栈 310a-310b。响应于无损协议分组的接收的虚假确认的接收，在步骤 385，各个网络堆栈 310a-310b 不执行一个或多个，或全部的、提供无损协议的可靠的或无损特性的算法和操作。在步骤 390，在网络堆栈 310a-310b 之间传送具有有损协议有效负载的无损协议分组。

在说明性方法 360 的步骤 365，无损协议连接可以经由使用一种类型和/或形式的无损协议的任何适当的装置和/或机构被建立。在一个实施例中，客户端 105a 的网络堆栈 310a 建立到具有网络堆栈 310b 的一方客户端 105a 的无损协议连接，诸如 TCP。在另一个实施例中，客户端 105a 的网络堆栈 310a 建立到具有网络堆栈 310b 的网关 340 的无损协议连接。另外，步骤 365 的无损协议连接可以以诸如 SSL 那样的安全的方式被建立，或作为虚拟专用连接。虽然网络堆栈 310a-310b 被显示为具有相同的网络层，但本领域技术人员将认识和理解，网络堆栈可以具有对应的层，它们可以是不同的版本

或是与不同的操作系统和/或驱动器关联的，以及每个网络堆栈 310a-310b 可以具有附加的层、更少的层、或不同的层。

在说明性步骤 360，在一个实施例中，远程接入客户端 120 截取网络分组，诸如经由分组捕获机构 365，和通过适当的装置和/或机构检查网络分组，以确定在网络分组的有效负载中使用的协议的类型，或在网络分组的有效负载中内容的类型。在一些实施例中，远程接入客户端 120 的垫层 322a-322b 可用于截取和检查网络分组。在一个实施例中，远程接入客户端 120 可以截取网络分组，并确定网络分组是否包括任何的无损协议或特定的无损协议，诸如 TCP。如果网络分组是无损协议，则远程接入客户端 120 检验有效负载，以确定协议的类型和/或数据的类型。在一个实施例中，远程接入客户端 120 可以通过网络分组的有效负载的任何适当字段，诸如表示有效负载的有损协议的首部的任何部分，来确定有效负载具有有损协议内容。在另一个实施例中，远程接入客户端 120 可以通过有效负载的任何数据来确定，有效负载是否包括有损协议或包括实时数据。

在一个实施例中，远程接入客户端 120 确定 TCP 分组包括 RTP 或 UDP 的有效负载，并施加有效负载的加密。远程接入客户端 120 可以通过使用任何类型和/或形式的加密来用以任何适当的方式提供的密钥加密网络分组的有效负载。在一些实施例中，密钥或密码在客户端 105a-105b 或客户端 105a 与网关之间经由带外 TLS 被协商，如图 3A 所示，与在其它实施例中的传统 TLS 会话相反，在传统 TLS 会话中会话首先被协商并且同一个套接字用于数据通信。在一些实施例中，在步骤 375 的加密逐个分组地进行。在另一个实施例中，一次对多个分组执行加密。

在本发明的说明性方法 360 的步骤 380，网络分组，例如无损协议分组的接收的虚假确认被发出、传送、或否则被提供给包括各个发送和接收计算设备 102a-102b 的网络堆栈 310a-310b 或网关 340。垫层 322a-322b、远程接入客户端 120 的任何部分、或网络堆栈 310a-310b 的任何部分可以发出网络分组的接收的虚假确认。一方面，网络分组的接收的虚假确认是虚假的，其意义在于其被传送而不确认网络分组的实际接收，以便阻止与网络堆栈 310a-310b 关联

的无损协议的无损和可靠的机构。这样，网络分组的接收的虚假确认可以包括与网络分组的接收的实际确认相同的形式和/或类型。

在一些实施例中，接收的虚假确认在传送网络分组之前被发送到网络堆栈 310a-310b。在其它实施例中，接收的虚假确认在传送网络分组后但同时或以某种方式被发送，诸如阻止接收的网络堆栈 310a-310b 的无损协议机构不应用到发送的网络分组。在一个实施例中，对于每个网络分组发送网络分组的接收的虚假确认，和在另一个实施例中，可以对每个通信会话或无损协议连接发送一次网络分组的接收的虚假确认。而且，本领域技术人员将认识和理解，接收的虚假确认对于不同的操作系统可以在网络堆栈 310a-310b 的不同的位置执行。例如，在一个实施例中，接收的确认可以在微软的视窗操作系统家族中在网络驱动器接口技术规范（NDIS）驱动器级别被发送。

在说明性方法 360 的步骤 385，接收来自步骤 380 的网络分组的接收的虚假确认的网络堆栈 310a-310 可以响应于这样的接收，而可以不执行、停住执行、或阻止执行提供无损协议的一个或多个无损特性的任何一个或多个算法和操作。例如，在作为无损协议的 TCP 的实施例中，网络堆栈 310a-310n 可以对于网络分组或 TCP 连接不执行任何一个或多个以下的操作：分组排序、分组重发、流控制算法、滑动窗口算法、和/或 nagle 算法。在一些实施例中，接收的虚假确认必须逐个分组地接收，以阻止网络堆栈 310a-310n 的无损层采用可靠性算法。这样，发送的网络堆栈 310a-310n 可以逐个分组地确定本发明的虚假确认技术应用到哪些分组。可以有一些无损协议网络分组包括对于其应当施加无损协议的可靠性算法的有损协议。在其它实施例中，网络分组的接收的虚假确认可以对于无损协议连接接收一次，以便阻止对于在无损协议会话或连接期间接收的任何以后的分组采用可靠性算法。

在步骤 390，说明性方法 360 经由网络堆栈 310a-310n 传送具有无损协议有效负载的无损协议分组。在一个实施例中，无损协议分组在步骤 385 后被传送，或在其它实施例中，在步骤 385 之前传送。这样，虽然无损协议分组在网络中变为丢失的，但不试图在预期有损协议分组时回收该分组。

虽然通过使用网络分组的接收的虚假确认，诸如在 TCP 中，讨论方法 360 的说明性实施例，但任何的类型和/或形式的指示、请求、或指令可被传送到网络堆栈 310a-310n，以阻止采用无损协议的任何可靠性或无损算法。在一些实施例中，网络堆栈 310a-310n 的无损协议层可被适配或被配置成使得配置、标记或指令不逐个分组地或基于会话或连接来使用可靠性算法。例如，无损协议可以在无损协议分组的首部中具有表示对于分组是否应当丢弃或避免可靠性的字段。

现在参照图 3C，通过说明性方法 345 示出对于经由无损协议发送按照有损协议构建的分组所采取的步骤的另外的实施例，这也被称为有效负载移位技术。关于说明性方法 345 的概貌，在步骤 348，要通过使用不可靠的传输协议发送的第一分组由诸如客户端 105 的第一设备接收。在步骤 350，第一设备 105 创建第一 TCP 分组，其包括接收的第一分组的第一有效负载和与在第一设备 105 与第二设备之间建立的 TCP 连接关联的信息的第一 TCP 首部。在步骤 352，第一设备 105 发送第一 TCP 分组到第二设备。在步骤 354，第一设备 105 接收要通过使用不可靠的传输协议发送的第二分组，并且在步骤 356，创建第二 TCP 分组，其包括接收的第二分组的第二有效负载和与第一 TCP 首部信息。在步骤 358，第一设备在接收到来自第二设备的第一有效负载的接收的确认之前，发送第二 TCP 分组到第二设备。

仍旧参照图 3C，并且现在更详细地，在步骤 348，要通过使用不可靠的传输协议发送的第一分组由第一设备 105 接收。在一些实施例中，分组打算通过使用 UDP 的有损协议被发送。在另外的实施例中，分组包括 UDP 上的 RDP。在其它实施例中，第一分组由在用户模式 332 下执行的应用程序 338 生成。在一些实施例中，分组由在内核模式 334 下执行的应用 338 生成。在其它实施例中，第一分组由第一设备 105 接收，用于重发。在另外的实施例中，第一分组在它到达网络堆栈 310a-310b 之前由过滤器进程 322 截取。过滤器进程 322 可以在用户模式 332 或在内核模式 334 下执行。在一些实施例中，滤波器 322 是迷你驱动器。在其它实施例中，滤波进程 322 使用应用挂钩，以截取第一分组。在另外的实施例中，应用挂钩经由应用编程接口（API）被实施。在一个实施例中，网络分组的挂钩发

生在网络堆栈 310a-310n 的网络层。

在步骤 350，第一设备 105 创建第一 TCP 分组，其包括接收的第一分组的第一有效负载和与在第一设备 105 与第二设备之间建立的 TCP 连接关联的信息的第一 TCP 首部。例如在一个实施例中，TCP 连接可以在客户端 105 与网关 340 之间被建立，以及在另一个实施例中，可以在客户端 105 与网关 340 之间被建立。在一些实施例中，第一设备 105 表示，TCP 分组包含通过打开特定的 TCP 端口经由有损协议发送而被构建的分组的有效负载。在其它实施例中，第一设备 105 表示，TCP 分组包含通过在 TCP 首部中设置一个标记经由有损协议发送而被构建的分组的有效负载。TCP 首部可包括有关源节点的信息、有关目的地节点的信息、或具体地标识 TCP 分组的序列号。

在步骤 352，第一设备 105 发送第一 TCP 分组到第二设备。在一些实施例中，第二设备可以是网关 340。在其它实施例中，第二设备是“对等”计算设备 102b。第一 TCP 分组可以在例如通过使用 SSL 或 TLS 发送到第二设备之前被加密。

在步骤 354，第一设备 105 接收要通过使用不可靠的传输协议，诸如 UDP，发送的第二分组。第二分组可以从生成第一分组的同一个应用 338 接收。在步骤 356，如上所述，第一设备 105 创建第二 TCP 分组，其包括接收的第二分组的第二有效负载和与第一 TCP 首部信息的。在步骤 358，第一设备 105 然后在接收来自第二设备的第一有效负载的接收的确认之前，发送第二 TCP 分组到第二设备。在一些实施例中，当从第二设备接收确认时，第一设备 105 在发送分组之前更新 TCP 首部信息。在其它实施例中，第一设备 105 创建具有更新的 TCP 首部信息和具有第二有效负载的第三 TCP 分组。第一设备然后发送第三 TCP 分组。

在接收 TCP 分组后，如有必要，第二设备解密 TCP 分组，并且确定有效负载是对于使用有损协议发送被构建的一个或多个分组。第二设备可以基于分组被接收的端口或是通过在 TCP 首部信息中的标记来对此进行确定。一旦确定，第二设备就从有效负载剥离 TCP 首部，并传递有效负载。

另一方面，本发明涉及调节报告的最大传输单元 (MTU) 参数，以通过减小用于加密的网络分组的分组分段而使得网络通信最优

化。这种技术可被应用到图 3A 的说明性环境 300 的一个或两个网络堆栈 310a-310n。通过加密网络分组的有效负载，诸如按照上述的说明性方法 360 处理的任何网络分组，可增加有效负载的尺寸。即，考虑到未加密的原先的有效负载到加密的有效负载的尺寸改变，可能增加网络分组的尺寸。

仍旧参照图 3A，网络堆栈 310a-310b 可包括最大传输单元 402a-402b (MTU) 参数，以表示在网络中，诸如在基于以太网的网络中，通过一种物理媒体可被发送的最大数据单元的尺寸。在 TCP/IP 的实施例中，MTU 402a-402b 表示可以由互联网协议 (IP) 层接口发送的最大数据报或分组而不需要接口把数据报分解或分段为更小的单元。MTU 参数 402a-402b 可以与诸如网络接口卡那样的通信接口相关联。用于以太网的缺省的 MTU 尺寸是 1500 字节，而 IEEE 802.3 是 1492 字节。本领域技术人员将认识和理解，缺省 MTU 尺寸将是基于连网技术，诸如令牌环、FDDI、X.25 等等。

现在参照图 4，流程图显示本发明的 MTU 调节方法 400 的说明性实施例。概略地，在步骤 405，建立在计算设备之间的会话，诸如在第一计算设备 102a 与第二计算设备 102b 之间的会话。在步骤 410，一个计算设备 102，诸如第一计算设备 102a，检测具有加密的有效负载的网络分组。在步骤 415，计算设备 102a-102b 考虑到有效负载的加密的部分的尺寸，确定对于网络堆栈 310a-310n 的 MTU 402a-402b 参数的设置。在步骤 420，考虑到加密的部分，减小 MTU 402a-402b 参数。如果 MTU 402a-402b 被请求或被报告，则 MTU 402a-402b 将表示比与物理层关联的 MTU 尺寸，诸如对于以太网的 1500，更小的尺寸。

