(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 103828299 B
(45)授权公告日 2017.04.05

(21)申请号 201280046183.X

(22)申请日 2012.10.19

(65)同一申请的已公布的文献号
申请公布号 CN 103828299 A

(43)申请公布日 2014.05.28

(30)优先权数据
61/550,344 2011.10.21 US
13/655,399 2012.10.18 US

(85)PCT国际申请进入国家阶段日
2014.03.21

(86)PCT国际申请的申请数据
PCT/US2012/061216 2012.10.19

(87)PCT国际申请的公布数据
WO2013/059744 EN 2013.04.25

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 W·G·邓兰普 B·M·门查卡
R·A·诺瓦渥斯基

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 唐杰敏

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 12/851(2006.01)
H04L 12/859(2006.01)

(56)对比文件
CN 101079779 A,2007.11.28,
CN 101088256 A,2007.12.12,
US 8370466 B2,2013.02.05,
US 2007/0033636 A1,2007.02.08,

审查员 刘万志

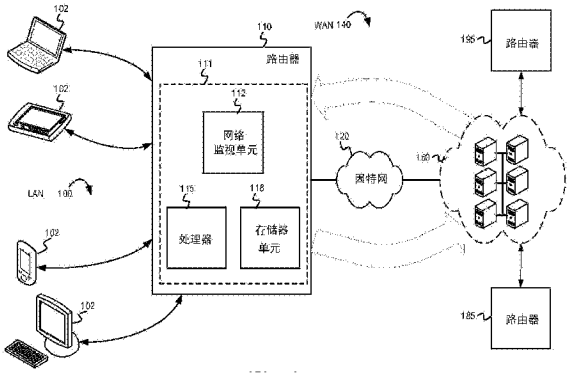
权利要求书3页 说明书12页 附图5页

(54)发明名称

用于通信网络的云计算增强网关

(57)摘要

局域网的网络话务管理节点(诸如,路由器或网关)可监视局域网的网络话务。使用网络话务管理节点来检测与局域网相关联的网络事件。从该网络话务管理节点向基于云的计算网络的一个或多个服务器报告网络事件。从基于云的计算网络接收针对网络话务管理节点的网络策略更新。网络策略更新至少部分地基于报告给基于云的计算网络的网络事件类型。在网络话务管理节点处实现网络策略更新以处理和/或解决该网络事件。



CN 103828299 B

1.一种通信方法,包括:

对在局域网LAN的网络话务管理节点处检测到的多个分组流进行分类;

在所述网络话务管理节点处检测未知分组流;

为所述未知分组流选择默认分类;

经由广域网WAN从所述网络话务管理节点向基于云的计算网络的一个或多个服务器报告与所述未知分组流相关联的信息,所述基于云的计算网络与聚集关于分组流的信息相关联,所述分组流来自与不同LAN相关联的多个网络话务管理节点;

在所述网络话务管理节点处从所述基于云的计算网络接收针对所述未知分组流的分组流检测策略更新;以及

在所述网络话务管理节点处实现所述分组流检测策略更新以供随后检测和分类所述未知分组流。

2.如权利要求1所述的方法,其特征在于,所述对在所述网络话务管理节点处检测到的所述多个分组流进行分类包括:

检测与所述多个分组流相关联的分组流特性;

至少部分地基于相应的分组流特性来确定与所述多个分组流中的至少一个分组流相关联的应用;以及

至少部分地基于与所述分组流中的每一分组流相关联的应用,对所述多个分组流中的每一分组流进行分类。

3.如权利要求1所述的方法,其特征在于,所述对在所述网络话务管理节点处检测到的所述多个分组流进行分类包括基于与所述多个分组流中的每一分组流相关联的应用以及与所述多个分组流中的每一分组流相关联的应用类型中的至少一者来对所述多个分组流进行分类。

4.如权利要求1所述的方法,其特征在于,所述在所述网络话务管理节点处检测所述未知分组流以及为所述未知分组流选择所述默认分类包括:

确定与在所述网络话务管理节点处收到的分组流相关联的应用是未知的;以及

响应于确定所述应用是未知的,为所述未知分组流选择所述默认分类。

5.如权利要求1所述的方法,其特征在于,所述在所述网络话务管理节点处检测所述未知分组流以及为所述未知分组流选择所述默认分类包括:

确定与在所述网络话务管理节点处收到的分组流相关联的应用是未知的;

确定与所述未知分组流相关联的应用类型;以及

基于与所述未知分组流相关联的所述应用类型来为所述未知分组流选择所述默认分类。

6.如权利要求1所述的方法,其特征在于,所述从所述网络话务管理节点向基于云的计算网络的一个或多个服务器报告与所述未知分组流相关联的信息包括报告与所述未知分组流相关联的分组流特性。

7.如权利要求1所述的方法,其特征在于,进一步包括除了接收所述分组流检测策略更新以外还接收指示与所述未知分组流相关联的应用以及所述未知分组流的分类的信息。

8.如权利要求1所述的方法,其特征在于,所述在所述网络话务管理节点处实现所述分组流检测策略更新以供随后检测和分类所述未知分组流包括:

根据所述分组流检测策略更新，在所述网络话务管理节点处检测与之前未知的分组流相关联的分组流特性；

根据所述分组流检测策略更新来确定与所述分组流特性相关联的应用；以及

基于与所述分组流特性相关联的所述应用来为所述之前未知的分组流选择分类。

9.一种通信方法，包括：

在基于云的计算网络的一个或多个服务器处经由广域网WAN从局域网LAN的路由器接收指示在所述路由器处检测到的所述LAN的网络事件的报告消息；

确定由所述LAN处的所述路由器所检测到的网络事件类型；

把与所述路由器所报告的所述网络事件类型相关联的数据同之前从也检测到所述网络事件类型的其它路由器收到的数据聚集在一起；

分析与所述网络事件类型相关联的聚集数据；

基于分析与所述网络事件类型相关联的所述聚集数据的结果，确定与所述网络事件类型相关联的网络策略更新；以及

向所述LAN的所述路由器发送所述网络策略更新以用与所述网络事件类型相关联的所述网络策略更新来配置所述路由器。

10.如权利要求9所述的方法，其特征在于，所述确定由所述LAN处的所述路由器所检测到的所述网络事件类型包括确定所述网络事件类型是所述LAN处的过度订阅事件、所述路由器处检测到未知分组流、收到来自所述路由器的网络分析报告，以及检测到所述LAN处的网络故障事件中的一者。

11.如权利要求9所述的方法，其特征在于，进一步包括基于分析与所述网络事件类型相关联的所述聚集数据的结果来向所述LAN的所述路由器发送指令以请求在所述路由器处对内容的临时存储。

12.如权利要求9所述的方法，其特征在于，所述基于分析与所述网络事件类型相关联的所述聚集数据的结果来确定与所述网络事件类型相关联的网络策略更新包括确定用于处理和解决在所述路由器处检测到的所述网络事件类型的网络策略更新。

13.一种网络路由器，包括：

处理器；以及

网络监视单元，其与所述处理器耦合并配置成：

对在局域网LAN的所述网络路由器处检测到的多个分组流进行分类；

检测在所述网络路由器处收到的未知分组流；

为所述未知分组流选择默认分类；

经由广域网WAN向基于云的计算网络的一个或多个服务器报告与所述未知分组流相关联的信息，所述基于云的计算网络与聚集关于分组流的信息相关联，所述分组流来自与不同LAN相关联的多个网络话务管理节点；

从所述基于云的计算网络接收针对所述未知分组流的分组流检测策略更新；以及

在所述网络路由器处实现所述分组流检测策略更新以供随后检测和分类所述未知分组流。

14.如权利要求13所述的网络路由器，其特征在于，所述网络监视单元被配置成对在所述网络路由器处检测到的所述多个分组流进行分类包括所述网络监视单元被配置成：

检测与所述多个分组流相关联的分组流特性；

至少部分地基于相应的分组流特性来确定与所述多个分组流中的至少一个分组流相关联的应用；以及

至少部分地基于与所述分组流中的每一分组流相关联的应用来对所述多个分组流中的每一分组流进行分类。

15.如权利要求13所述的网络路由器，其特征在于，所述网络监视单元被配置成对在所述网络路由器处检测到的所述多个分组流进行分类包括所述网络监视单元被配置成：基于与所述多个分组流中的每一分组流相关联的应用以及与所述多个分组流中的每一分组流相关联的应用类型中的至少一者来对所述多个分组流进行分类。

16.如权利要求13所述的网络路由器，其特征在于，所述网络监视单元被配置成在所述网络路由器处检测所述未知分组流以及为所述未知分组流选择所述默认分类包括所述网络监视单元被配置成：

确定与在所述网络路由器处收到的分组流相关联的应用是未知的；以及

响应于确定所述应用是未知的，为所述未知分组流选择所述默认分类。

17.如权利要求13所述的网络路由器，其特征在于，所述网络监视单元被配置成在所述网络路由器处检测所述未知分组流以及为所述未知分组流选择所述默认分类包括所述网络监视单元被配置成：

