

权 利 要 求

1、一种可信状态证明的方法，其特征在于，所述方法用于网络设备，所述网络设备连接于上游设备和下游网络设备之间，所述上游设备为所述网络设备的上游网络设备或证明服务器，所述方法包括：

5 对所述网络设备的第一可信证明代理进行度量以获取第一代理度量值，所述第一代理度量值用于证明所述第一可信证明代理的可信状态；

 向所述上游设备发送所述第一代理度量值；

 接收来自所述上游设备的至少一个基线值，所述至少一个基线值中的至少部分基线值用于证明所述下游网络设备的可信状态。

10 2、根据权利要求 1 所述的方法，其特征在于，所述网络设备包括与所述第一可信证明代理连接的至少一个第一待证明对象，所述方法还包括：

 获取所述至少一个第一待证明对象中每个第一待证明对象的第一度量值，所述第一度量值用于证明所述第一待证明对象的可信状态；

 所述至少一个基线值包括与所述第一待证明对象对应的第一基线值，所述接收来自所
15 述上游设备的至少一个基线值之后，所述方法还包括：

 根据所述第一待证明对象对应的所述第一基线值和所述第一度量值，证明所述第一待证明对象的可信状态。

 3、根据权利要求 2 所述的方法，其特征在于，所述获取所述第一待证明对象的第一度量值之后，所述方法还包括：

20 将所述第一度量值向所述上游设备发送。

 4、根据权利要求 1 至 3 任一项所述的方法，其特征在于，所述至少一个基线值包括第二基线值，所述第二基线值与所述下游网络设备的第二可信证明代理对应，所述接收来自所述上游设备的至少一个基线值之后，所述方法还包括：

 接收来自所述下游网络设备的第二代理度量值，所述第二代理度量值用于证明所述第
25 二可信证明代理的可信状态；

 根据所述第二基线值和所述第二代理度量值，证明所述第二可信证明代理的可信状态。

 5、根据权利要求 1 至 3 任一项所述的方法，其特征在于，所述方法还包括：

 接收来自所述下游网络设备的第二代理度量值，所述第二代理度量值用于证明所述第
30 二可信证明代理的可信状态；

 将所述第二代理度量值向所述上游设备发送。

 6、根据权利要求 1 至 5 任一项所述的方法，其特征在于，所述至少一个基线值包括第三基线值，所述第三基线值与所述下游网络设备的第二待证明对象对应，所述接收来自所述上游设备的至少一个基线值之后，所述方法还包括：

 接收来自所述下游网络设备的第二度量值，所述第二度量值用于证明所述第二待证明
35 对象的可信状态；

 根据所述第二待证明对象对应的所述第三基线值和所述第二度量值，证明所述第二待证明对象的可信状态。

7、根据权利要求 1 至 5 任一项所述的方法，其特征在于，所述至少一个基线值包括第三基线值，所述第三基线值与所述下游网络设备的第二待证明对象对应，所述接收来自所述上游设备的至少一个基线值之后，所述方法还包括：

向所述下游网络设备发送所述第三基线值。

5 8、根据权利要求 2 或 3 所述的方法，其特征在于，所述第一待证明对象和所述第一可信证明代理为两个板卡；或，所述第一待证明对象和所述第一可信证明代理为两个虚拟机；或，所述第一待证明对象和所述第一可信证明代理为虚拟机、网络功能虚拟化管理和编排系统或网络功能虚拟化基础设施层中的任意两个。

9、一种可信状态证明的方法，其特征在于，所述方法用于上游设备，所述上游设备、
10 网络设备和下游网络设备依次连接，所述上游设备为所述网络设备的上游网络设备或证明服务器，所述方法包括：

接收来自所述网络设备的第一代理度量值，所述第一代理度量值用于证明所述网络设备的第一可信证明代理的可信状态；

根据所述第一代理度量值证明所述第一可信证明代理处于可信状态；

15 向所述网络设备发送至少一个基线值，所述至少一个基线值中的至少部分基线值用于证明所述下游网络设备的可信状态。

10、根据权利要求 9 所述的方法，其特征在于，所述至少一个基线值包括与所述网络设备的第一待证明对象对应的第一基线值。

11、根据权利要求 9 或 10 所述的方法，其特征在于，所述向所述网络设备发送至少一个
20 基线值之后，所述方法还包括：

接收来自所述网络设备的第一度量值，所述第一度量值用于证明所述网络设备的第一待证明对象的可信状态；

根据所述第一待证明对象对应的第一基线值和所述第一度量值，证明所述第一待证明对象的可信状态。

25 12、根据权利要求 9 至 11 任一项所述的方法，其特征在于，所述至少一个基线值包括第二基线值，所述第二基线值与所述下游网络设备的第二可信证明代理对应。

13、根据权利要求 9 至 11 任一项所述的方法，其特征在于，所述向所述网络设备发送至少一个基线值之后，所述方法还包括：

30 接收来自所述网络设备的第二代理度量值，所述第二代理度量值用于证明所述下游网络设备的第二可信证明代理的可信状态；

根据所述第二可信证明代理对应的第二基线值和所述第二代理度量值，证明所述第二可信证明代理的可信状态。

14、根据权利要求 9 至 13 任一项所述的方法，其特征在于，所述至少一个基线值包括第三基线值，所述第三基线值与所述下游网络设备的第二待证明对象对应。

35 15、一种网络设备，其特征在于，所述网络设备连接于上游设备和下游网络设备之间，所述上游设备为所述网络设备的上游网络设备或证明服务器，所述网络设备包括第一可信证明代理，所述第一可信证明代理用于执行权利要求 1 至 8 任一项所述的可信状态证明的

方法。

16、一种上游网络设备，其特征在于，所述上游网络设备、网络设备和下游网络设备依次连接，所述上游网络设备的可信证明代理用于执行权利要求 9 至权利要求 14 任一项所述的可信状态证明的方法。

- 5 17、一种证明服务器，其特征在于，所述证明服务器、网络设备和下游网络设备依次连接，所述证明服务器包括处理器、存储器以及光收发器，其中，所述处理器通过线路分别与所述存储器以及所述光收发器互联；

所述光收发器用于接收来自所述网络设备的第一代理度量值，所述第一代理度量值用于证明所述网络设备的第一可信证明代理的可信状态；

- 10 所述处理器调用所述存储器中的程序代码用于执行如下步骤：

根据所述第一代理度量值证明所述第一可信证明代理处于可信状态；

所述光收发器还用于，向所述网络设备发送至少一个基线值，所述至少一个基线值中的至少部分基线值用于证明所述下游网络设备的可信状态。

- 15 18、一种计算机可读存储介质，其特征在于，包括指令，当所述指令在计算机上运行时，使得所述计算机执行如权利要求 1 至 14 任一项所述的可信状态证明的方法。

19、一种包含指令的计算机程序产品，其特征在于，当所述计算机程序产品在计算机上运行时，使得所述计算机执行如权利要求 1 至 14 任一项所示的可信状态证明的方法。