通过使用这个技术，在网络 104 上任何设备可以按照减小的 MTU 尺寸把网络分组传送到网络堆栈 310a-310n，减小的 MTU 尺寸可以沿到网络堆栈 310a-310n 的路由被加密并不被分段。如果网络分组被加密，则它仍旧应当适配于物理网络层媒体的实际的 MTU 尺寸，诸如以太网。例如，MTU 参数 402a-402b 可被设置为对于以太网的 1500 的缺省 MTU 尺寸，并考虑到加密开销，按照说明性方法 400，被减小确定的数目的字节，例如 100。网络分组可以从服务器资源被发送到客户端，包括与 1400 的报告的 MTU 402a-402b 尺寸相等的尺寸。网

络分组可以经过网关 340，并经由 SSL 隧道被加密，这又使得网络分组尺寸增加到 1475。由于这个尺寸适配于以太网物理媒体的 MTU 尺寸，网络分组将不分段。

在说明性方法 400 的步骤 405，可以建立在第一计算设备 102a 与第二计算设备 102b，诸如图 2A 的客户端 105b 或网关 340 之间的任何类型和/或形式的通信会话。在一些实施例中，通过使用在第一计算设备上的远程接入客户端 120 建立会话。在一个实施例中，远程接入客户端 120 建立与网关 340 的会话，诸如 SSL VPN 会话，或到对等计算设备 102b 上的另一个远程接入客户端的会话。

在步骤 410 的一些实施例中，远程接入客户端 120 检测具有加密的有效负载的网络分组。在一个实施例中，分组捕获机构 365 截取网络分组，并且代理 326 确定分组是否被加密。然而，远程接入客户端 120 的任何其它部分，诸如滤波器 322 或帧监视器 360 可以确定分组是否被加密。在一个实施例中，网络分组的整个有效负载被加密，而在一个实施例中，有效负载的一部分被加密。本发明可以使用任何类型和/或形式的装置或机构，用于确定分组是否具有加密。例如，在一些情况中，远程接入客户端 120 可以检验网络分组的、表示有效负载被加密的标记或字段。在其它实施例中，远程接入客户端 120 可以检验有效负载的任何部分是否难以理解，因为它包含来自加密的随机数据或噪声。另外，加密的有效负载可以相关于网络堆栈 310a-310n 的任何层，诸如第 2、3、6 或 7 层的加密而被加密。

在步骤 415 的一些实施例中，本发明的说明性方法 400 逐个分组地确定对报告的 MTU 402a-402b 的调节，或在其它实施例中，根据连接或会话来确定，以及在步骤 420，由此来调节 MTU 402a-402b。在一个实施例中，MTU 402a-402b 被正好减小了网络分组的加密开销量。在某些情形下，说明性方法 400 确定一次对于整个会话或连接的 MTU 402a-402b 尺寸调节，和减小 MTU 402a-402b 尺寸到考虑了对于整个会话加密开销的数值。例如，虽然网络分组可以具有变化的加密开销，但调节考虑最大加密开销。在另外的实施例中，MTU 402a-402b 可以考虑一下内容被调节，即考虑当网络分组离开网络堆栈 310a-310n 时可能出现的加密，诸如在网络分组的端对端网络行

进时可能出现的、由网关 340 进行的加密。

另外，MTU 402a-402b 尺寸除了加密开销以外可以对于其它网络性能因素被调节。在一些实施例中，虽然 MTU 402a-402b 由于加密开销而被减小，但考虑与网络通信关联的其它开销和因素，它可能进一步减小，以及在其它情形下增加。例如，MTU 402a-402b 对于与加密无关的因素被事先调节，以及在使用本发明的技术后，考虑加密开销，来减小 MTU 402a-402b。本领域技术人员将认识和理解，对于调节 MTU 边界或除了按照本发明的技术对于加密开销减小调节以外可以有其它的因素和考虑。

现在参照图 5A 和 5B，另一方面，本发明涉及客户端端应用知道的网络通信优先化技术。本发明的远程接入客户端 120 根据应用的类型和/或优先权提供客户端上应用网络通信的智能的和客户端中心优先化。如图 5A 的系统 500 中显示的，计算设备 102 的远程接入客户端 105 连接到网络 104。客户端 105 可以执行一个或多个应用 338a-338n，它们经由远程接入客户端 120 的代理 326 和滤波器 322 接入网络 104。在一些实施例中，应用 338a-338n 提供一个或多个实时数据通信，诸如 VoIP。在其它实施例中，一个或多个应用 338a-338n 可以提供电子邮件、合作、在线会议、和/或桌面共享关联的服务或功能。

如图 5A 所示，分组捕获机构 365, 365' 可被包括在远程接入客户端 120 的代理 326 和滤波器 322 中，用于截取客户端 105 的任何的应用 338a-338n 的网络业务。远程接入客户端 120 可包括任何队列 540a-540n，用于排队和优先化客户端 105 的网络通信。在一个实施例中，队列 540a-540n 可被包括在网络驱动器中，诸如用于滤波器 322 的 NDIS 驱动器，以及在其它实施例中，可以与代理 326 包括在一起，或由代理 326 可接入的。队列 540a-540n 可包括任何类型和/或形式的、用于存储和/或安排诸如由分组捕获机构 365 截取的网络分组那样的网络分组的适当的装置和/或机构。在一些实施例中，队列 540a-540n 可以与客户端 105 的应用 338a-338n 关联的网络分组相关联或被分配给该网络分组。在其它实施例中，队列 540a-540n 可以按优先权的级别，诸如高、中、低，或数字地诸如优先权 1...10，被组织。本领域技术人员将认识和理解，队列 540a-540n 的数目可

以是基于任何想要的优先权粒度，诸如 3, 5 或 10 个优先权级别。另外，队列 540a-540n 中的一些可用于在网络分组被放置到基于优先权的队列 540a-540n 和/或从该队列取出之前接收和/或发送网络分组。

远程接入客户端 120 还可以接入或使用路由表 538，用于确定如何经由代理 326 路由客户端的网络分组，诸如经由网关 340 到网络 104。在一个实施例中，代理 326 建立和保持到网关 340 的 SSL VPN 连接，如图 1A 所示。在一个实施例中，路由表 538 包括有关源计算设备与目的地计算设备的信息，以便识别在源计算设备与目的地计算设备之间的通信路径或连接。路由表 538 可包括源 IP 地址与源端口，和目的地 IP 地址与目的地端口，以识别在网络 104 上的通信路径。例如，源 IP 地址与源端口可表示客户端 105 的 IP 地址和客户端 105 处的应用 338a-338n 藉以在网络 05 上通信的端口。目的地 IP 地址可表示应用 338a-338n 经由对等设备使用的目的地端口与其通信的对等计算设备的 IP 地址。

另外，远程接入客户端 120 可以具有一个或多个策略 520，用于规定与在应用于上运行的、与应用 338a-338n 关联的网络通信的客户端端优先化。这些策略 520 可以由任何适当的装置和/或应用被规定。在一些实施例中，策略 520 可以由应用 338a-338n 的名称和/或应用 338a-338n 的类型被规定。在其它实施例中，策略 520 可以按由应用 338a-338n 使用的一个或多个协议的类型和/或网络分组的有效负载的尺寸被规定。在另一个实施例中，策略 520 根据应用是运行在客户端 105 的前台还是后台来规定优先化。在再一个实施例中，策略 520 可以根据目的地地址，诸如主机名称或 IP 地址，和/或目的地端口号表示优先化。另外，策略 520 可以考虑多个应用 338a-338n 和/或可以在任何点在客户端 105 处执行的多个协议分级结构地被规定。而且，策略 520 可以按条件地被规定，诸如如果一个应用 338a 正在运行，则第二个应用 338b 可以具有较高的或较低的优先权。本领域技术人员将认识和理解规定客户端端应用优先权的多种方式。

策略 520 可以由代理 326 接入、被配置成代理 326、或被代理 326 加载。例如，策略 520 可以由网关 340 提供或经由网关 340 被下载。策略 520 可包括用于规定策略的任何类型和格式的语义和/或语言，

和可以经由任何类型和/或形式的媒体被提供，诸如由一个或多个网络分组电子地，或经由文件，诸如 XML 文件。策略 520 可以由用户通过任何适当的装置和/或机构被配置。例如，代理 326 可提供配置机构，诸如用户接口、图形或否则设计，和该配置机构被构建用于配置或规定策略 520。

鉴于图 5A 和图 1A-1C 的系统 500，将描述由图 5B 的方法 550 显示的本发明的优先化技术。概述地，在说明性方法 550 的步骤 555。客户端 105 截取与在客户端 105 上的应用 338a-338n 关联的一个或多个网络分组，以及在步骤 560，网络分组被存储在队列 540a-540n。在步骤 565，用于截取的和排队的网络分组的优先权根据应用 338a-338n 的类型和/或优先权被确定。在步骤 570，对于网络分组表示所确定的优先权，和在步骤 575，按照所确定的优先权传送网络分组。这样，由在客户端 105 处的应用 338a-338n 生成的外出网络分组在发送之前根据应用 338a-338n 的类型和/或优先权被客户端 105 优先化。例如，应用 338a 可以生成 VoIP 通信的实时数据，诸如经由到网关 340 的 SSL 连接的 TCP/IP 会话在 UDP 上的 RTP。客户端 105 通过使用本发明的技术，可以在诸如非实时数据通信应用那样的其它应用之前，优先化应用 338a 的实时数据通信。这个技术可以称为服务质量 (QoS) 网络，其中在诸如交换机和路由器的中间网络设备中进行网络业务优先化。

在说明性方法 500 的步骤 555，客户端 105 可以对于应用 338a-338n、网关 340、对等计算设备、和网络堆栈的任何网络层透明地截取一个或多个应用 338a-338n 的网络分组。这样，本发明的技术支持客户端 105 处的任何类型的应用 338a-338n。在一些实施例中，网络分组由分组捕获机构 360 经由代理 326 或滤波器 322 被截取。应用 338a-338n 的任何进入和/或外出网络分组可以由本发明的远程接入客户端 120 截取。

在步骤 560，在步骤 555 截取的网络分组可被存储在队列 540a-540n。在一个实施例中，网络分组在步骤 565 和 570 优先化网络分组之前被存储在临时队列 540a-540n。在其它实施例中，网络分组在步骤 565 和/或 570 给网络分组排优先权之后被存储在所确定的队列 540a-540n 或与应用 338a-338n 关联的队列 540a-540n。

在步骤 565，本发明的远程接入客户端 120 确定网络分组与应用 338a-338n 的关系，以便确定优先权和应用任何基于优先权的策略 520。客户端 105，诸如经由代理 326，可以通过任何适当的装置和/或机构把网络业务与应用 338a-338n 相关联。在一些实施例中，代理 326 通过网络分组的任何内容，诸如在网络的有效负载中任何首部、字段、或数据的类型和内容，来识别如从应用 338a-338n 生成的网络分组。在其它实施例中，网络分组通过把来自路由表 538 的信息，诸如源和目的地地址和 IP 地址及端口号与网络分组的 IP 地址和端口号相匹配而与应用 338a-338n 相关联。在一些实施例中，代理 326，诸如经由帧监视器 360，可以对于分组执行检验和，以验证所识别的应用实际上生成分组。

另外，远程接入客户端 120 可以确定与网络分组关联的应用 338a-338n 是在客户端 105 的前台还是在后台运行。而且，远程接入客户端 120 可以通过客户端 105 的操作系统确定分配给应用 338a-338n 的任何优先权，诸如处理任务优先权。在其它实施例中，远程接入客户端 120 可以确定应用 338a-338n 的任何其它特性和统计资料，诸如尺寸、存储器使用、总的执行时间、和/或使用的频率。本领域技术人员将认识和理解，本技术使用的应用的各种特性可用于提供客户端端应用知道的网络通信优先化。