确定与在所述网络路由器处收到的分组流相关联的应用是未知的；

确定与所述未知分组流相关联的应用类型；以及

基于与所述未知分组流相关联的所述应用类型来为所述未知分组流选择所述默认分类。

18.如权利要求13所述的网络路由器，其特征在于，所述网络监视单元被配置成向基于云的计算网络的一个或多个服务器报告与所述未知分组流相关联的信息包括所述网络监视单元被配置成：报告与所述未知分组流相关联的分组流特性。

19.如权利要求13所述的网络路由器，其特征在于，所述网络监视单元被配置成在所述网络路由器处实现所述分组流检测策略更新以供随后检测和分类所述未知分组流包括所述网络监视单元被配置成：

根据所述分组流检测策略更新，检测与之前未知的分组流相关联的分组流特性；

根据所述分组流检测策略更新来确定与所述分组流特性相关联的应用；以及

基于与所述分组流特性相关联的应用来为所述之前未知的分组流选择分类。

用于通信网络的云计算增强网关

[0001] 相关申请

[0002] 本申请要求2011年10月21日提交的美国临时申请S/N.61/550,344和2012年10月18日提交的美国申请S/N.13/655,399的优先权权益。

[0003] 背景

[0004] 本发明主题的各实施例一般涉及通信网络领域，尤其涉及用于通信网络的云计算增强网关。

[0005] 局域网(LAN)(诸如家庭或办公室网络)通常包括将LAN连接至广域网(WAN)并在这两个网络之间路由分组的路由器(或网关)。LAN中的各种网络设备可经由路由器从因特网访问并下载信息，并且路由器可管理来自访问因特网的不同网络设备的各种分组流。LAN的路由器还可提供各种网络管理员选项以用于配置和定制路由器的操作。但是，网络管理员通常不得不基于为网络管理员所知晓的与网络话务和网络状况有关的有限信息来手动配置路由器。

[0006] 概述

[0007] 在一些实施例中，一种方法包括：监视局域网(LAN)的网络话务；检测与该LAN相关联的网络事件；向基于云的计算网络的一个或多个服务器报告该网络事件；从该基于云的计算网络的一个或多个服务器接收针对该LAN的网络策略更新，其中该网络策略更新至少部分地基于报告给该基于云的计算网络的一个或多个服务器的网络事件类型；以及在该LAN处实现该网络策略更新。

[0008] 在一些实施例中，所述监视、检测、报告、接收以及实现是由该LAN的网络话务管理节点执行的。

[0009] 在一些实施例中，该网络话务管理节点包括该LAN的路由器。

[0010] 在一些实施例中，该网络话务管理节点包括计算机系统，该计算机系统包括该LAN的路由器、接入点、电缆调制解调器和网络交换机中的一者或多者。

[0011] 在一些实施例中，所述检测与该LAN相关联的网络事件包括以下至少一者：检测该LAN处的过度订阅事件、检测该LAN处的未知分组流、以及检测该LAN处的网络故障事件。

[0012] 在一些实施例中，所述实现该网络策略更新包括在配置该LAN的网络话务管理节点之后实现该网络策略更新以处理和解决该网络事件。

[0013] 在一些实施例中，所述监视该LAN的网络话务包括监视从该LAN的多个网络设备中的一个或多个发送到广域网的网络话务，以及监视从该广域网的远程网络节点发送到该LAN的该多个网络设备中的一个或多个的网络话务。

[0014] 在一些实施例中，其中从该基于云的计算网络的一个或多个服务器收到的该网络策略更新基于报告给该基于云的计算网络的一个或多个服务器的网络事件类型并且基于对在该基于云的计算网络处从多个附加的局域网收集的与该网络事件类型相关联的聚集数据的分析。

[0015] 在一些实施例中，进一步包括检测与该LAN相关联的网络活动；向基于云的计算网络的一个或多个服务器报告与该LAN相关联的网络活动；以及在该LAN处从该基于云的计算

网络接收网络警报。

[0016] 在一些实施例中，一种方法包括：对在局域网(LAN)的网络话务管理节点处检测到的多个分组流进行分类；在该网络话务管理节点处检测未知分组流；为该未知分组流选择默认分类；从该网络话务管理节点向基于云的计算网络的一个或多个服务器报告与该未知分组流相关联的信息；在该网络话务管理节点处从该基于云的计算网络接收针对该未知分组流的分组流检测策略更新；以及在该网络话务管理节点处实现该分组流检测策略更新以供随后检测和分类该未知分组流。

[0017] 在一些实施例中，所述对在网络话务管理节点处检测到的多个分组流进行分类包括检测与该多个分组流相关联的分组流特性；至少部分地基于相应的分组流特性来确定与该多个分组流中的每一分组流相关联的应用；以及至少部分地基于与每一分组流相关联的应用，对该多个分组流中的每一分组流进行分类。

[0018] 在一些实施例中，所述对在网络话务管理节点处检测到的多个分组流进行分类包括基于与该多个分组流中的每一分组流相关联的应用以及与该多个分组流中的每一分组流相关联的应用类型中的至少一者来对该多个分组流进行分类。

[0019] 在一些实施例中，所述在网络话务管理节点处检测未知分组流以及为该未知分组流选择默认分类包括确定与在该网络话务管理节点处接收到的分组流相关联的应用是未知的；以及响应于确定该应用是未知的，为该未知分组流选择默认分类。

[0020] 在一些实施例中，其中所述在网络话务管理节点处检测未知分组流以及为该未知分组流选择默认分类包括确定与在该网络话务管理节点处接收到的分组流相关联的应用是未知的；确定与该未知分组流相关联的应用类型；以及基于与该未知分组流相关联的应用类型来为该未知分组流选择默认分类。

[0021] 在一些实施例中，所述从该网络话务管理节点向基于云的计算网络的一个或多个服务器报告与该未知分组流相关联的信息包括报告与该未知分组流相关联的分组流特性。

[0022] 在一些实施例中，所述方法进一步包括除了接收分组流检测策略更新以外还接收指示与未知分组流相关联的应用以及未知分组流的分类的信息。

[0023] 在一些实施例中，所述在该网络话务管理节点处实现该分组流检测策略更新以供随后检测和分类该未知分组流包括根据该分组流检测策略更新，在该网络话务管理节点处检测与之前未知的分组流相关联的分组流特性；根据该分组流检测策略更新来确定与该分组流特性相关联的应用；以及基于与该分组流特性相关联的应用来为该之前未知的分组流选择分类。

[0024] 在一些实施例中，一种方法包括：在基于云的计算网络的一个或多个服务器处从局域网(LAN)的路由器接收指示在该路由器处检测到的网络事件的报告消息；确定由该LAN处的该路由器所检测到的网络事件类型；把与该路由器所报告的网络事件类型相关联的数据与之前从也检测到该网络事件类型的其它路由器接收到的数据聚集在一起；分析与该网络事件类型相关联的聚集数据；基于对与该网络事件类型相关联的聚集数据的分析的结果，确定与该网络事件类型相关联的网络策略更新；以及向该LAN的该路由器发送该网络策略更新以用与该网络事件类型相关联的网络策略更新来配置该路由器。

[0025] 在一些实施例中，所述确定由该LAN处的该路由器所检测到的网络事件类型包括确定该网络事件类型是该LAN处的过度订阅事件、在该路由器处检测到未知分组流、收到来

自该路由器的网络分析报告、以及检测到该LAN处的网络故障事件中的一者。

[0026] 在一些实施例中，该方法进一步包括基于对与该网络事件类型相关联的聚集数据的分析的结果来向该LAN的该路由器发送指令以请求在该路由器处对内容的临时存储。

[0027] 在一些实施例中，所述基于对与该网络事件类型相关联的聚集数据的分析的结果来确定与该网络事件类型相关联的网络策略更新包括确定用于处理和解决在该路由器处检测到的该网络事件类型的网络策略更新。

[0028] 在一些实施例中，一种网络路由器包括一个或多个处理器；以及配置成存储一条或多条指令的一个或多个存储器单元，所述指令在由该一个或多个处理器执行时使所述网络路由器执行包括以下的操作：监视局域网(LAN)的网络话务；检测与该LAN相关联的网络事件；向基于云的计算网络的一个或多个服务器报告该网络事件；从该基于云的计算网络的一个或多个服务器接收针对该网络路由器的网络策略更新，其中该网络策略更新至少部分地基于报告给该基于云的计算网络的一个或多个服务器的网络事件类型；以及在该网络路由器处实现该网络策略更新。

[0029] 在一些实施例中，与该LAN相关联的网络事件包括该LAN处的过度订阅事件、该网络路由器处收到的未知分组流、以及该LAN处的网络故障事件中的一者。

[0030] 在一些实施例中，由该一个或多个处理器执行的一条或多条指令使所述网络路由器执行进一步包括以下的操作：在配置该网络路由器之后通过实现该网络策略更新来处理和解决该网络事件。