在步骤 570，本发明的远程接入客户端 120 根据在步骤 565 与分组关联的应用 338a-338n 表示对于截取的和排队的网络分组的优先权。在一个实施例中，代理 326 使用策略 520 按照由策略 520 规定的或表示的优先化法则施加优先权到应用 338a-338n 的网络分组。在一些实施例中，代理 326 可以使用应用 338a-338n 的特性，诸如运行在前台或后台，以表示应用 338a-338n 的网络分组的优先权。在其它实施例中，代理 326 可以使用策略 520 与应用 338a-338n 的特性的任何组合，以表示应用 338a-338n 的网络分组的优先权。

在一些实施例中，代理 326 向滤波器 322 表示用于管理分组队列的优先权，以便应用表示的优先权。代理 326 可以通过任何适当的装置和/或机构，诸如经由应用编程接口（API），诸如 IOCTL 接口，或本领域技术人员已知的、任何类型和/或形式的接口，来把网络分组的优先权传送到滤波器 322。在一个实施例中，滤波器 322 通过名

称不知道应用 338a-338n，但可以经由路由表 538 把优先权与应用 338a-338n 的网络分组相关联。对于网络分组的应用 338a-338n 可以通过源和目的地标识符的任何组合，诸如 IP 地址和端口号，被识别。这样，在一些实施例中，代理 326 通过路由信息而不是应用名称，向滤波器 322 表示优先权。在其它实施例中，代理 326 向滤波器 322 提供在应用 338a-338n 之间诸如通过应用名称或进程 id 到路由表 538 中的路由信息的映射。

根据对于应用 338a-338n 的表示的优先权，在一些实施例中，滤波器 322 可以在优先权的支持下将网络分组放置、安排、或协调到队列 540a-540n 中。在一个实施例中，滤波器 322 可以把网络分组从临时队列 540a-540n 或从存储器或前台存储装置移动到与应用 338a-338n 关联的队列 540a-540n、与优先权关联的队列 540a-540n、或与应用和优先权关联的队列 540a-540n。例如，在一个实施例中，所有的高优先权网络业务可被放置在高优先权队列 540a，并按照应用 338a-338n 的优先权的次序，诸如优先于其它应用 338a-338n 的实时数据应用 338a-338n 按次序排列。在一些实施例中，网络分组可以根据网络分组由分组捕获机构 365 被截取的时间，诸如以 FIFO 方式按次序被安排在优先权队列 540a-540n 中。在再一个实施例中，一个队列 540a-540n 可以用于通过滤波器 322 的优先化。每个网络分组可以相对于所有其它的截取的网络分组以优先权次序被放置和排列，以便逐个分组地提供对于所有的应用 338a-338n 和截取的网络分组的优先化。本领域技术人员将认识和理解，网络分组可在各种优先权队列 540a-540n，诸如高、中、低，或通过任何其它粒度被放置和，并且以实施这里描述的本发明的操作的任何适当的方式在队列中被放置或被排列。

在一个实施例中，对于应用 338a-338n 的网络分组被放置在与应用 338a-338n 关联的队列 540a-540n。例如，对于传送到第一目的地 IP 地址和第一目的地端口的应用的所截取的网络分组可被放置在第一队列 540a。在另一个实施例中，对于诸如电子邮件或语音应用的一种类型的应用 338a-338n 的所有的网络分组或对于由诸如 RTP 或 UDP 的应用 338a-338n 使用的一种类型的协议的所有的网络分组可被放置在队列 540a-540n 中，用于优先化一个或多个应用的网络分组。

例如，在线合作关联的应用 338a-338n 可在第一队列 540a 中被放置和优先化，用于合作关联的应用。第二队列 540b 可用于电子邮件关联的应用 338a-338n。在另一个例子中，队列 540a 可用于传送实时数据或通过使用 RTP 和/或 UDP 协议传送应用 338a-338n。在再一个例子中，队列 540a 可用于通过使用诸如 ICA 或 RDP 的远程显示协议进行通信的应用 338a-338n。

在与由特定的应用 338a-338n、通过应用 338a-338n 的类型或类别，或通过协议组织的、每个应用相关的队列 540a-540n 内，网络分组可以通过生成它们的应用 338a-338n1 特性，例如前台应用、网络分组的尺寸、或网络分组被截取的时间被进一步优先化。在一些实施例中，一个或多个队列 540a-540n 可用于被截取的但没有优先化的网络分组，因为策略 520 不存在或施加到网络分组，或策略 520 表示忽略或不处理网络分组，用于优先化。本领域技术人员将认识和理解，网络分组以基于优先权的方式被放置和被放置在队列 540a-540n 的各种方式与应用 338a-338n、应用 338a-338n 的类型、或由应用 338a-338n 使用的协议有关，以及优先权可以是基于对于客户端 105 规定的策略 520。

在说明性方法 550 的步骤 575，网络分组按照对于网络分组的确定的优先权从队列 540a-540n 被传送。在一些实施例中，网络分组被组织成优先权队列 540a-540n，这样，最高优先权队列 540a-540n 的网络分组首先被传送，然后下一个最高的优先权队列第二，等等。在其它实施例中，队列 540a-540n 由应用 338a-338n 被组织，所以，在步骤 575，本发明根据应用 338a-338n 的各个优先权传送来自队列 540a-540n 的网络分组。不管队列 540a-540n 组织和管理，本领域技术人员将认识和理解，本发明的远程接入客户端将以按照或遵从确定的优先权的方式传送来自队列的网络分组，确定的优先权又是基于或从客户端的策略 520 得出的。

在一些实施例中，本发明的远程接入客户端 120 在确定哪些分组从哪个队列进行传送时考虑其它网络因素。例如，远程接入客户端 120 可以接收网络配置的指示，诸如接收用于与应用 338a-338n 关联的 TCP 连接的零窗口尺寸。在另一个例子中，远程接入客户端 120 可能认识到大量到特定的目的地的重发。这样，在一些实施例中，

远程接入客户端 120 可能减缓或不传送与其它网络因素关联的网络分组，诸如拥塞，即使在网络分组比在队列 540a-540n 中的其它网络分组，具有更高的优先权。因此，客户端 105 根据应用 338a-338n 和按照用于客户端 105 的任何策略 520，和鉴于任何网络统计资料与在网络上发生的其它因素，来控制和管理在应用 338a-338n 上客户端 105 的网络通信的优先化。

再一方面和现在参照图 6A 和 6B，本发明涉及提供网络中断保护技术，以便得到持久的和可靠的连接性。图 6A 显示以上结合图 3A 讨论的环境 300。环境 300 显示诸如在图 1A-1C、2A、或 5A 上显示的任何的计算设备 102 和网关 340 的网络堆栈 310a 和 310b。每个网络堆栈 310a-310b 可包括一个或多个网络层，诸如在帧网络层之上的 TCP/IP 网络层，正如本领域技术人员将认识和理解的。虽然网络堆栈 310a-310b 在图 6A 的环境 300 中被显示为具有某个组的网络层，但本领域技术人员将认识和理解，网络堆栈 310a-310b 可以具有以任何适当的组合的任何类型和/或形式的网络层，以及每个网络堆栈 310a-310b 可以相对于其它网络堆栈具有每个层的不同的形式。

网络堆栈 310a-310b 可被认为具有网络堆栈的第一部分 605a-605b 和网络堆栈的第二部分 610a-610b。如图 6A 的示例性网络堆栈 310a-310b 所示，网络堆栈的第一部分 605a-605b 包括在 TCP 网络层处和下面的网络层。第二部分 610a-610b 可包括在 TCP 网络层，诸如通过 SSL 的 UDP 协议层上面的那些网络层。虽然第一部分 605a-605b 和第二部分 610a-610b 被显示为在 TCP 层上被分配的、分段的、或划分的，但在实施本发明的网络中断保护技术中，第一部分和第二部分可在较高的或较低的所划分层上形成，正如本领域技术人员将认识和理解的。

图 6A 上显示的网络堆栈 310a-310b 可以表示在客户端 105 处的应用 338a-338b，诸如图 5A 所示的客户端，以建立到第二计算设备 102b，或替换地到网关 340 的对等 SSL VPN 连接。客户端 105 可以是移动客户端，诸如笔记本电脑、个人数字助理 (PDA)、智能电话、或任何类型的移动计算或通信设备。客户端 105 可以传送实时数据，诸如经由 UDP 协议或在 UDP 上的 RTP，经由对于对等设备 102b 或网

关 340 建立的 SSL 会话的 VoIP 通信。在一个实施例中，远程接入客户端 120 的代理 326 建立和保持到网关 340 或对等计算设备 102b 的 SSL 或 SSL VPN 会话。代理 326 可以工作在用户模式 332，和可以操控任何网络层和与网络堆栈 310a-310b 的第二部分 610a-610b 关联的协议处理，以及任何应用层协议。作为基于 TCP/IP 网络 104，网络堆栈 310a-310b 的第二部分 610a-610b 在 SSL 上的 UDP 会话可以通过形成网络堆栈 310a-310b 的第一部分 605a-605b 的 TCP/IP 堆栈被传送。鉴于本发明的远程接入客户端 120，诸如图 1A 或 5A 所示的，滤波器 322 可以是在网络堆栈 310a-310b 的第一部分 605a-605b 内工作在内核模式 332 的网络驱动器。

本发明使用如图 6B 的说明性方法 650 所显示的网络中断保护技术，以便在网络级别连接断开，诸如对于网络堆栈 310a-310b 的第一部分 605a-605b 的任何类型和/或形式的网络中断时，保持网络堆栈 310a-310b 的第二部分 610a-610b。本发明的网络中断保护技术，可以对于客户端 105 的应用 338a-338n、客户端 105 的用户、在网络堆栈 310a-310b 的第一部分 605a-605b 以上的一个或多个网络层、和网关 340 或对等计算设备 102b、和它们的各个网络堆栈 310a-310b 的任何部分透明地执行。在一个实施例中，网络中断被保护，而不用通知客户端的用户：网络被中断或会话被断开。

在说明性方法 650 的概观中，在步骤 665，客户端 105 通过在客户端和诸如对等计算设备或网关的另一个设备之间的网络连接经由至少第一协议建立会话。这样，网络堆栈 310a-310b 在客户端 105 处被建立或被使用。网络堆栈 310a-310b 具有第一部分 605a-605b 和第二部分 610a-610b。在步骤 660，检测网络连接的中断，该网络连接的中断使得网络堆栈 310a-310b 的第一部分 605a-605b 解除或被中断成不能使用或不能继续使用。在步骤 665，本发明在中断期间保持网络堆栈 310a-310b 的第二部分 610a-610b 和保持与第二部分 610a-610b 的网络层关联的会话。

在中断期间，在步骤 670，与网络堆栈 310a-310b 的第二部分 610a-610b 关联的任何网络分组可以被排队。在步骤 675，网络堆栈 310a-310b 的第一部分 605a-605b 被重新建立，或否则从网络中断进行接收。虽然网络堆栈 310a-310b 的第一部分 605a-605b 被重新建

立，但本发明保持第二部分 610a-610b 和它的会话，在步骤 680，允许通过链接或重新关联网络堆栈 310a-310b 的第二部分 610a-610b 与第一部分 605a-605b，来继续进行会话。网络连接和/或会话可以在步骤 680 自动重新鉴权。在步骤 685，说明性方法可以传送任何排队的网络分组并继续透明地进行会话，就好像没有发生网络中断那样。

在说明性方法 655 的实施例中，第一计算设备 102a 可以通过适当的装置和/或机构和使用任何类型和/或形式的基于连接的协议来建立与诸如对等计算设备 102b 或网关 340 那样的第二设备的网络连接。例如，网络连接可以经由在 TCP/IP 网络上的 TCP 连接或通过在 IPX/SPX 网络上的 SPXP 连接被建立。在一些实施例中，网络连接可以由在客户端处的任何应用 338a-338n，诸如图 5A 所示的任何应用发起。例如，远程显示客户端，诸如 Citrix Systems 公司的 ICA 客户端或微软公司的远程显示客户端，可以发起或建立网络连接。在其它实施例中，说明性步骤 665 的网络连接可以经由代理 326、滤波器 322 或远程接入客户端 120 的任何其它部分被发起和/或被建立。在一个实施例中，网络连接的建立形成网络堆栈 310a-310b 的第一部分 605a-605b。在其它实施例中，网络堆栈 310a-310b 的第一部分 605a-605b，或它的部分，在客户端 105 启动后经由到网络 104 的连接被建立。

在一些实施例中，网络堆栈 310a-310b 的第二部分 610a-610b 通过经由在网络连接上的任何类型和/或形式的协议，诸如 ICA 或 RDP 的远程显示协议建立一个或多个会话，诸如 SSL 会话，而被形成。会话可以经由客户端的应用 338a-338b 或远程接入客户端 102 被建立。在一个实施例中，会话可以对应于与对等计算设备 102b 或网关 340 的隧道或网关会话。在另一个实施例中，会话可以是任何类型的交互会话，诸如，例如经由信令协议 SIP 建立的媒体会话。例如，网络堆栈 310a-310b 的第二部分 610a-610b 可包括 VoIP 通信会话，诸如由图 2B 的说明性方法 260 建立的会话。另外，可以有与网络堆栈 310a-310b 的第二部分 610a-610b 关联的多个会话。例如，SSL 或 SSL VPN 会话可以形成一个会话，而第二个会话，诸如经由在 UDP 上的 RTP 的媒体会话，可以形成第二个会话。另外，在网络堆栈

310a-310b 的任何网络层上，在客户端 105 处的一个或多个应用 338a-338n 可以建立与对等计算设备 102b 的应用级别会话。在一个实施例中，远程接入客户端 120 的代理 326 负责建立和保持网络堆栈 310a-310b 的第二部分 610a-610b 和一个或多个相关的会话。

在本发明的说明性方法 650 的步骤 660，检测网络连接的中断。在一个实施例中，网络中断可能是由于移动客户端在网络与网络分段之间的漫游造成的，这在一些实施例中使得客户端 105 得到新的网络 IP 地址和/或主机名称。在一些实施例中，这种中断将断开网络堆栈 310a-310b 的第一部分 605a-605b，诸如，例如使得 TCP 或 SPX 连接断开。一方面，该中断使得网络堆栈 310a-310b 的第一部分 605a-605b，或它的任何部分被解除，或否则需要重新建立、重新连接、重新配置、或重新构建。例如，在一些实施例中，网络堆栈的 IP 层在 TCP 层重新建立时可以保持完整。在一个实施例中，任何 TCP 关联的驱动器可能需要被重新启动。在其它实施例中，即使在网络连接中断时 TCP/IP 层是完整的，仅仅需要建立新的 TCP 连接。在其它实施例中，TCP/IP 层是完整的但需要为新的网络或网络分段重新配置它自己，诸如改变客户端 105 的 IP 地址。本领域技术人员将认识和理解，网络连接被中断和冲击或影响网络堆栈的第一部分的各种方式。

在一些实施例中，代理 326，或远程接入客户端 120 的任何其它部分可以通过任何适当的装置和/或机构检测网络中断。在一个实施例中，代理 326 可以通过在呼叫或对网络堆栈 310a-310b 的第一部分 605a-605b 执行 API 调用时接收错误消息或故障而确定网络中断。例如，对于第二部分 610a-610b 由代理 326 保存的 SSL 会话依赖于或取决于网络堆栈 310a-310b 的第一部分 605a-605b 的 TCP 连接。当代理 326 经由 SSL 会话进行协商时，代理 326 可以接收表示与 TCP 连接的问题的错误或故障消息。在其它实施例中，代理 326 可以接收来自网络堆栈 310a-310b 的第一部分 605a-605b 的、表示网络中断的任何网络层的事件或消息。本领域技术人员将认识和理解，可以检测网络中断的各种方式。

在说明性步骤 665，在一些实施例中，在检测到网络中断时，本发明的代理或远程接入客户端 120 的任何其它部分在中断期间保持

网络堆栈 310a-310b 的第二部分 610a-610b。例如，虽然由代理 326 保持的基于 SSL 会话取决于根本的 TCP 连接，但代理 326 通过对 TCP 连接的中断保持 SSL 会话打开或激活。由于可以有与网络堆栈 310a-310b 的第二部分 610a-610b 的一个或多个层关联的多个会话，在一些实施例中，代理 326 保持多个会话的一个或多个或全部会话打开或激活，虽然网络堆栈 310a-310b 的第一部分 605a-605b 中断。

在说明性方法 650 的步骤 670，本发明的远程接入客户端 120，在一些实施例中，在网络中断期间将与网络堆栈 310a-310b 的第二部分 610a-610b 关联的任何协议的一个或多个网络分组进行排队。远程接入客户端 120 可以使用任何类型和/或形式的排队机构，诸如在图 5A 上显示的任何队列 540a-540n。在其它实施例中，远程接入客户端 120 在中断期间可以丢弃网络分组，诸如与有损协议关联的任何分组，诸如用于话音通信的在 UDP 上的 RTP。在某些情形下，可能希望丢弃诸如 UDP 分组那样的分组，以便减小诸如在话音通信中的等待时间和质量问题。在另外的实施例中，远程接入客户端 120 可以将一些网络分组排队和丢弃其它网络分组。在附加的实施例中，远程接入客户端 120 可以将网络分组排队和在预定的时间间隔后丢弃一些或所有的网络分组。远程接入客户端 120 可以使用策略 520 来确定哪些网络分组排队和/或丢弃。例如，第一应用 338a 的网络分组可以进行排列，而第二应用 338b 的网络分组被丢弃。在其它实施例中，远程接入客户端 120 可以使用任何网络统计资料或任何网络业务检查技术，例如本领域技术人员已知的状态检查，来确定在中断期间是否排队和/或丢弃网络分组。

在说明性方法 650 的步骤 675，重新建立网络堆栈 310a-310b 的第一部分 605a-605b，而网络堆栈 310a-310b 的第二部分 610a-610b 被保持，以及保持网络堆栈 310a-310b 的第二部分 610a-610b 的任何想要的会话。网络堆栈 310a-310b 的第一部分 605a-605b 可以通过任何适当的装置和/或机构被重新建立。例如，客户端 105 可以通过诸如登录到用于漫游的移动客户端 105 的新网络而重新建立到网络的 TCP/IP 连接。在其它实施例中，远程接入客户端 120，诸如经由代理 326 或滤波器 322，重新建立网络堆栈 310a-310b 的第一部分 605a-605b。例如，代理 326 可以发起和建立新的 TCP 连接。在重新

建立第一部分 605a-605b 时，网络堆栈 310a-310b 的第二部分 610a-610b 与第一部分 605a-605b 链接、与其重新关联、或开始使用或继续使用其来重新建立网络堆栈 310a-310b。在一些实施例中，代理 326 通过任何网络层的事件被告知以：第一部分 605a-605b 已被重新建立，和在其它实施例中，可以以任何预定的频率轮询，以便确定第一部分 605a-605b 被重新建立。例如，代理 326 可以检验 TCP 连接是否激活或是否可被重新连接。

在一些实施例中，在步骤 680，远程接入客户端 120，诸如代理 326，可以自动重新鉴权客户端 105，或客户端 105 的用户，用于网络连接，诸如对于网络堆栈 310a-310b 的第一部分 605a-605b 的 TCP 连接。例如，远程接入客户端 120 可以使用客户端 105 的用户的任何网络关联的证书来自动重新鉴权到网络 104 的客户端 105。另外，远程接入客户端 120 可以自动重新鉴权客户端 105 或客户端 105 的用户，用于与网络堆栈 310a-310b 的第二部分 610a-610b 关联的任何会话。例如，在代理 326 与网关 340 或对等计算设备 102c 之间的 SSL 会话可以被重新鉴权。

在另一个例子中，应用 338a 可以接入主机服务、web 服务器、或使用鉴权证书以便接入的应用服务器。代理 326 可以通过使用与应用关联的鉴权证书来自动重新鉴权对于相应的服务或服务器的应用 338a。在一些实施例中，远程接入客户端 120 可以在多个级别上重新鉴权客户端和/或客户端 105 的用户，诸如用于网络接入和/或 TCP 连接、SSL 或 SSL VPN 会话、和/或任何应用级别会话，诸如媒体互动用户会话，例如 VoIP 电话会话。而且，在步骤 685 之前的任何时间、在步骤 685 期间，例如在传送排队的网络分组之后但在继续进行其它通信之前、和在步骤 865 之后，可响应于对于来自对等计算设备，诸如服务器或网关 340，的鉴权的请求，可以重新鉴权远程接入客户端 120。

在说明性方法 650 的步骤 685，本发明的远程接入客户端 120 继续使用网络堆栈的第二部分 610a-610b 的一个或多个会话。如果任何网络堆栈已被排列或在步骤 670 保持排队，则远程接入客户端 120 传送排队的网络分组并继续传送客户端 105 的任何网络分组，诸如通过客户端 105 的一个或多个应用 338a-338n 生成的或发送到其的

网络分组。这样，本发明的网络中断保护技术对漫游的移动计算解决方案提供无缝的和透明的解决方案，并用于一般地提供可靠的和持久的网络连接和接入。

在 VoIP 通信的例子中，本发明的说明性方法 650 将减小由于网络中断造成的电话呼叫失败的次数和改进 VoIP 的使用和体验。VoIP 用户不需要由于在网络可得到性方面的临时网络中断而重新连接电话呼叫，因为本发明的远程接入客户端 120 将自动保持会话并重新连接到网络。另外，本发明的远程接入客户端 120 将自动重新鉴权连接和会话，用于在网络中断后提供安全性。而且，本发明的为了保护技术对于以下项目是有用的：1) 在网络中断过程中继续自动进行事务、命令、或操作，2) 在网络中断过程中保持会话关联的上下文和缓冲存储器，和 3) 自动处理由于网络中的改变造成的客户端的网络地址的改变。

通过提供可靠的和持久的连接，本发明还避免断开作为在第一计算设备 102a 与计算设备 102b，诸如图 1C 所示的客户端 105a 和 105b 之间作为一部分功能的事务、命令或操作。例如，使用 Windows Explorer 的文件复制操作没有被设计成在网络连接中断之后继续工作。在客户端 105 处的用户可以使用 Windows Explorer 的文件复制特征，把文件从客户端 105 复制到服务器 102c。因为文件的尺寸，这个操作可能花费相当大的时间间隔完成。如果在文件复制到服务器的操作的中间期间，在客户端 105 与服务器之间的网络连接有断开，则文件复制失败。一旦网络连接被重新建立，用户就需要启动来自 Windows Explorer 的另一个文件复制操作，把文件从客户端 105 复制到服务器。在本发明下，用户不需要启动另一个文件复制操作。网络连接按照本发明的网络中断保护技术被重新建立，如图 6B 所示。这样，将不把网络连接的断开通知 Windows Explorer 的文件复制，所以不会失败。远程接入客户端 120 会重新建立任何连接和发送任何排队的数据，这样，操作可以继续进行而不失败。远程接入客户端 120 保持因为网络连接的断开没有被传送到服务器的、与文件复制操作关联的数据队列。一旦网络连接被重新建立，远程接入客户端 120 就可以发送排队的数据，然后继续传送与在预期的过程中文件复制操作关联的数据。

虽然本发明的这个方面是对于文件复制操作描述的，但本领域技术人员将认识到，在第一计算设备 102a 与第二计算设备 102b 之间执行的任何操作、事务、命令、功能等等可被保持和继续进行，而不因为网络连接中断而失败，而且不用客户端 105 或客户端 105 的用户认识到存在中断或有中断的通知。另外，事务或操作可以对于应用 338、网关 340、第二计算设备 102c 和网络堆栈 310a-310b 的第二部分 610a-610b 的任何部分被透明地保持和继续进行。