[0031] 在一些实施例中，由该一个或多个处理器执行的一条或多条指令使所述网络路由器执行进一步包括以下的操作：检测与该LAN相关联的网络活动；向基于云的计算网络的一个或多个服务器报告与该LAN相关联的网络活动；以及在该网络路由器处从该基于云的计算网络接收网络警报。

[0032] 在一些实施例中，一种网络路由器包括处理器；以及网络监视单元，该网络监视单元耦合至该处理器并配置成：对在局域网(LAN)的网络路由器处检测到的多个分组流进行分类；检测在该网络路由器处收到的未知分组流；为该未知分组流选择默认分类；向基于云的计算网络的一个或多个服务器报告与该未知分组流相关联的信息；从该基于云的计算网络接收针对该未知分组流的分组流检测策略更新；以及在该网络路由器处实现该分组流检测策略更新以供随后检测和分类该未知分组流。

[0033] 在一些实施例中，该网络监视单元被配置成对在该网络路由器处检测到的多个分组流进行分类包括该网络监视单元被配置成：检测与该多个分组流相关联的分组流特性；至少部分地基于相应的分组流特性来确定与该多个分组流中的每一分组流相关联的应用；以及至少部分地基于与每一分组流相关联的应用来对该多个分组流中的每一分组流进行分类。

[0034] 在一些实施例中，该网络监视单元被配置成对在该网络路由器处检测到的多个分组流进行分类包括该网络监视单元被配置成：基于与该多个分组流中的每一分组流相关联的应用以及与该多个分组流中的每一分组流相关联的应用类型中的至少一者来对该多个分组流进行分类。

[0035] 在一些实施例中，该网络监视单元被配置成在网络话务管理节点处检测未知分组流以及为该未知分组流选择默认分类包括该网络监视单元被配置成：确定与在该网络路由

器处收到的分组流相关联的应用是未知的；以及响应于确定该应用是未知的，为该未知分组流选择默认分类。

[0036] 在一些实施例中，该网络监视单元被配置成在网络路由器处检测未知分组流以及为该未知分组流选择默认分类包括该网络监视单元被配置成：确定与在该网络路由器处收到的分组流相关联的应用是未知的；确定与该未知分组流相关联的应用类型；以及基于与该未知分组流相关联的应用类型来为该未知分组流选择默认分类。

[0037] 在一些实施例中，该网络监视单元被配置成向基于云的计算网络的一个或多个服务器报告与该未知分组流相关联的信息包括该网络监视单元被配置成：报告与该未知分组流相关联的分组流特性。

[0038] 在一些实施例中，该网络监视单元被配置成在该网络路由器处实现该分组流检测策略更新以供随后检测和分类该未知分组流包括该网络监视单元被配置成：根据该分组流检测策略更新，检测与之前未知的分组流相关联的分组流特性；根据该分组流检测策略更新来确定与该分组流特性相关联的应用；以及基于与该分组流特性相关联的应用来为该之前未知的分组流选择分类。

[0039] 在一些实施例中，一种或多种其中存储有指令的机器可读存储介质，这些指令在由一个或多个处理器执行时使这一个或多个处理器执行包括以下的操作：对在局域网(LAN)处检测到的多个分组流进行分类；在该LAN处检测未知分组流；为该未知分组流选择默认分类；向基于云的计算网络的一个或多个服务器报告与该未知分组流相关联的信息；从该基于云的计算网络接收针对该未知分组流的分组流检测策略更新；以及实现该分组流检测策略更新以供随后检测和分类该未知分组流。

[0040] 在一些实施例中，所述对在该LAN处检测到的多个分组流进行分类的操作包括基于与该多个分组流中的每一分组流相关联的应用以及与该多个分组流中的每一分组流相关联的应用类型中的至少一者来对该多个分组流进行分类。

[0041] 在一些实施例中，所述检测未知分组流以及为该未知分组流选择默认分类的操作包括确定与在该LAN处收到的分组流相关联的应用是未知的；以及响应于确定该应用是未知的，为该未知分组流选择默认分类。

[0042] 在一些实施例中，所述检测未知分组流以及为该未知分组流选择默认分类的操作包括确定与在该LAN处收到的分组流相关联的应用是未知的；确定与该未知分组流相关联的应用类型；以及基于与该未知分组流相关联的应用类型来为该未知分组流选择默认分类。

[0043] 附图简述

[0044] 通过参考附图，可以更好地理解本发明的诸实施例并使众多目的、特征和优点为本领域技术人员所显见。

[0045] 图1是根据一些实施例的解说用于通信网络的云计算增强路由器的示例框图；

[0046] 图2是根据一些实施例的解说用于实现图1中所示的用于局域网的云计算增强路由器的示例操作的流程图；

[0047] 图3是根据一些实施例的解说用于实现图1中所示的云计算增强路由器系统的示例操作的流程图；

[0048] 图4是根据一些实施例的解说用于在图1-3中所述的云计算增强路由器中实现分

组流检测的示例操作的流程图;以及

[0049] 图5是根据一些实施例的网络设备的一个实施例的框图,该网络设备包括用于局域网路由、监视和基于云的支持的机制。

[0050] 实施例描述

[0051] 以下描述包括体现本发明主题的技术的示例性系统、方法、技术、指令序列、以及计算机程序产品。然而应理解,所描述的实施例在没有这些具体细节的情况下也可实践。例如,虽然诸示例述及在家庭局域网(LAN)中利用云计算增强路由器,但是在其它示例中,云计算增强路由器可用于任何适合类型的网络,诸如办公室网络、多住宅式网络、大学网络,等等。在其他实例中,公知的指令实例、协议、结构和技术未被详细示出以免淡化本描述。

[0052] 用于通信网络的路由器(或网关)正变得日益复杂。同时,竞争正敦促减少路由器的成本。结果,从性能观点以及特征观点两者而言,家庭LAN路由器中的处理能力如今都不足以利用将增强路由器能力的复杂算法。此外,所有路由器固有地具有有限量的可用资源,诸如处理能力、存储、软件以及其它特征。

[0053] 图1是根据一些实施例的解说用于通信网络的云计算增强路由器的示例框图。LAN100包括多个网络设备102和路由器110。多个网络设备102可包括各种类型的有线和无线联网设备,诸如,笔记本计算机、平板计算机、移动电话、台式计算机、数码相机、电视、游戏控制台、智能电器以及其他合适的设备。路由器110(或网关)是通信网络中从通信网络接收分组并向通信网络路由分组的节点。路由器110是两个或更多个网络之间的网络话务管理节点,其接收、处理并路由与这些网络相关联的分组。然而应注意,在其他实施例中,LAN100可包括其它类型的网络话务管理节点和/或配置成执行(诸)网络的各种功能的网络话务管理节点,例如,纳入了电缆调制解调器、网关/路由器、无线接入点、桥接器、交换机和/或存储中的一者或多者的服务器计算机系统,其也可实现本文参考图1-5所描述的功能性。如图1中所示,路由器110允许LAN100的网络设备102接入WAN140并从WAN140接收内容。LAN100是形成WAN140的许多LAN中的一个,WAN140一般可被称作因特网120。如图所示,WAN140还可包括各种服务器网络(以及其他网络设备和软件)。在一个示例中,服务器网络可实现因特网120上的云计算,其在本文中将被称作云计算网络150(或云150)。路由器110可允许LAN100经由因特网120获得由云150所提供的各种服务的益处。服务其它LAN的各种其它路由器(例如,路由器185和195)也可连接至云150。由于所有路由器皆连接至因特网,因而使用在云150处可用的云计算资源来扩增路由器可导致更加复杂的路由器并且还可减少路由器的成本。

[0054] 云150可被配置成使用众包概念从连接至因特网120的各种路由器收集统计量以及完善在路由器中运行的网络管理算法,这可导致利用连接至云150的所有其他路由器的经验的更智能的“学习”路由器。在一些实施例中,路由器110(以及还有诸如路由器185和195之类的各种路由器)可向云150报告各种类型的网络事件、统计信息以及其它网络活动例如,如下文将进一步描述的,路由器110可报告与在该路由器处收到的未知分组流相关联的信息,以及LAN100中被该路由器检测到的过度订阅事件。云150可聚集与由各种路由器所报告的网络事件相关联的数据并且分析该数据以改进和更新路由器策略及规程(例如,更新存储在路由器处的网络管理算法)。路由器110还可向云150发送网络活动报告以允许云对LAN100执行网络分析并向路由器发送网络警报。路由器110除了报告网络活动以外,路由

器110还可利用云150处的存储。云150可监视网络活动和存储利用以使服务个性化并且可为LAN100及LAN100的用户提供建议(例如,在非高峰夜间小时期间执行公共文件和软件下载)。

[0055] 在某些实现中,路由器110可被配置成智能地检测生成并处理通过路由器110去往和来自WAN140的分组流的应用。例如,路由器110可检测来自(例如,在第一网络设备102中实现的)Netflix®视频流送应用的分组流和来自通过路由器110活跃地发送分组的文件下载应用(例如,在第二网络设备102中实现的比特洪流(bit torrent))的分组流。在某些示例中,提供视频流送服务(或其它内容)的服务器可经由路由器110向LAN100以及向在诸网络设备102之一处正被执行的客户端应用流送视频内容。然而,在某些情况下,路由器110可检测到未知分组流,或确定分组流为不可识别。在其它情况下,带有已知流"指纹"或流特性的已知应用可改变其产生的分组流(即,改变流特性),这可使之前可检测的分组流变为不可检测。在一种实现中,路由器110可被配置成向云计算网络150的一个或多个服务器发送与所有未知分组流有关的信息(例如,流特性)。云150可访问已经从各种其它路由器收集的与未知分组流有关的相关聚集数据。基于执行分组检查和/或对相关聚集数据的统计分析,并且还基于连续地监视来自因特网120上的各种服务提供者的分组流,云150可智能地标识未知分组流。随后,云150可下载新检测规则到路由器110(并且还可下载到其它路由器,诸如路由器185和195)。

[0056] 在一些实现中,路由器110可配置有用以检测经由因特网发送的最常见的应用分组流(例如,头100个应用)的算法。通过路由器100的任何其他未知分组流可被发送到云150以用于检测和标识。在一个示例中,在未知分组信息被发送到云150以供进一步分析之后,路由器110可临时向未知分组流指派默认分类。例如,虽然路由器110可能不能检测与分组流相关联的具体应用,但是路由器110可确定分组流是流送视频并且可临时指派关于视频话务的默认分类。换言之,即使路由器110可能不能检测具体应用,路由器110也可检测应用类型(例如,视频话务)并基于该应用类型来为未知分组流选择默认分类。在云150确定新检测规则之后,结果可发回到路由器110,并且路由器110可实现该新检测规则以适当地标识和处理分组流。这创建了自反馈环路,其中路由器110运行检测算法,收集发送到云150的统计量,来自各种路由器的统计量在云150处被聚集和分析,并且新检测算法随后被确定并且被发出到所有路由器。

[0057] 在一些实现中,路由器110还可报告LAN100中的过度订阅事件。路由器110可报告该路由器如何处置LAN100中不同类型的过度订阅事件。在一个示例中,LAN100的一些用户可发起五个不同的视频流送应用以同时从WAN140通过路由器110流送五部电影到该LAN的不同网络设备102。在该情形下,网络将可能不具有足以支持用于五个不同视频流送应用的五个不同分组流的带宽,并且因此路由器将检测到过度订阅事件。路由器110可实现一种用以解决过度订阅事件的技术,并向云150报告所使用的该技术以及结果。例如,路由器110可决定将所有视频流的带宽都减少某个百分比(例如,10-20%)。云150中的服务器可使用从其它路由器收集来的关于相似情景的聚集数据,执行分析以及确定存在用以处置路由器110所遭遇的过度订阅事件的更佳技术。云150中的服务器随后可向路由器110提供与新过度订阅解决技术有关的详情,即,云150的一个或多个服务器可用新算法对路由器110编程以解决那种类型的过度订阅事件。例如,云150可确定取代将所有五个视频流的带宽都减少15%,

路由器110应为这些视频流中的4个视频流保持最优带宽而将这些视频流中的一个视频流的带宽减少到最小可接受水平。

[0058] 在一些实现中，路由器110还可向云150报告一些或全部网络活动，以及在云150中存储大多数或全部数据。响应于检测到来自路由器110的报告和从路由器110收集数据，云150可对LAN100执行网络分析并且还可发送网络警报。云150可随周、随月以及随年执行网络分析而没有局域网路由器或其他设备将固有地具有的限制，诸如有限资源和存储。在一个示例中，基于网络活动报告，云150可确定当某个设备或某类设备活跃(例如，该设备连续地传送)时该设备或该类设备使用不成比例的带宽量。云150可监视LAN100并且当其检测出设备活跃且正展现此类行为时发送网络警报。在另一个示例中，云150可检测到上游话务过载，并且向路由器110发送网络警报，该网络警报建议路由器110将所广告的可用带宽减半(例如，从10mbps到5mbps)以减少上游话务并潜在地获得更佳性能。应注意，路由器110可报告其它类型的网络事件。在一些情况下，路由器110可向云150报告网络故障，并且云150可基于聚集数据来确定解决规程以及向路由器110报告解决方案(例如，配置更新或新解决规程步骤)。在一些实现中，由于云150正在从路由器110接收与LAN100相关联的大多数或所有网络活动和网络事件，因而云150还可为LAN100提供其它个性化服务。例如，云150可检测到一个或多个网络设备102中的软件程序(例如，Adobe® Acrobat®)被配置成自动更新(或者用户定期检查更新)。当云150从另一路由器接收到关于用户正在下载更新的信息时，它可向在过去已经更新应用的其它路由器通知有更新可用并且路由器应该在话务较轻(例如，非高峰小时)时下载该更新(例如，将其临时存储在高速缓存中)。在另一个示例中，云150可检测在电子书发行时用户之一从某个作者下载该电子书。基于该活动，当该作者发行新电子书时，云150可自动下载该电子书到路由器110处的本地存储，使得用户能在不使用WAN链路的情况下本地访问并下载该电子书。如图1中所示，在一些实施例中，路由器110可包括网络监视单元112、一个或多个处理器115，以及存储器单元118。路由器110的网络监视单元112、一个或多个处理器115以及存储器单元118可被配置成实现本文中所述的结合云计算网络150操作的网络事件监视及报告操作。在一些实施例中，路由器110的一个或多个处理器115可执行与网络监视单元112相关联的程序指令(例如，存储于存储器单元118中的程序指令)以实现本文中所述的网络事件监视及报告技术，诸如向云150报告未知分组流和过度订阅事件，以及基于从云150获取的信息来实现新检测及解决策略。在一些实现中，路由器110可包括网络接口卡(或模块)111。网络接口卡111可实现网络监视单元112、一个或多个处理器115以及存储器单元118(例如，实现在一个或多个集成电路中)。在其他实现中，路由器110可包括多个网络接口卡和(包括网络接口卡111的)电路板，并且这多个网络接口卡可实现网络监视单元112、一个或多个处理器115以及存储器单元118。尽管图1中未示出，但在一些实现中，路由器110可包括除处理器115和存储器单元118之外的一个或多个附加的处理器和存储器单元(以及其他组件)。例如，路由器110可在一个或多个附加的电路板里包括一个或多个处理器和一个或多个存储器单元。

[0059] 图2是根据一些实施例的解说用于实现图1中所示的用于局域网的云计算增强路由器的示例操作的流程图(“流程”)200。该流程开始于图2的框202。

[0060] 在框202，使用路由器监视局域网的网络话务。例如，路由器110的网络监视单元112(图1中所示)监视从一个或多个网络设备102发送到WAN140的网络话务(例如，文件上

传)，以及在LAN100处从WAN收到的网络话务(例如，视频流送)。另外，网络监视单元112可监视在LAN100中的诸网络设备102之间发送的网络话务。在框202之后，该流程在框204处继续。

[0061] 在框204，使用路由器检测与局域网相关联的一个或多个网络事件。在一些实现中，网络监视单元112基于LAN100的网络话务来检测一个或多个网络事件。如上所述，在一些示例中，网络监视单元112可检测经由路由器110路由的未知分组流和/或检测LAN100中的过度订阅事件。网络监视单元112还可检测其它网络事件，诸如网络故障或对网络带宽的不成比例的使用。在框204之后，该流程在框206处继续。

[0062] 在框206，从路由器向云计算网络报告该一个或多个网络事件。在一些实现中，网络监视单元112可把该一个或多个网络事件从路由器110报告到云计算网络150的一个或多个服务器。在一些实现中，取代向云计算网络150报告所有网络事件或网络活动，路由器110可被配置成报告某些网络事件(“预定义网络事件”)。例如，路由器110可被配置成仅向云150报告过度订阅事件和未知分组流。在框206之后，该流程在框208处继续。

[0063] 在框208，从基于云的计算网络的一个或多个服务器接收用于路由器的网络策略更新。网络策略更新至少部分地基于报告给基于云的计算网络的一个或多个服务器的网络事件类型。在一些实现中，路由器110从云150接收网络策略更新。收到的网络策略更新至少部分地基于报告给云150的网络事件类型。例如，云150可基于所报告的网络事件类型并且基于对从WAN140的多个局域网收集的与相同类型的网络事件相关联的聚集数据执行的分析的结果来确定网络策略更新，如下文将参考图3进一步描述的。例如，如果由路由器110报告的网络事件是在路由器110处检测到的未知分组流，则云150对已经从LAN100以及从WAN140中也已在未知分组流中检测到一些相同的分组流特性的其它局域网收集到的聚集数据执行分析。根据该聚集数据，云150可基于未知分组流的特性确定新分组流检测策略以用于对未知分组流的未来检测和标识。云150可随后将新分组流检测策略发送给路由器110以更新正在路由器110处实现的流检测策略。在框208之后，该流程在框210处继续。