通过给客户端 105 提供与对等计算设备 102b 或网关 340 的可靠的和持久的连接，本发明通过在网络连接断开时保持用户会话而避免在对等体处打开与应用 338 的新的用户会话的过程，诸如在服务器处的主机服务。对于在对等计算设备之间的每个用户会话，每个计算设备可以保持会话特定的上下文和缓冲存储器，以及其它用户会话的那个实例关联的应用特定的机构。对于建立的每个新的用户会话，这些会话特定的上下文和缓冲存储器需要被恢复或重新建立，以便反映新的用户会话。例如，在客户端 105 处的用户可以具有与具有 web 服务器或 web 应用的服务器 102c 的 http 会话。服务器 102c 可以保持对于提供与客户端 105 的 http 会话的这个实例特定的上下文。上下文可被存储在服务器的存储器、服务器的文件、数据库或与提供服务器 102c 的功能关联的其它部件中。并且，客户端 105 可以具有对于 http 会话的实例特定的本地上下文，诸如用于跟踪对于 web 服务器的未完成请求的机构。这个上下文可被存储在客户端 105 的存储器、客户端 105 的文件、或与客户端 105 接口的其它软件部件中。如果在客户端 105 与服务器 102c 之间的连接不是持久的，则需要在服务器 102c 和客户端 105 处用新会话特定的上下文来建立新的用户会话。本发明保持会话，这样，不需要重新建立新的会话，以及新的特定会话上下文。

本发明在网络级连接断开时保持用户会话和不用通知客户端的用户：会话被断开。在本发明的这方面的操作时，客户端 105 建立到对等计算设备的连接。经由该连接，建立在客户端 105 与服务器之间的会话。远程接入客户端 120 可以存储和保存任何会话关联的消息，诸如鉴权证书，和对于建立的会话的客户端 105 和主服务器 102c 上下文。在检测到网络连接的中断时，远程接入客户端 120 可

以重新建立网络堆栈 310a-310b 的第一部分 605a-605b，而同时保持网络堆栈的第二部分 610a-610b。网络连接中断可以引起由在客户端 105 与服务器 102c 之间的会话所使用的基础 TCP/IP 连接的断开。然而，由于网络堆栈 310a-310b 的第二部分 610a-610b 被保持，会话可以在网络连接被重新建立后被重新建立和/或继续进行，而不用通知客户端 105 的用户：会话被断开。因此，通过使用本发明的网络中断保护技术，由网络连接中断造成的会话断开有效地对于用户是隐蔽的。

而且，通过提供可靠的和持久的连接，本发明还使得客户端 105 能够经过不同的网络拓扑，而不用在客户端 105 处重新启动会话或应用 338。例如，客户端 105 可以是具有无线网连接的笔记本电脑。当客户端 105 从第一无线网移动到第二无线网时，客户端的网络连接可能与第一无线网临时断开，因为在建立了与第二无线网的网络连接。第二无线网可以分配新的网络标识符给客户端 105，诸如主机名称或互联网协议地址。这个新的网络标识符可以不同于由第一无线网分配给客户端 105 的网络标识符。在另一个例子中，客户端 105 可以物理地通过以太网电缆连接到网络上的端口。物理连接可被拔去，客户端 105 移动到另一个位置，以将插入到网络的不同的端口。这造成网络连接的中断，并有可能造成分配的网络标识符的改变。不利用本发明，在对等计算设备之间的任何会话由于网络拓扑的改变、网络连接的中断，和/或分配的网络标识符的改变，可能需要重新启动。通过这里描述的方法和系统，本发明的远程接入客户端 120 保持用于客户端的网络连接和自动地重新建立客户端 105 的网络连接，包括处理网络拓扑和网络标识符的改变。客户端 105，和在客户端 105 处的任何应用或会话，可以继续工作，就好像没有网络连接中断或网络标识符改变那样。而且，在客户端 105 处的用户可能没有认识到，有任何断开或改变，以及客户端 105 没有接收到这样的断开的任何通知。

另一方面，本发明的任何技术，诸如图 2B、3B、3C、4、5B 和 6B 的说明性方法，可以以一个或多个互相组合被实施。在一个实施例中，对等路由技术可以用虚假确认和/或 MTU 调节技术来实施。这提供客户端通信实时数据，诸如 VoIP，以经由更加优化和直接的路

由连接到对等体和经由安全 SSL/TCP/IP 连接上的 UDP 传送实时数据，而同时避免由于 TCP 的任何可靠性机构造成的任何等待时间和减小由于加密开销造成的分段。另外，这个实施例还可以与客户端端应用知道的优先化技术和/或网络中断保护技术相组合。这样，安全实时数据通信可以从客户端以比客户端的其它应用更高的优先权被传送，以便改进诸如 VoIP 的实时体验的质量。网络中断技术允许移动 VoIP 电话，诸如笔记本电脑的软电话、在网络接入点之间漫游、和自动继续进行会话。

本发明的技术是对于网络通信最优化的互相补充，诸如，例如通过 SSL VPN 网关的 VoIP 通信。这样，1) 对等路由技术，2) 虚假确认技术，3) 有效负载移位技术，4) MTU 调节技术，5) 客户端端应用知道的技术，和 6) 网络中断保护技术中的每一项可以通过本发明的一个或多个以下的技术和最优化被实施：1) 对等路由技术，2) 虚假确认技术，3) 有效负载移位技术，4) MTU 调节技术，5) 客户端端应用知道的技术，和/或 6) 网络中断保护技术。

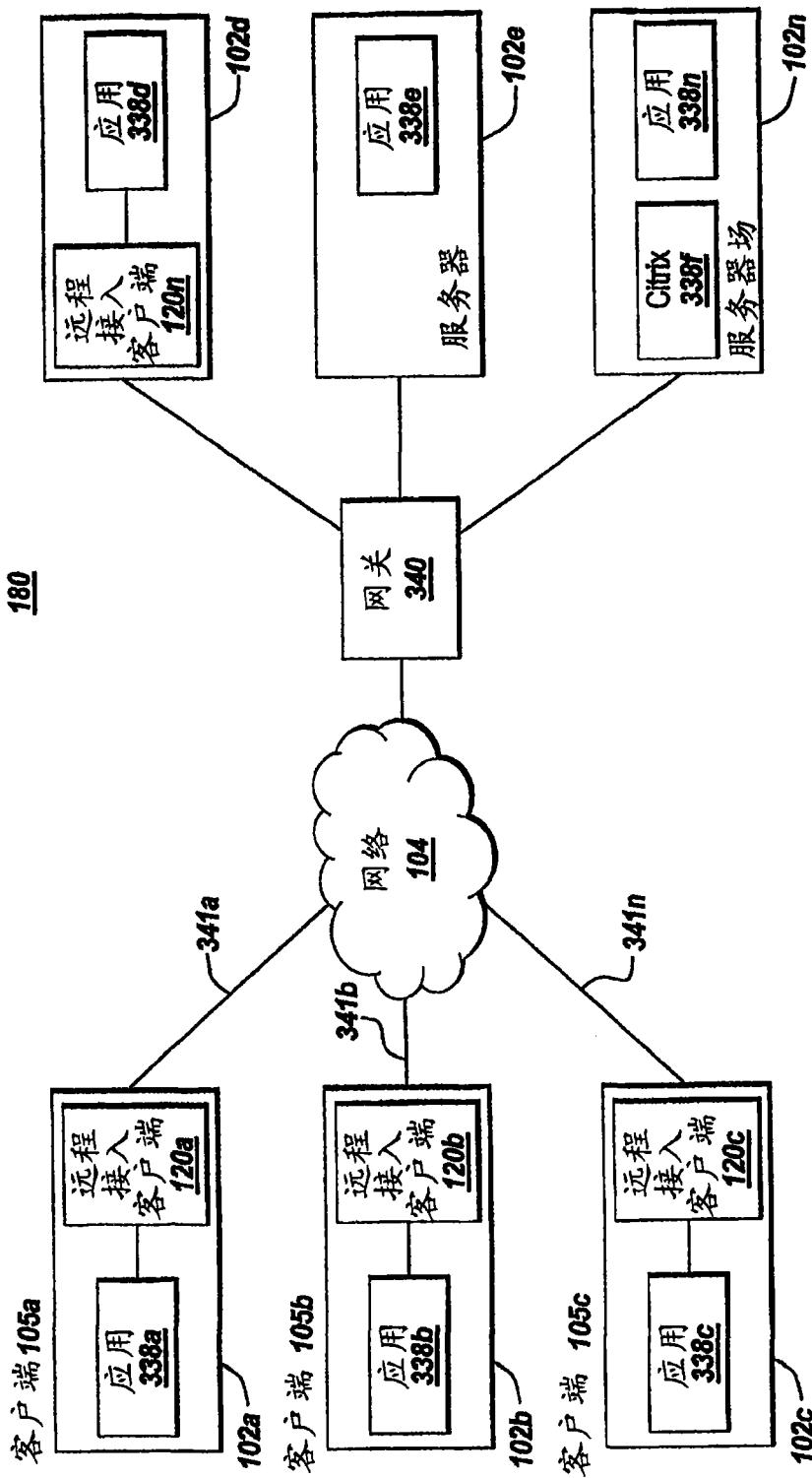
在本发明的另一个说明性例子中，在线会议、合作、和/或桌面共享业务，诸如 GoToMeeting. com, WebEx. com 或 LiveMeeting. com 的主机业务在本发明的一个或多个实施例中可使用本发明的技术。主机业务可以使用网关 340 和说明性方法 260 的技术，来实行在会议主持者的第一计算设备与会议参加者的第二计算设备之间的对等连接。会议主持者与会议参加者的计算设备可以经由主机业务下载远程接入客户端 120，或它的任何部分。一旦会议主持者与会议参加者建立对等连接，则对等计算设备就可以使用本发明任何的最优化技术使得它们的通信最优化，诸如 MTU 调节技术、客户端侧应用知道的技术、或网络中断保护技术。本发明的最优化技术连同对等路由一起，将改进在线会议、合作、或桌面共享的性能、效率和用户体验。

在再一个方面和参照图 2A，例如，本发明的远程接入客户端 120 可以把客户端 105 的动态主配置协议 (DHCP) IP 地址和公共可见的 IP 地址分发到电信设备 210a-210b，诸如基于硬件或软件的 VoIP 电话。本发明的网关 340 易于发现诸如图 2A 所示的客户端 105b 那样的客户端的公共 IP 地址。这样，本发明的技术使得通过协议传送它

---

们的 IP 地址的协议能够继续起作用。

许多改变和修改方案可以由本领域技术人员作出，而不背离本发明的精神和范围。所以，必须清楚地理解，所说明的实施例仅仅是作为例子被显示的，不应当看作为限制本发明，本发明是由以下的权利要求规定的。这些权利要求被读出为包括它们在文字上阐述的内容，并且也包括没有实质的不同的、那些等价的单元，虽然与在上面的说明中显示和描述的其它方面是不同的。