[0064] 在框210，在网络话务管理节点处在配置之后实现网络策略更新。在一些实现中，网络监视单元112用该网络策略更新来配置并且随后在检测和处理LAN100的网络事件时在路由器110处实现该网络策略更新。例如，在未知分组流示例中，网络监视单元112可被更新以实现从云150收到的新分组流检测策略以用于分组流检测和标识。在框210之后，该流程结束。

[0065] 图3是根据一些实施例的解说用于实现图1中所示的云计算增强路由器系统的示例操作的流程图(“流程”)300。该流程开始于图3的框302。

[0066] 在框302，云计算网络150的一个或多个服务器从路由器110接收指示在LAN100中检测到的网络事件的报告消息。例如，如之前在上文所述的，路由器110可确定正被路由的分组流之一是未知的，并且可向云150发送与该未知分组流相关联的信息。作为另一示例，路由器110可检测LAN100处的过度订阅事件并向云150发送指示被实现以尝试解决该过度订阅事件的技术的报告。在该报告中，路由器110还可指示该特定技术是否已成功解决过度订阅事件以及该技术的具体结果。在框302之后，该流程在框304处继续。

[0067] 在框304，云计算网络150确定与从路由器110收到的报告消息相关联的网络事件类型。例如，云150确定报告消息与在路由器110处收到的未知分组流相关联，或者报告消息

与在LAN100处检测到的过度订阅事件相关联。然而，要注意，报告消息可指示各种其它网络事件，如上文参考图1所述的(例如，网络故障报告)。在框304之后，该流程在框306处继续。

[0068] 在框306，云计算网络150把与所报告的网络事件相关联的数据同之前从其它局域网中的其它路由器收到的关于所检测到的相同或相似类型的网络事件的数据聚集在一起。例如，云150聚集与由各种路由器已经报告的未知分组流相关联的所有信息(例如，分组流特性)。作为另一示例，云150聚集与各种路由器所报告的相同或相似类型的过度订阅事件相关联的所有数据(例如，所使用的解决技术及结果)。在框306之后，该流程在框308处继续。

[0069] 在框308，云计算网络150分析与所报告的相同或相似类型的网络事件相关联的聚集数据。例如，云150分析与由其它局域网中的各种路由器已经报告的未知分组流相关联的聚集数据。在一个示例中，云150可对与未知分组流相关联的聚集数据执行深度分组检查以及统计分析，并且可分析与未知分组流相关联的不同流特性。同时，为了帮助标识未知分组流，云150可连续监视来自因特网120上的各种服务提供者的分组流，并且标识相应分组流中的任何改变。在另一个示例中，云150可分析与由各种路由器已经报告的各种过度订阅事件相关联的聚集数据。云150可检查用来解决过度订阅事件的各种技术并且比较实现不同技术的结果。在框308之后，该流程在框310处继续。

[0070] 在框310，云计算网络150确定用于处置检测到的网络事件的改进的网络策略或规程，并且向LAN100的路由器110发送经更新的网络策略或规程以更新路由器配置。例如，基于上面在框308中执行的分析，云150可确定用于检测分组流的改进的分组流检测策略(例如，经更新的流特性准则)或者可确定用于处置过度订阅事件的改进的解决策略。在框310之后，该流程结束。

[0071] 在一些实现中，云计算网络150实时地确定并向路由器110发送网络策略更新。例如，如果云计算网络150已经从WAN140中的各种路由器聚集了充足的数据，并且已经对聚集数据执行了分析，则当路由器110报告网络事件时，云计算网络150可实时地向路由器110发送网络策略更新。结果，路由器110可实时地实现网络策略更新以实时地处理和/或解决所报告的网络事件。在一些实现中，在从路由器110接收到与网络事件相关联的(诸)报告消息之后，云计算网络150可继续聚集与来自WAN140中的其它路由器的网络事件相关联的附加数据，和/或可对聚集数据执行附加分析。例如，云计算网络150可确定它需要众包附加数据和/或执行附加分析以确定针对网络事件的改进的网络策略。在此示例中，云计算网络150将不会实时地向路由器110发送网络策略更新。取而代之的是，云计算网络150将在稍后时间发送网络策略更新，并且路由器110将实现该网络策略更新以处理和/或解决该网络事件的下次发生。

[0072] 图4是根据一些实施例的解说用于在图1-3中所述的云计算增强路由器中实现分组流检测的示例操作的流程图(“流程”)400。该流程开始于图4的框402。

[0073] 在框402，对在局域网的路由器处检测到的多个分组流进行分类。在一些实现中，路由器110的网络监视单元112(图1中示出)监视网络话务，检测该多个分组流，以及对分组流进行分类。例如，在(例如，使用深度分组检查来)检测分组流的特性和统计量之后，网络监视单元112可确定与分组流相关联的应用并且基于该相关联的应用来对分组流进行分类。在一个示例中，如果分组流特性和统计量指示分组流是从Netflix®视频流送服务分发

的，则网络监视单元112把该分组流分类为Netflix® 应用分组流。在框402之后，该流程在框404处继续。

[0074] 在框404，在路由器处检测未知分组流。在一些实现中，网络监视单元112检测分组流特性和统计量，把分组流特性和统计量与已知分组流作比较，以及确定分组流是具有未知分组流特性和统计量的未知分组流。在框404之后，该流程在框406处继续。

[0075] 在框406，为未知分组流选择默认分类。在一些实现中，即使网络监视单元112不能确定与未知分组流相关联的具体应用，网络监视单元112也可基于与未知分组流相关联的应用类型(例如，流送视频或音频)来选择默认分类。例如，未知分组流的应用类型可以被确定为流送视频或流送音频，并且可以基于应用类型来向未知分组流指派默认分类。在一些实现中，网络监视单元112可能不能确定与未知分组流相关联的具体应用及应用类型两者，并且因此可为具有未知应用和应用类型的分组流临时选择默认分类。在能确定具体应用之前，可临时指派默认分类以允许未知分组流被路由器110处理。例如，默认分类可向未知分组流指派最小及最大带宽要求，并且在某些情况下可指派优先级值。在一个示例中，如果基于视频流送作为应用类型来为未知分组流选择默认分类，则默认分类指派对于视频流送应用而言典型的最小和最大带宽要求(例如，视频流送应用的平均带宽数)。在框406之后，该流程在框408处继续。

[0076] 在框408，与未知分组流相关联的信息被报告给云计算网络的一个或多个服务器。在一些实现中，网络监视单元112可经由因特网从路由器110向云150发送指示与未知分组流相关联的分组流特性和统计量的报告消息。在框408之后，该流程在框410处继续。

[0077] 在框410，从云计算网络接收经更新的分组流检测策略。在一些实现中，网络监视单元112可从云150接收经更新的分组流检测策略，该经更新的分组流检测策略可用于检测和分类之前未知的分组流。在一个示例中，云150对已经从路由器110和从WAN140中已在未知分组流中检测到一些相同的分组流特性和统计量的其它局域网收集到的聚集数据执行分析。云还继续从因特网中的服务提供者和应用收集分组流特性和统计量。根据聚集数据，云150可基于未知分组流的特性和统计量确定新分组流检测策略以用于未知分组流的未来标识和分类。例如，在把来自最近上线的新音频流送服务的分组流特性和统计量与由云150所聚集的分组流特性和统计量作比较之后，云150可确定未知分组流来自该新音频流送服务。在另一个示例中，云150可确定现有的视频流送服务改变了与其服务和应用相关联的分组流特性和统计量。在框410之后，该流程在框412处继续。

[0078] 在框412，在路由器处实现经更新的分组流检测策略。在一些实现中，在路由器110用新策略来配置之后，网络监视单元112实现经更新的分组流检测策略。经更新的分组流检测策略可用于对之前未知的分组流的随后检测及分类。在流程412之后，该流程结束。

[0079] 应理解，图1-5和本文中所描述的各操作是旨在帮助理解实施例的示例，而不应被用于限制实施例或限制权利要求的范围。诸实施例可执行附加操作、执行较少操作、以不同次序执行操作、并行地执行操作以及以不同方式执行一些操作。

[0080] 如本领域技术人员将领会的，本发明主题的各方面可体现为系统、方法或计算机程序产品。相应地，本发明主题内容的各方面可采取全硬件实施例、软件实施例(包括固件、驻留软件、微代码等)、或组合了软件与硬件方面的实施例的形式，其在本文可被统称为“电路”、“模块”或“系统”。此外，本发明主题内容的各方面可采取体现在其上含有计算机可读

程序代码的一个或多个计算机可读介质中的计算机程序产品的形式。

[0081] 可以使用一个或多个计算机可读介质的任何组合。计算机可读介质可以是计算机可读信号介质或计算机可读存储介质。计算机可读存储介质可以是例如但不限于:电子、磁性、光学、电磁、红外、或半导体系统、装置或设备,或者前述的任何合适组合。计算机可读存储介质的更为具体的示例(非穷尽性列表)可包括以下各项:具有一条或多条导线的电连接、便携式计算机软盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或闪存)、光纤、便携式压缩碟只读存储器(CD-ROM)、光存储设备、磁存储设备或者前述的任何合适组合。在本文档的上下文中,计算机可读存储介质可以是能包含或存储供指令执行系统、装置或设备使用或者结合其使用的程序的任何有形介质。计算机可读信号介质可包括例如在基带中或者作为载波一部分的其中含有计算机可读程序代码的所传播的数据信号。此类所传播信号可采取各种形式中的任一种,包括但不限于电磁信号、光学信号或其任何合适的组合。计算机可读信号介质可以为不是计算机可读存储介质的任何计算机可读介质,它能传达、传播或传输供由或结合指令执行系统、装置或设备使用的程序。包含在计算机可读介质上的程序代码可以使用任何恰适的介质来传送,包括但不限于无线、有线、光纤缆线、RF等或者前述的任何合适的组合。

[0082] 用于实施本发明主题内容的各方面的操作的计算机程序代码可以用一种或多种编程语言的任何组合来编写,包括面向对象编程语言(诸如Java、Smalltalk、C++等)以及常规过程编程语言(诸如“C”编程语言或类似编程语言)。程序代码可完全在用户计算机上、部分在用户计算机上、作为独立软件包、部分在用户计算机上且部分在远程计算机上或者完全在远程计算机或服务器上执行。在后一情境中,远程计算机可通过任何类型的网络连接至用户计算机,包括局域网(LAN)或广域网(WAN)、或者可进行与外部计算机的连接(例如,使用因特网服务提供商通过因特网来连接)。

[0083] 本发明主题内容的各方面是参考根据本发明主题内容的各实施例的方法、装置(系统)和计算机程序产品的流程图解说和/或框图来描述的。将理解,这些流程图解说和/或框图中的每个框以及这些流程图解说和/或框图中的框的组合可以通过计算机程序指令来实现。这些计算机程序指令可被提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器以用以制造机器,从而经由计算机或其他可编程数据处理装置的处理器执行的这些指令构建用于实现这些流程图和/或框图的(诸)框中所指定的功能/动作的装置。

[0084] 这些计算机程序指令也可存储在计算机可读介质中,其可以指导计算机、其他可编程数据处理装置或其他设备以特定方式起作用,从而存储在该计算机可读介质中的指令制造出包括实现这些流程图和/或框图的(诸)框中所指定的功能/动作的指令的制品。

[0085] 计算机程序指令也可被加载到计算机、其他可编程数据处理装置或其他设备上以使得在该计算机、其他可编程装置或其他设备上执行一系列操作步骤以产生由计算机实现的过程,从而在该计算机或其他可编程装置上执行的这些指令提供用于实现这些流程图和/或框图的(诸)框中所指定的功能/动作的过程。

[0086] 图5是根据一些实施例的网络设备500的一个实施例的框图,该网络设备500包括用于局域网监视和在广域网中基于云的支持的机制。在一些实现中,网络设备500是两个或更多个网络(例如,LAN和WAN)之间的接收、处理、并路由与这些网络相关联的分组的网络话务管理节点;例如,该网络话务管理节点可以是LAN(例如,图1中所示的LAN100)的路由器/

网关。然而注意到，在其他实现中，网络设备500可以是能被配置成实现以上参考图1-4所描述的功能性的其他合适类型的网络设备，诸如，电缆调制解调器、无线接入点、网桥、网络交换机、台式计算机、游戏控制台、移动计算设备，等等。网络设备500包括处理器单元502(有可能包括多处理器、多核、多节点、和/或实现多线程等)。网络设备500包括存储器单元506。存储器单元506可以是系统存储器(例如，高速缓存、SRAM、DRAM、零电容器RAM、双晶体管RAM、eDRAM、EDO RAM、DDR RAM、EEPROM、NRAM、RRAM、SONOS、PRAM等中的一者或多者)或者上面已经描述的机器可读存储介质的可能实现中的任何一者或多者。网络设备500还包括总线510(例如，PCI、ISA、PCI-Express、HyperTransport®、InfiniBand®、NuBus、AHB、AXI等)、以及网络接口508，网络接口508包括无线网络接口(例如，蓝牙接口、WLAN802.11接口、WiMAX接口、ZigBee®接口、无线USB接口等)和有线网络接口(例如，以太网接口、电力线通信接口等)中的至少一者的(诸)。如示出的，(诸)网络接口508还包括网络监视单元512。例如，网络监视单元512可被实现在(诸)网络接口508的网络接口卡或网络接口模块内。网络监视单元512可操作用于为网络设备500实现用于网络话务监视、网络事件检测和基于云的访问和支持(以及其它特征)的机制，如以上参考图1-4所描述的。

[0087] 这些功能性中的任何一个都可部分地(或完全地)在硬件中和/或在处理器单元502上实现。例如，该功能性可用一个或多个专用集成电路、一个或多个片上系统(SoC)、或其他类型的(诸)集成电路来实现、在处理器单元502中实现的逻辑中、在外围设备或卡上的协作处理器中、在网络接口508内实现的分开的处理器和/或存储器等中实现。此外，诸实现可包括更少的组件或包括图5中未解说的额外组件(例如，视频卡、音频卡、额外网络接口、外围设备等)。处理器单元502、存储器单元506以及网络接口508被耦合至总线510。尽管被示为耦合至总线510，但是存储器单元506也可耦合至处理器单元502。

[0088] 尽管各实施例是参考各种实现和利用来描述的，但是应理解这些实施例是解说性的且本发明主题内容的范围并不限于这些实施例。一般而言，本文所描述的用于实现通信网络的云计算增强路由器的技术可以用符合任何硬件系统或诸硬件系统的设施来实现。许多变体、修改、添加和改善都是可能的。

[0089] 可为本文中描述为单数实例的组件、操作、或结构提供复数个实例。最后，各种组件、操作和数据存储之间的边界在某种程度上是任意的，并且在具体解说性配置的上下文中解说了特定操作。其他的功能性分配是已预见的并且可落在本发明主题内容的范围内。一般而言，在示例性配置中呈现为分开的组件的结构和功能性可被实现为组合式结构或组件。类似地，被呈现为单个组件的结构或功能性可被实现为分开的组件。这些以及其他变体、修改、添加及改善可落在本发明主题内容的范围内。

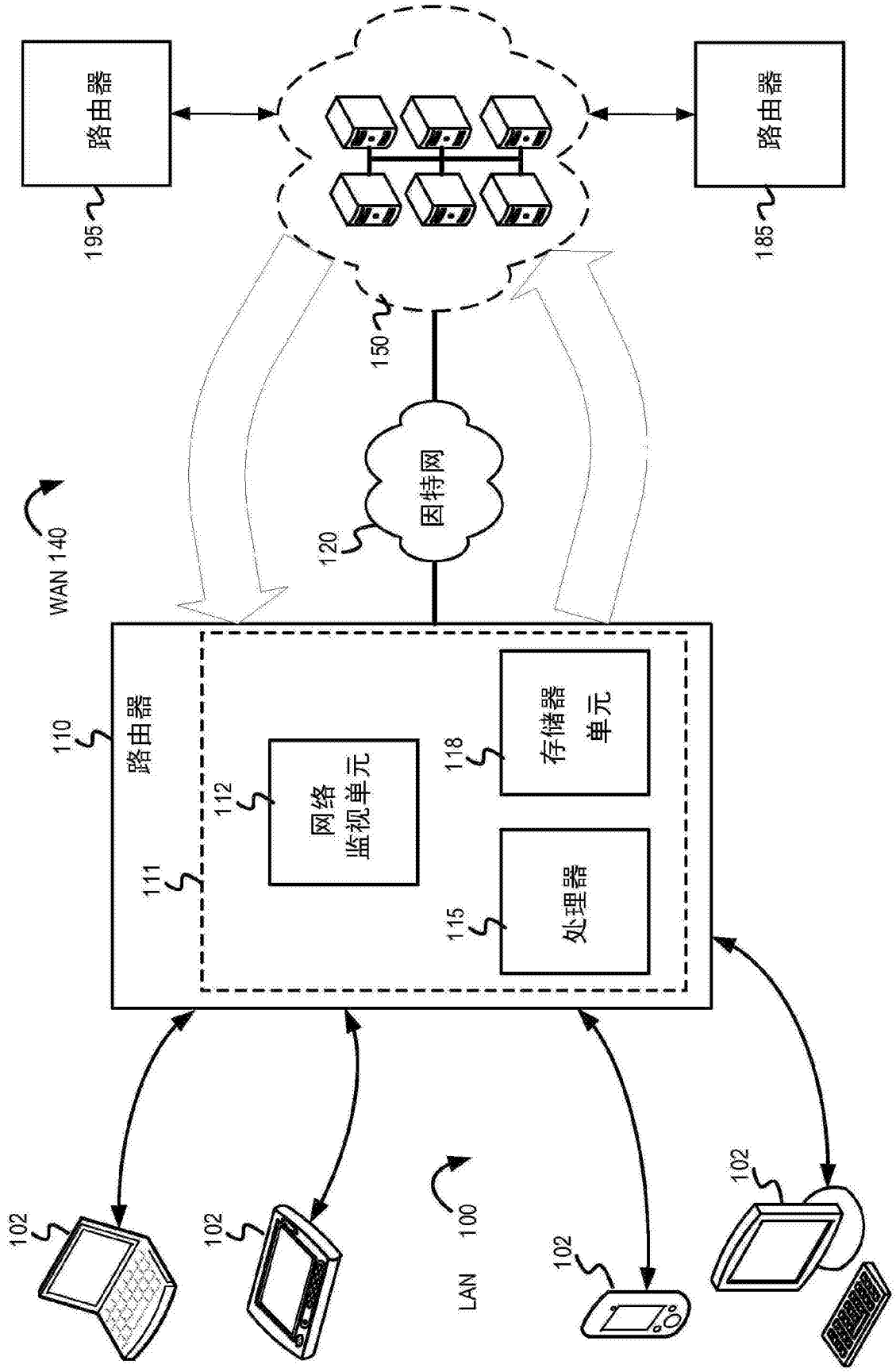

路由器
195
路由器
185
150
因特网
120
WAN 140
110
路由器
111
网络
监视单元
112
存储器
单元
118
处理器
115
102
102
102
LAN 100