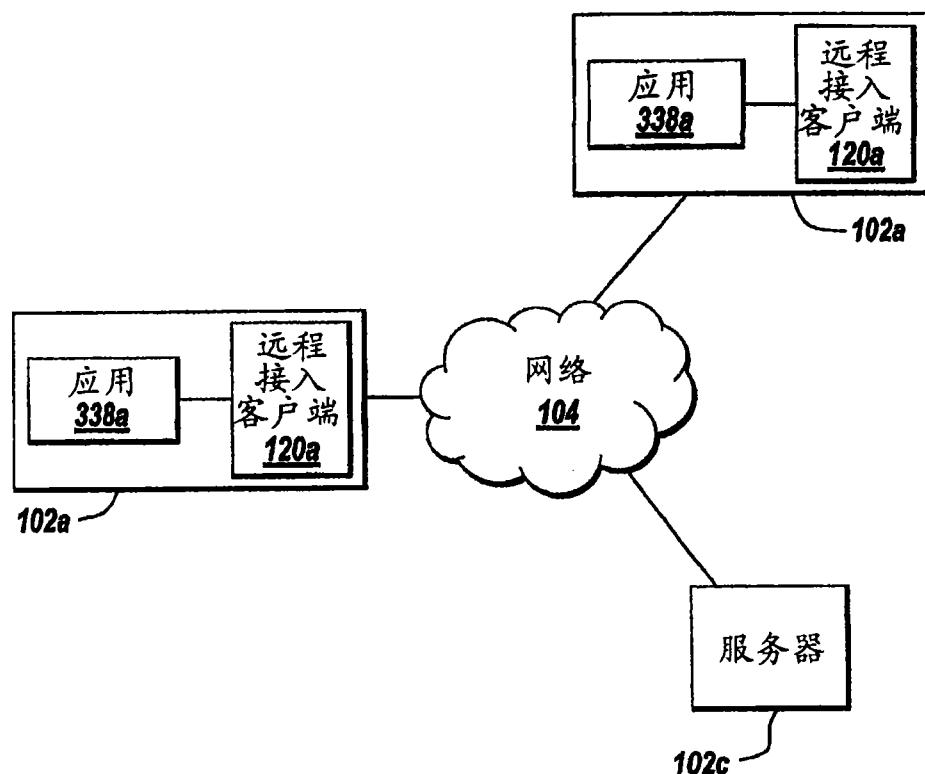


图 1B

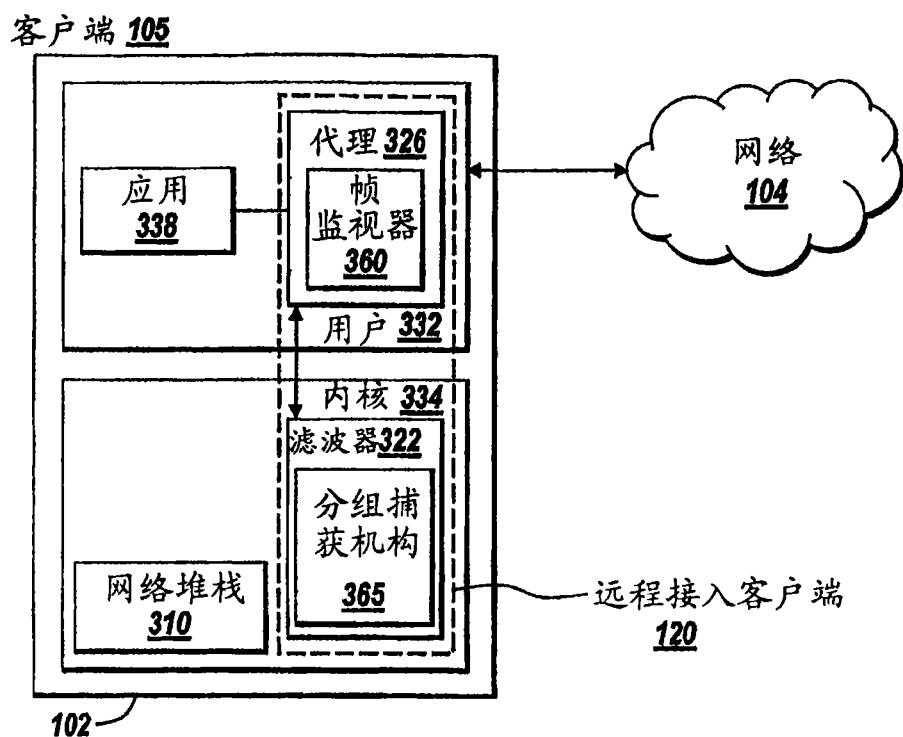


图 1C

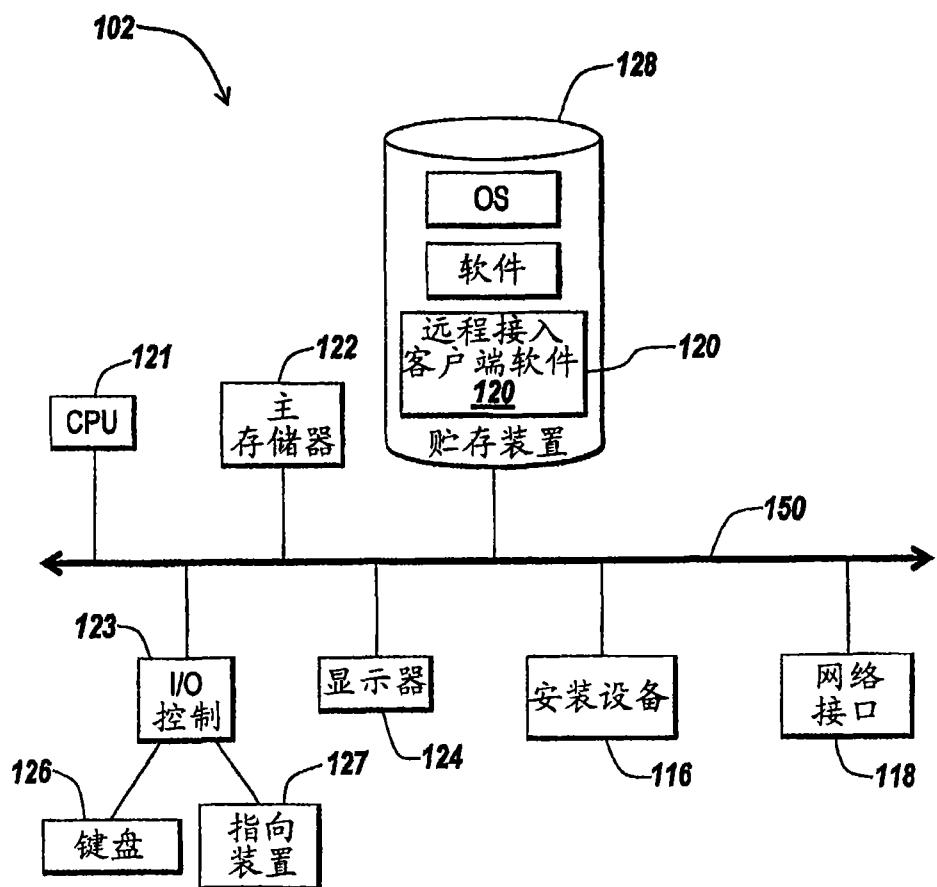


图 1D

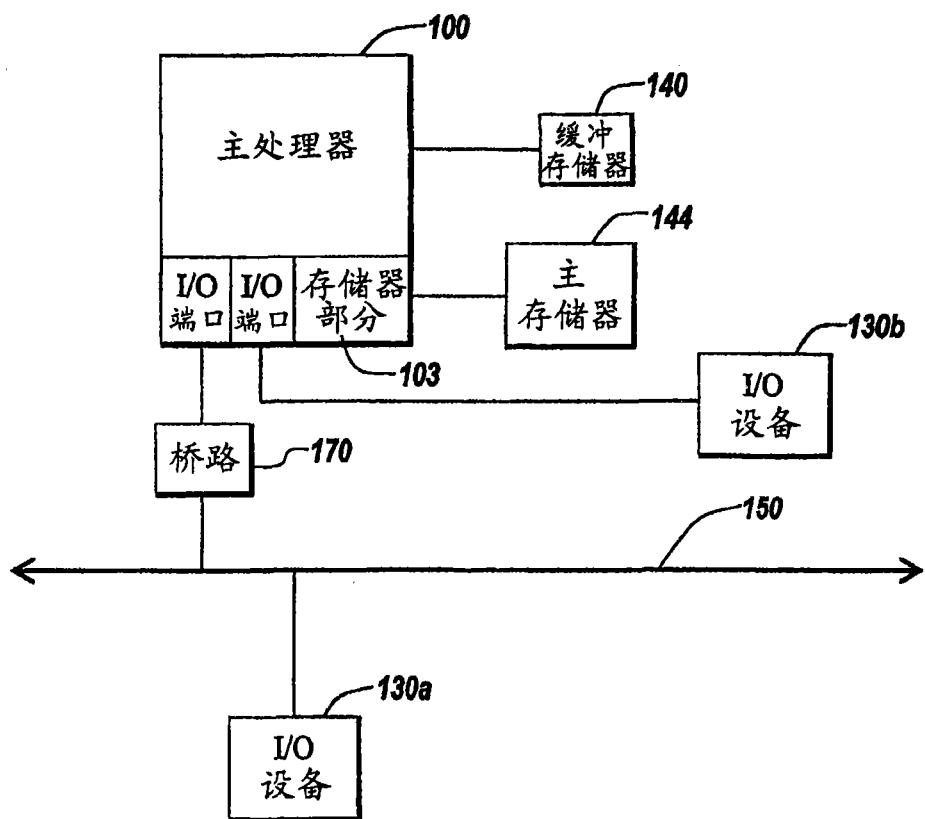


图 1E

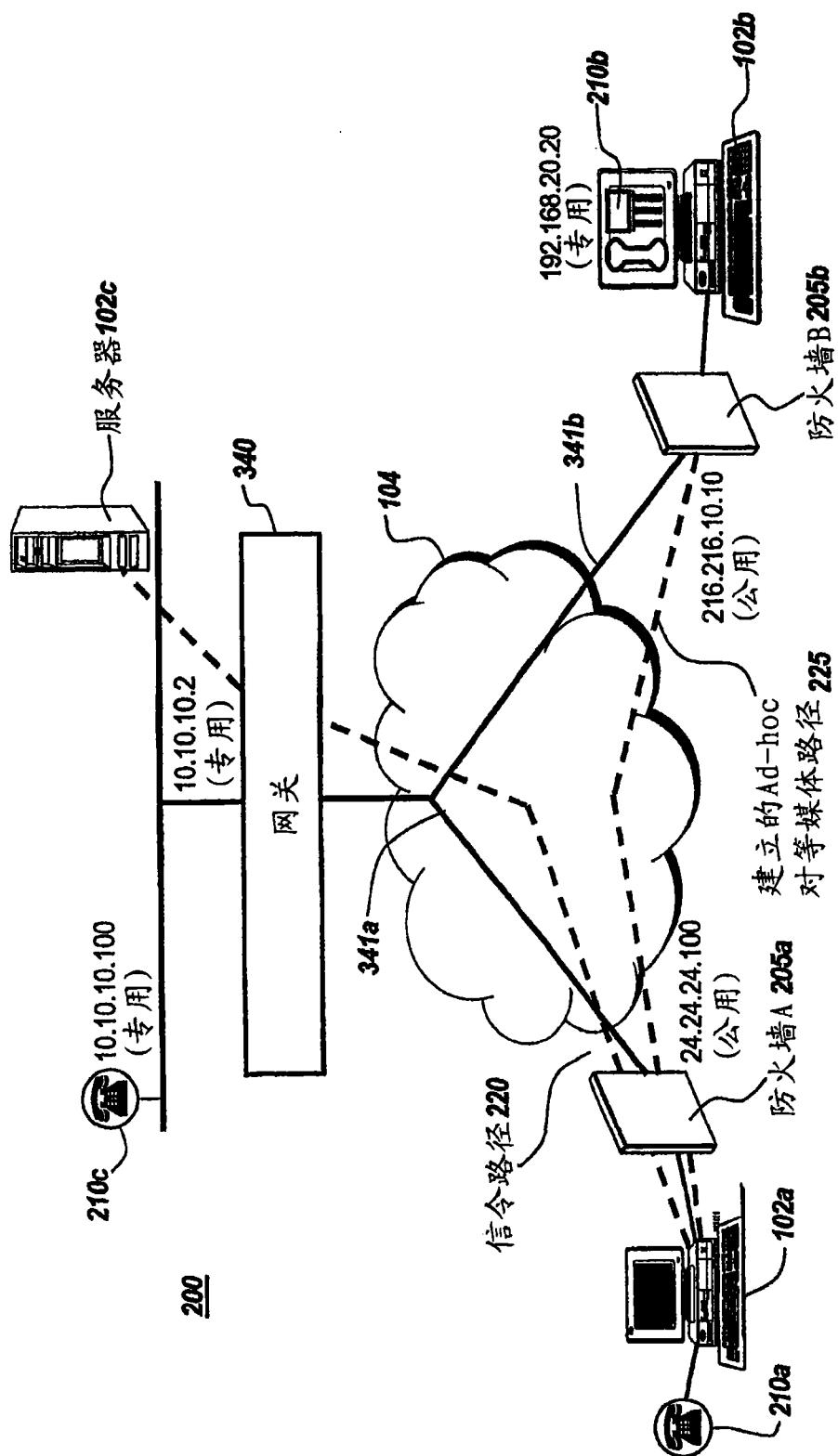


图 2A

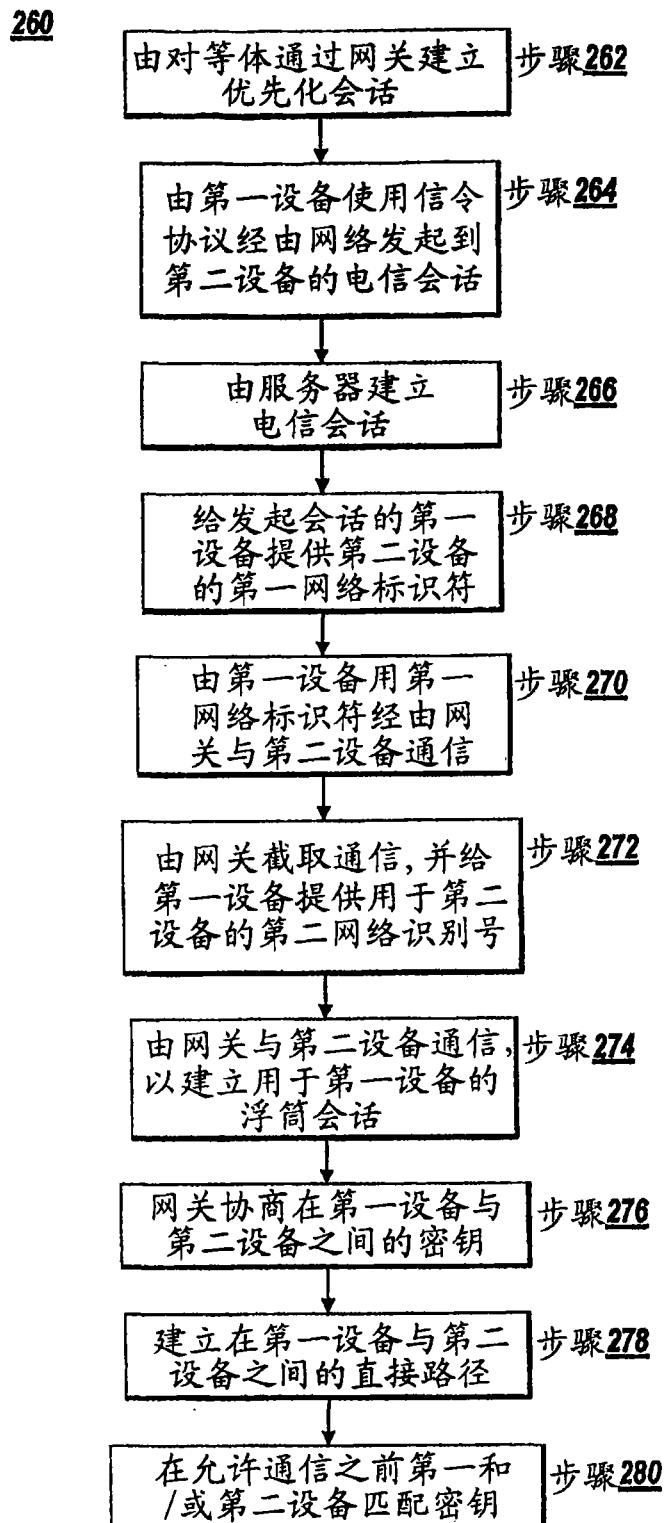


图 2B

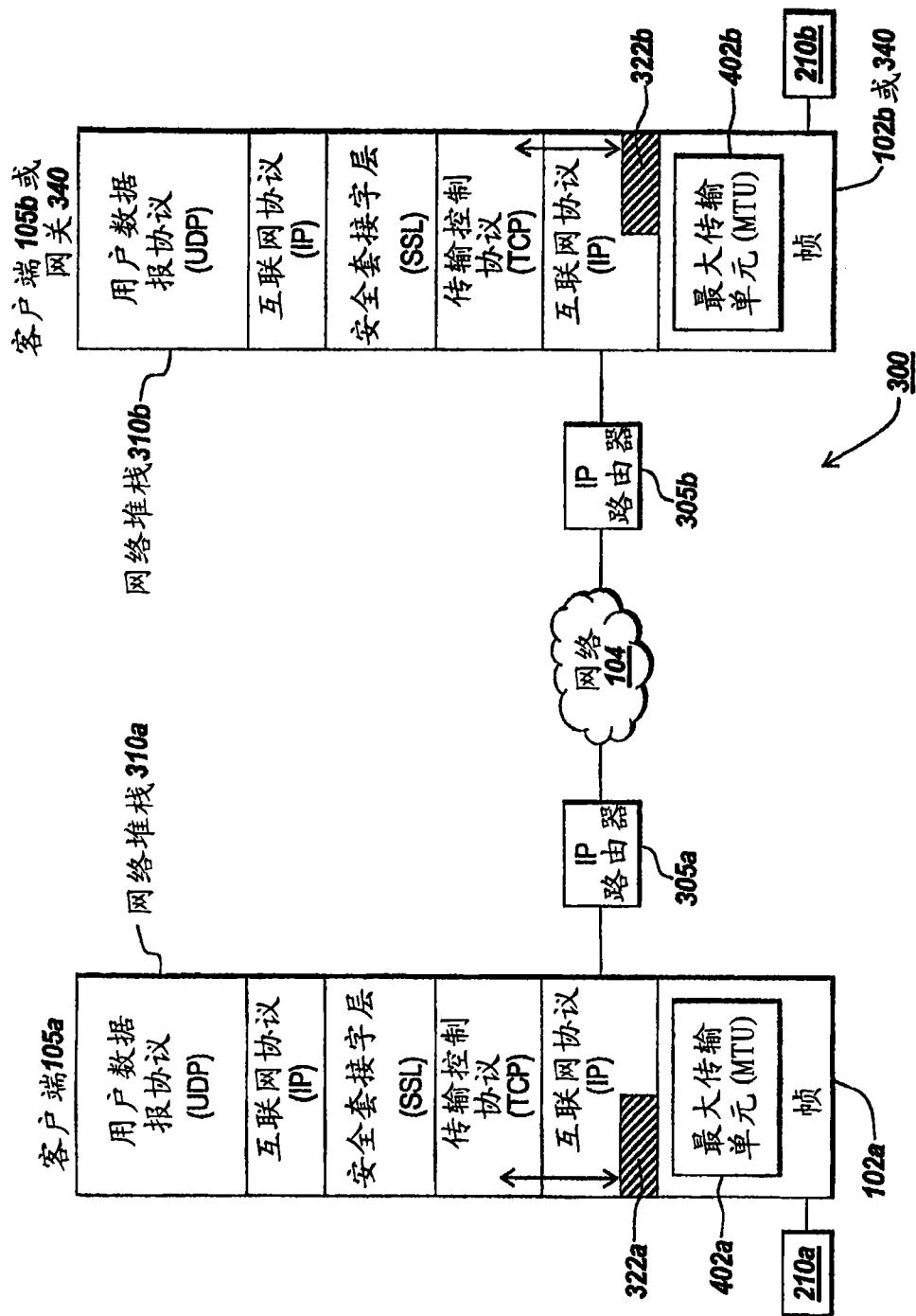


图 3A

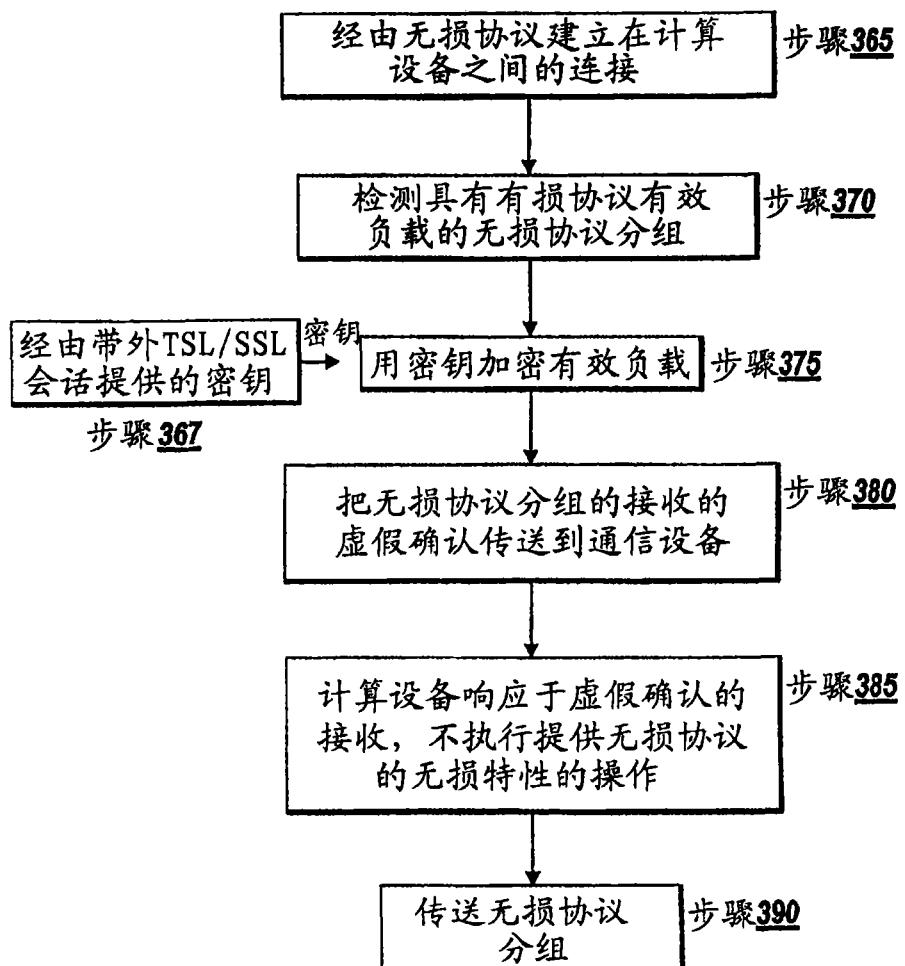


图 3B

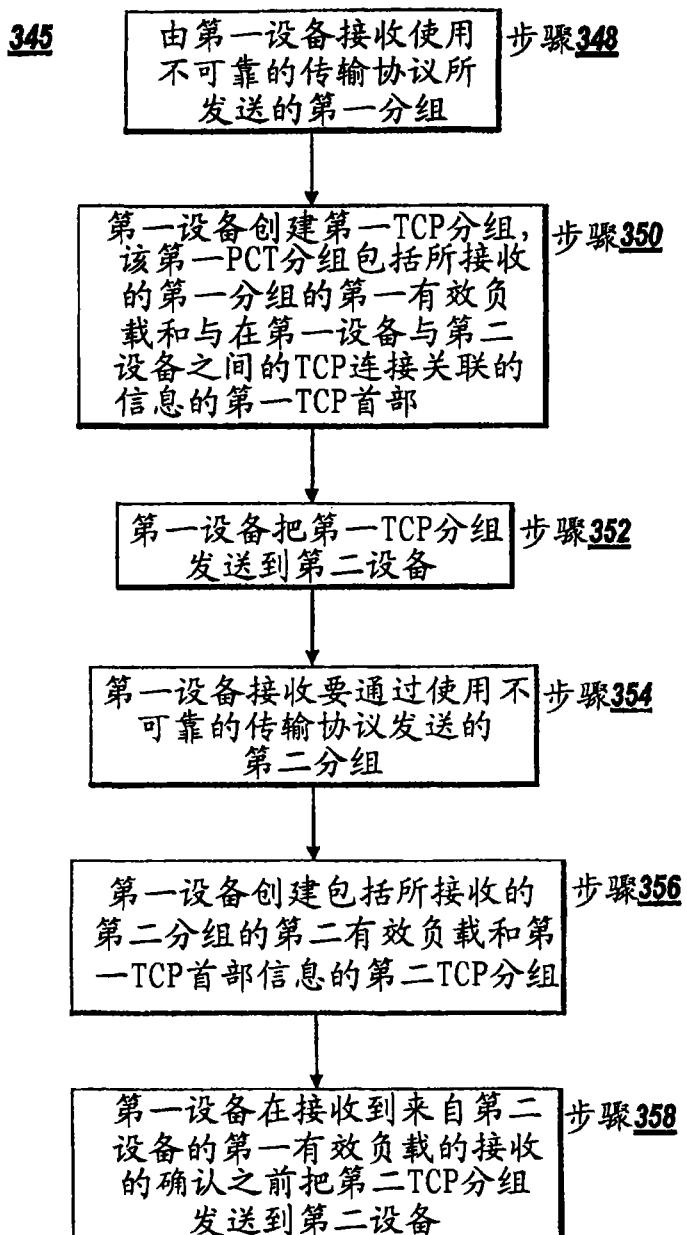


图 3C