图1

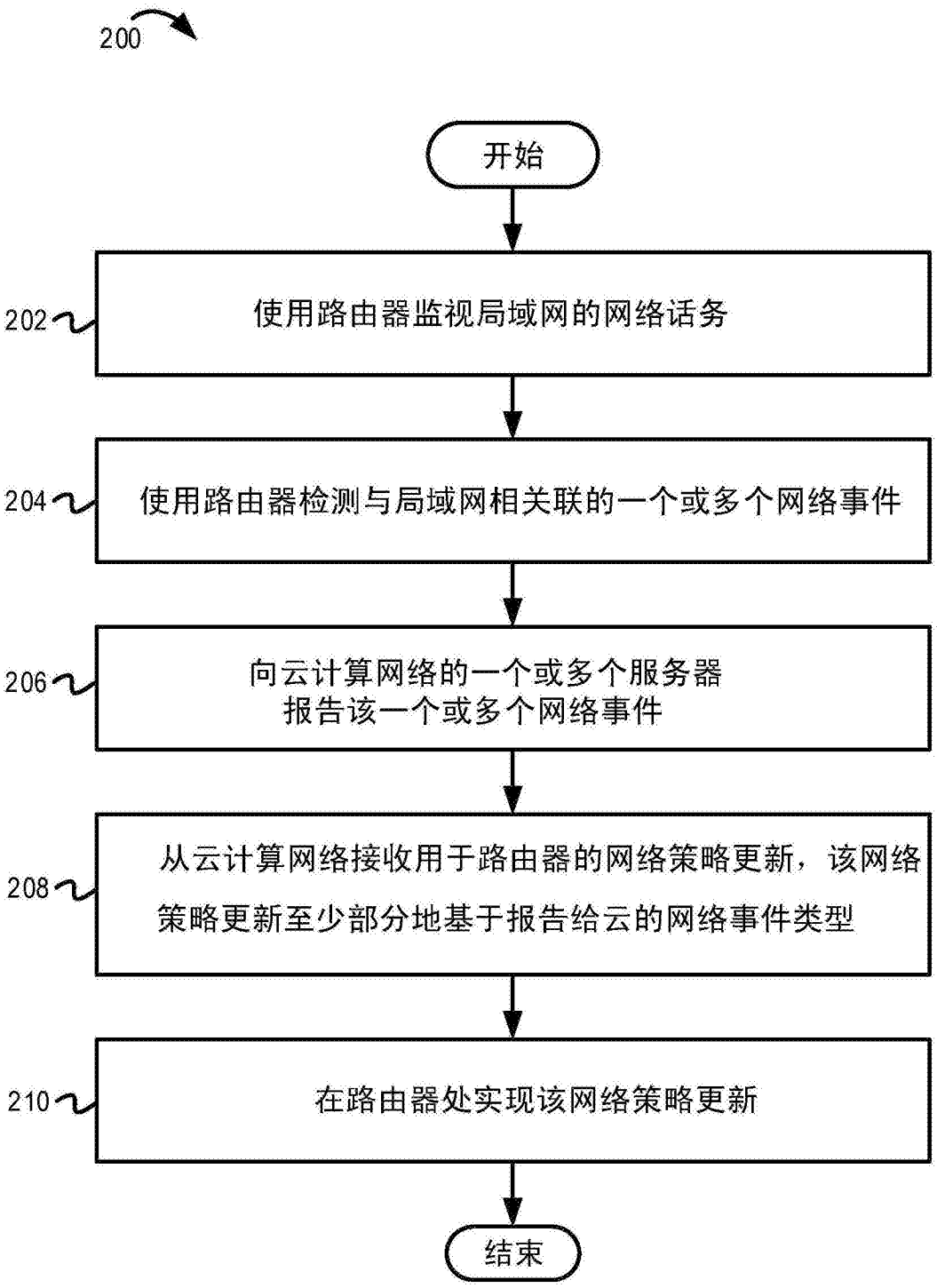

200
开始
202
使用路由器监视局域网的网络话务
204
使用路由器检测与局域网相关联的一个或多个网络事件
206
向云计算网络的一个或多个服务器
报告该一个或多个网络事件
208
从云计算网络接收用于路由器的网络策略更新，该网络策略更新至少部分地基于报告给云的网络事件类型
210
在路由器处实现该网络策略更新
结束

图2

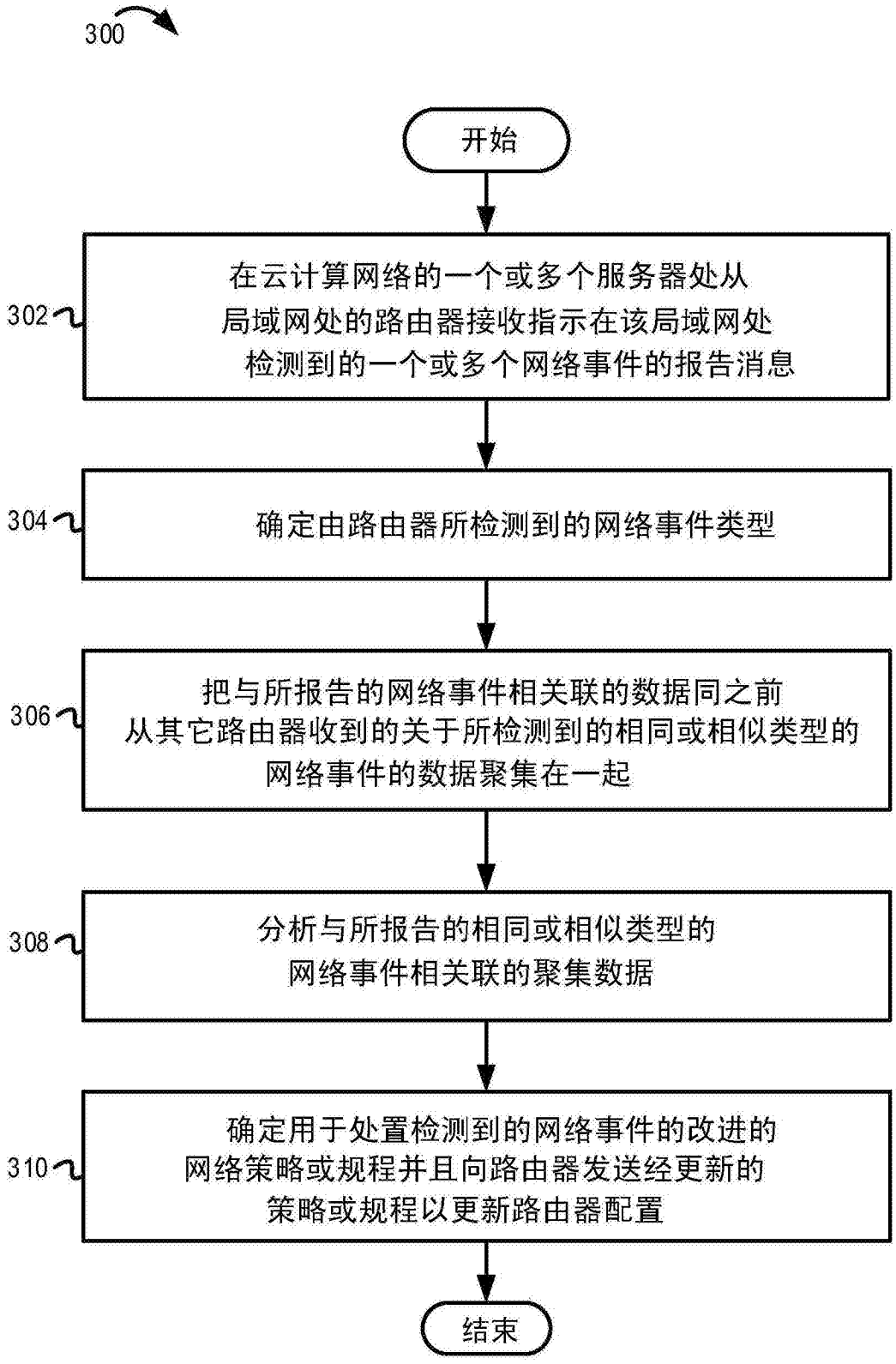

300
开始
302
在云计算网络的一个或多个服务器处从局域网处的路由器接收指示在该局域网处检测到的一个或多个网络事件的报告消息
304
确定由路由器所检测到的网络事件类型
306
把与所报告的网络事件相关联的数据同之前从其它路由器收到的关于所检测到的相同或相似类型的网络事件的数据聚集在一起
308
分析与所报告的相同或相似类型的网络事件相关联的聚集数据
310
确定用于处置检测到的网络事件的改进的网络策略或规程并且向路由器发送经更新的策略或规程以更新路由器配置
结束