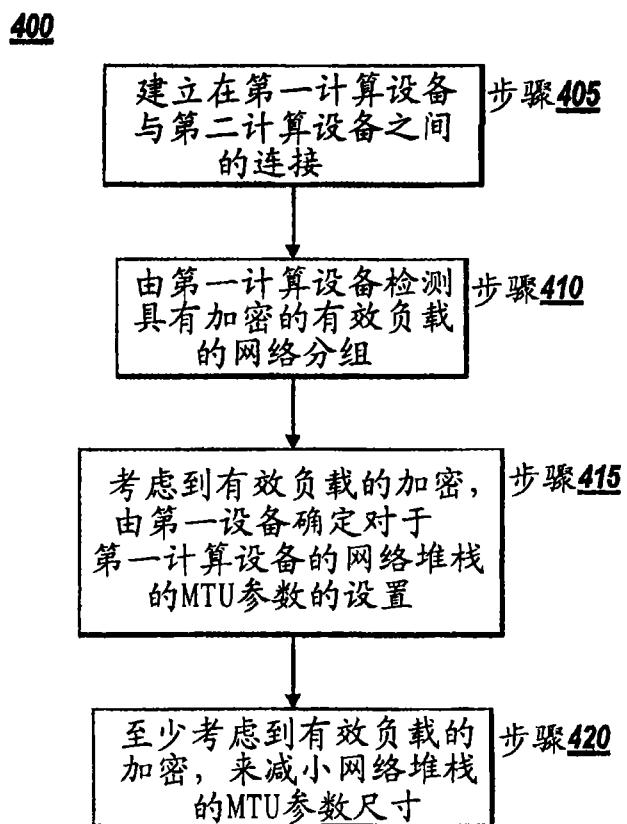


图 4

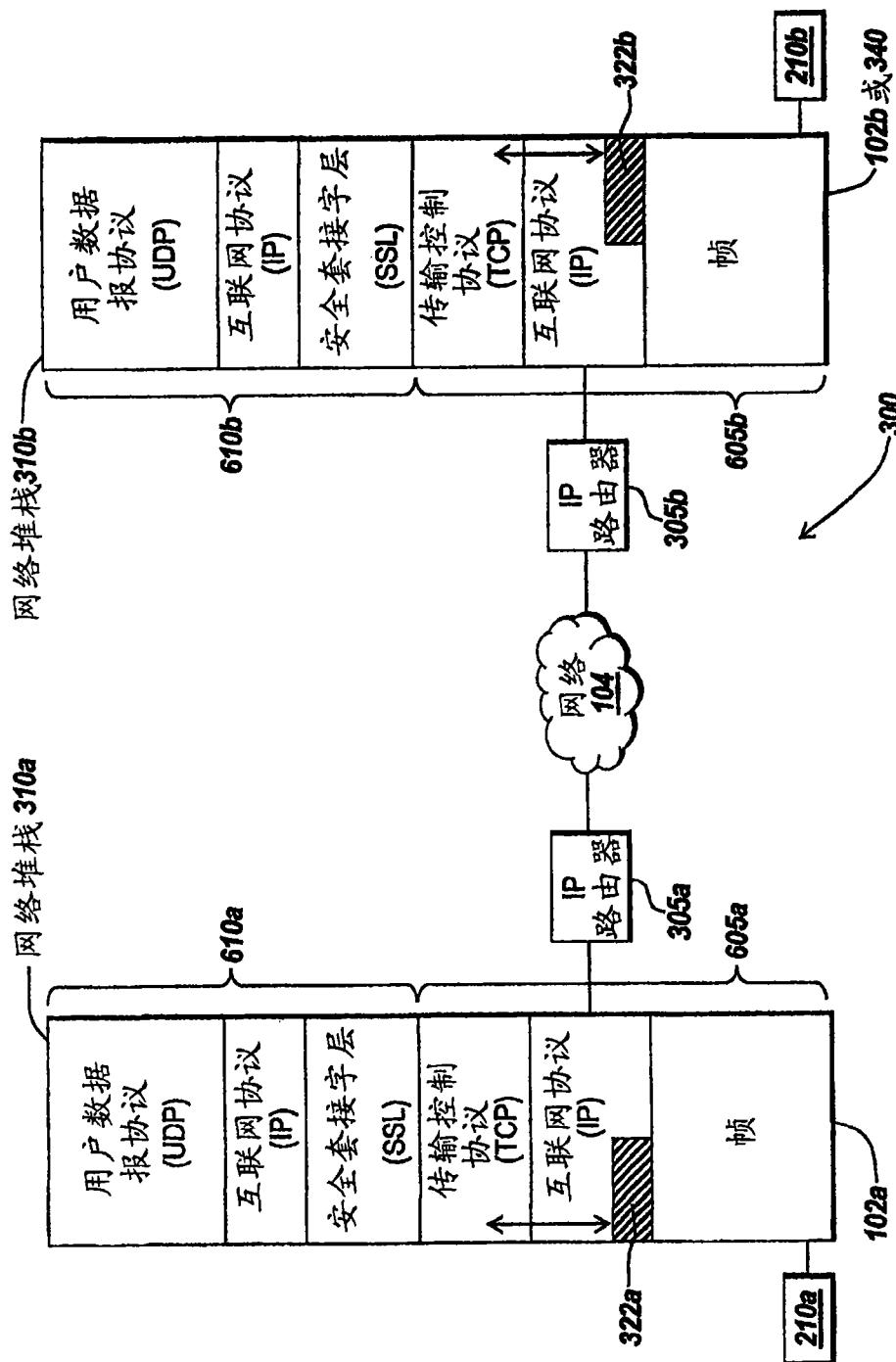


图 6A

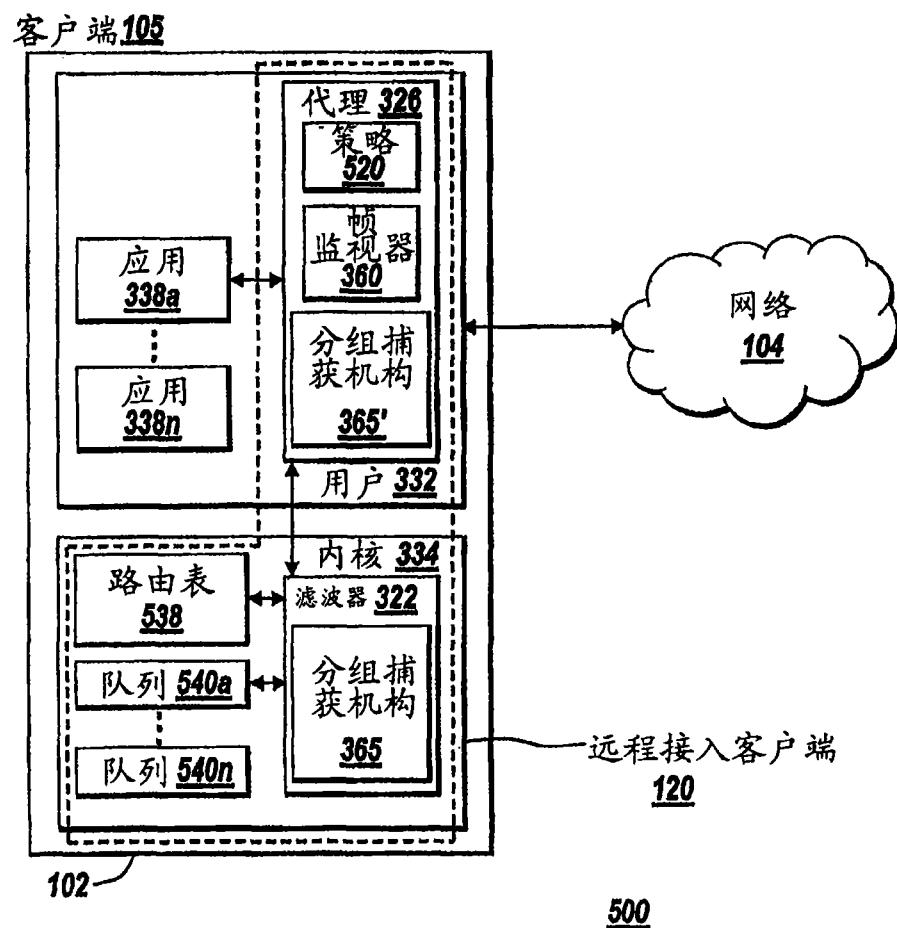


图 5A

550

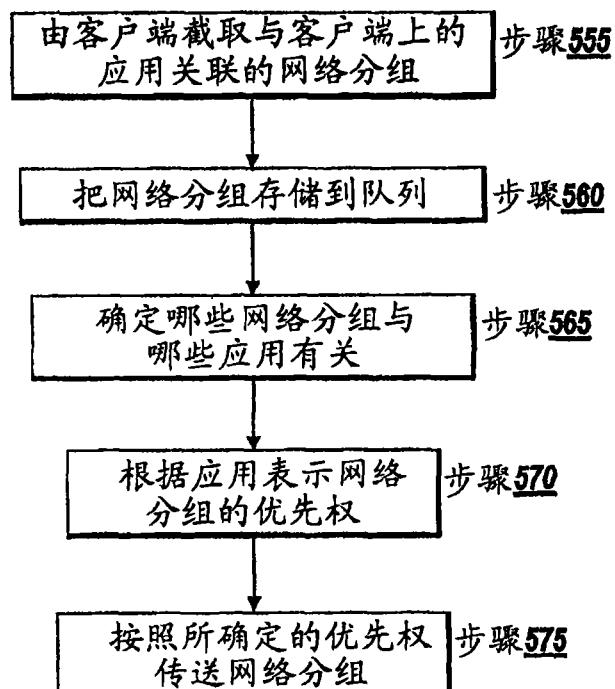


图 5B

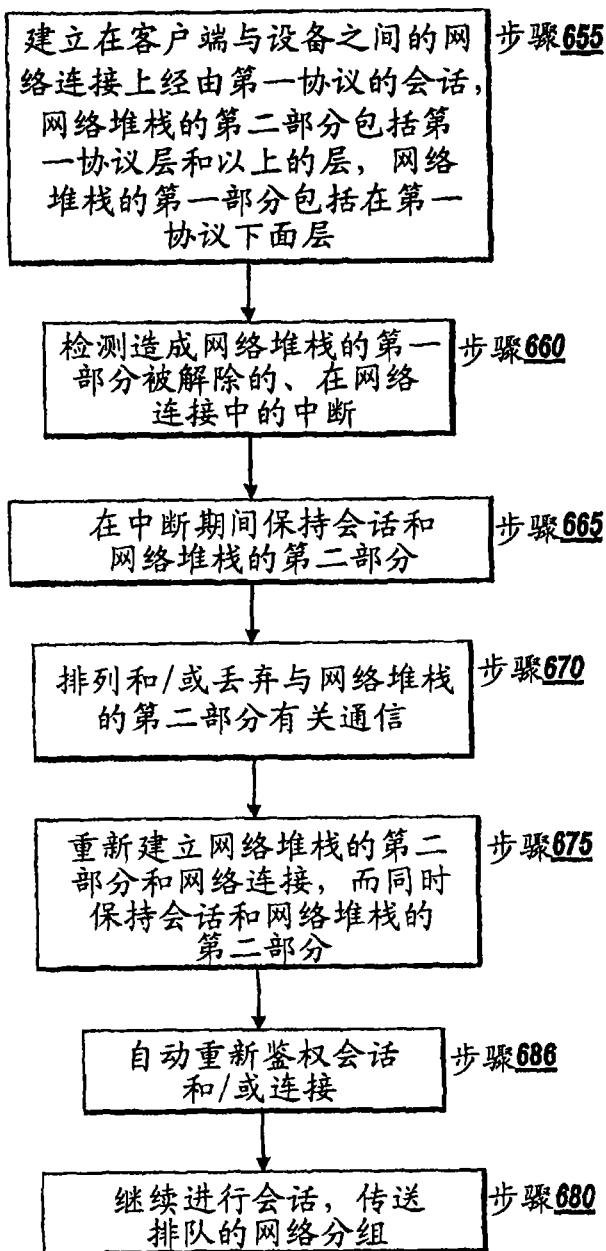
650

图 6B