图3

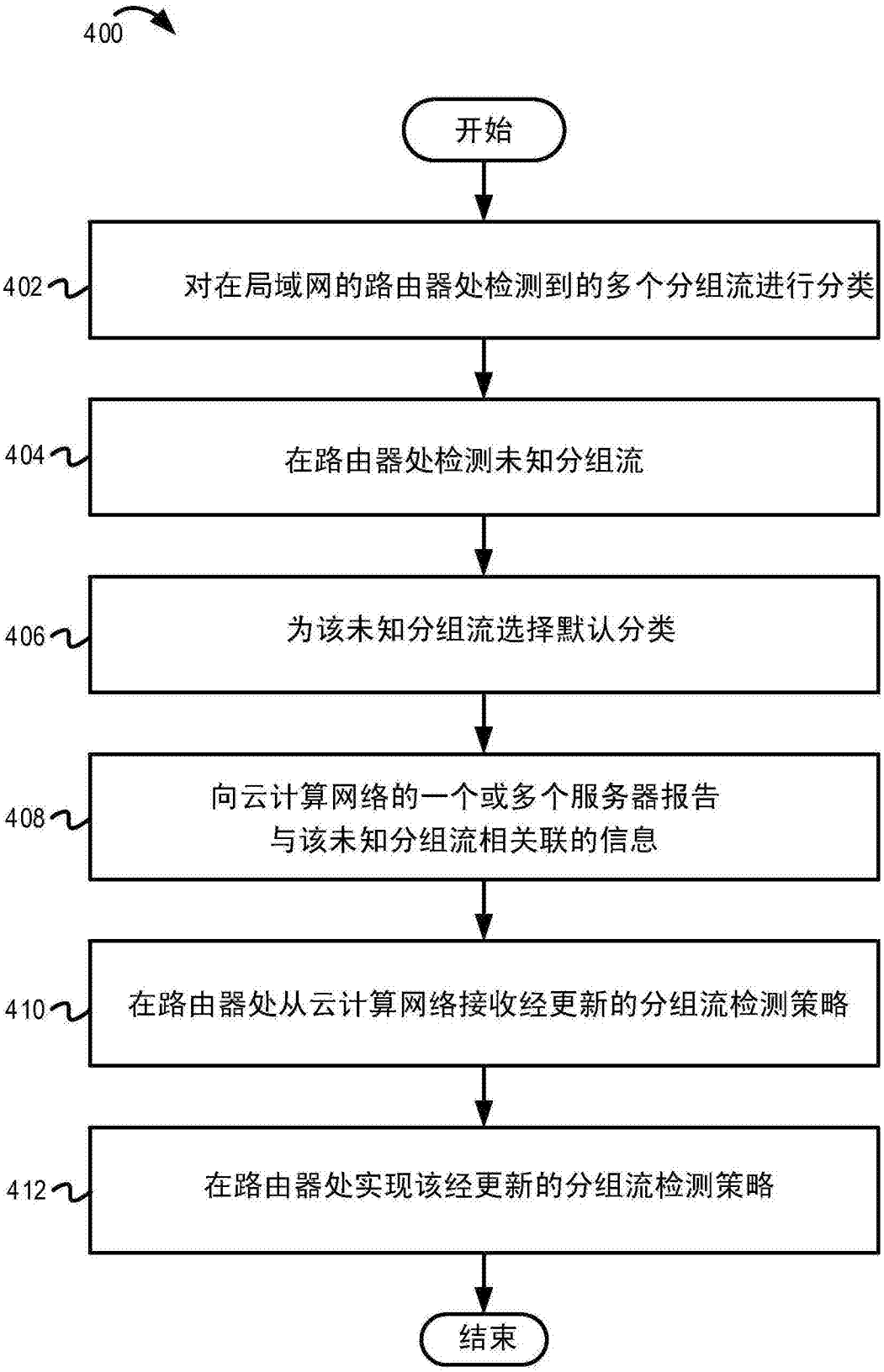

400
开始
402
对在局域网的路由器处检测到的多个分组流进行分类
404
在路由器处检测未知分组流
406
为该未知分组流选择默认分类
408
向云计算网络的一个或多个服务器报告
与该未知分组流相关联的信息
410
在路由器处从云计算网络接收经更新的分组流检测策略
412
在路由器处实现该经更新的分组流检测策略
结束

图4

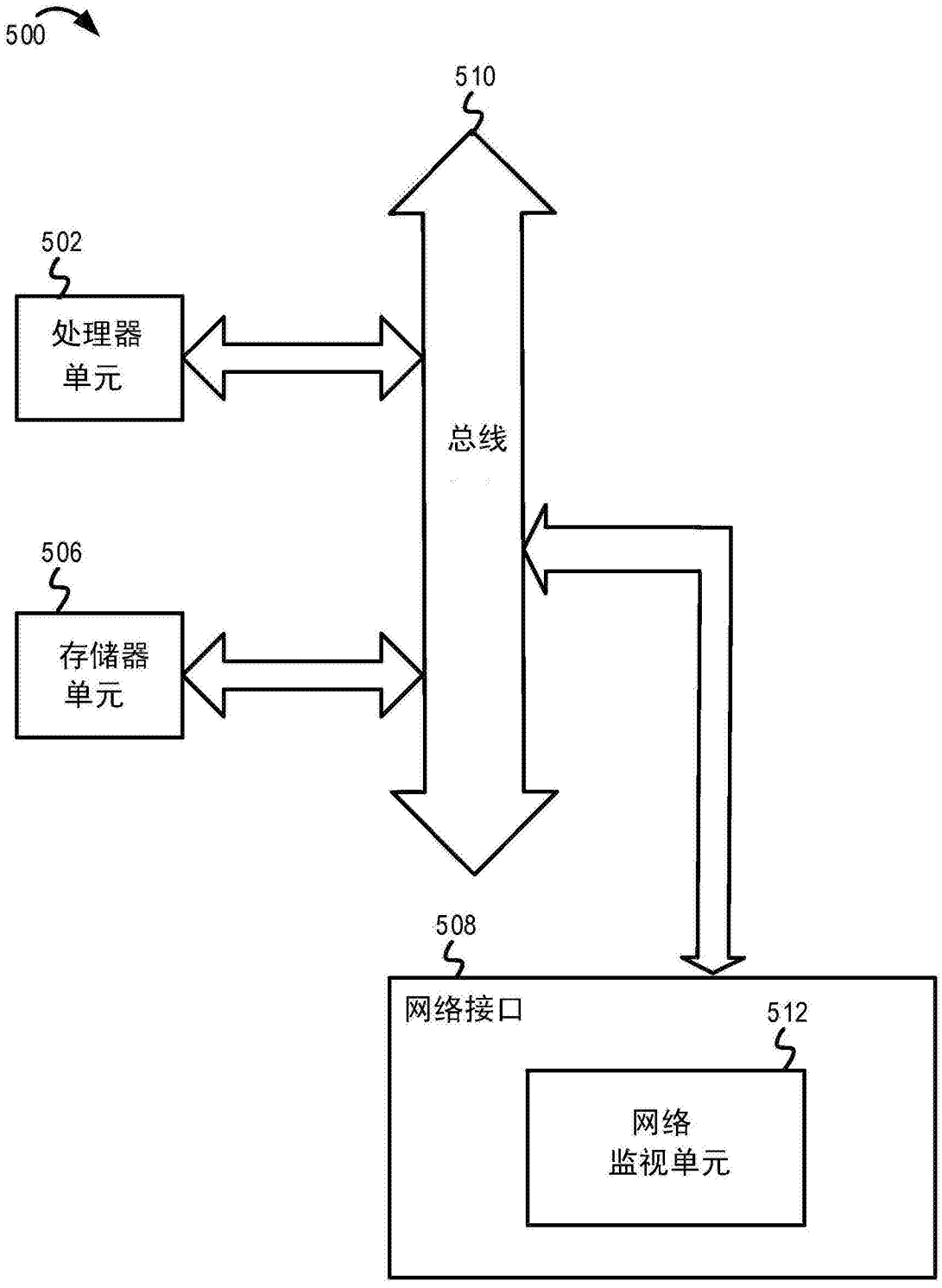


图5