



(12) 发明专利

(10) 授权公告号 CN 101023685 B

(45) 授权公告日 2011.04.06

(21) 申请号 200580031213.X

(51) Int. Cl.

(22) 申请日 2005.10.25

H04W 28/08 (2009.01)

(30) 优先权数据

(56) 对比文件

10/974,418 2004.10.26 US

WO 2004/028175 A1,2004.04.01,说明书第 16 页第 1 行至第 17 页第 22 行,第 32 页 4-21 行、附图 2,9b.

(85) PCT 申请进入国家阶段日

2007.03.16

CN 1444362 A,2003.09.24,全文.

(86) PCT 申请的申请数据

PCT/US2005/038831 2005.10.25

CN 1399490 A,2003.02.26,全文.

US 6366780 B1,2002.04.02,全文.

(87) PCT 申请的公布数据

WO2006/047699 EN 2006.05.04

审查员 姚雅倩

(73) 专利权人 思科技术公司

地址 美国加利福尼亚州

(72) 发明人 亚瑟·赞瓦勒科维斯克

杰里米·斯蒂格里兹

艾米·思琦贝尔

(74) 专利代理机构 北京东方亿思知识产权代理

有限责任公司 11258

代理人 王怡

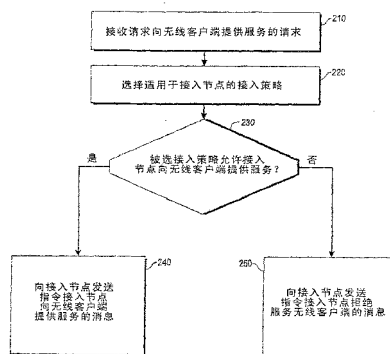
权利要求书 3 页 说明书 10 页 附图 4 页

(54) 发明名称

基于集中化信息平衡无线接入的方法和装置

(57) 摘要

提供了一种方法和装置,用于基于集中化信息管理和平衡无线接入。请求向无线客户端提供服务的请求从多个接入节点中的第一接入节点被接收到。适用于第一接入节点的接入策略从多个存储的策略中被选出。所存储的策略可以包括多种规则,例如,多少或者哪些无线客户端可由接入节点服务。集中化管理器(例如 AAA 服务器)可以执行对接入策略的选择。基于被选接入策略,确定出是否允许第一接入节点向无线客户端提供服务。指令第一接入节点是向无线客户端提供服务还是拒绝服务无线客户端的消息被发送到第一接入节点。



CN 101023685 B

1. 一种用于基于集中化信息平衡无线接入的方法,包括:

从多个接入节点中的第一接入节点接收请求向无线客户端提供服务的请求,其中所述多个接入节点中的每个被配置为向一个或多个客户端提供无线服务;

从多个存储的策略中选择适用于所述第一接入节点的第一接入策略;

基于所述第一接入策略确定是否允许所述第一接入节点向所述无线客户端提供服务;

在确定出所述第一接入策略允许所述第一接入节点向所述无线客户端提供服务时,向所述第一接入节点发送指令所述第一接入节点向所述无线客户端提供服务的第一消息;以及

在确定出所述第一接入策略不允许所述第一接入节点向所述无线客户端提供服务时,向所述第一接入节点发送指令所述第一接入节点拒绝服务所述无线客户端的第二消息。

2. 如权利要求1所述的方法,还包括以下步骤:

从所述多个接入节点中的第二接入节点接收请求向所述无线客户端提供服务的第二请求;

从所述多个存储的策略中选择适用于所述第二接入节点的第二接入策略;

基于所述第二接入策略确定是否允许所述第二接入节点向所述无线客户端提供服务;

在确定出所述第二接入策略允许所述第二接入节点向所述无线客户端提供服务时,向所述第二接入节点发送指令所述第二接入节点向所述无线客户端提供服务的第三消息;以及

在确定出所述第二接入策略不允许所述第二接入节点向所述无线客户端提供服务时,向所述第二接入节点发送指令所述第二接入节点拒绝服务所述无线客户端的第四消息。

3. 如权利要求1所述的方法,其中,所述第一接入策略至少部分包括关于多少无线客户端能够被所述多个接入节点中的一个或多个服务的一条或多条规则。

4. 如权利要求1所述的方法,其中,所述请求包括客户端标识数据,并且其中所述第一接入策略至少部分包括关于基于所述客户端标识数据是否允许所述第一接入节点向所述无线客户端提供服务的一条或多条规则。

5. 如权利要求1所述的方法,其中,所述第一接入策略至少部分包括关于基于多少其他无线客户端正由与所述第一接入节点相关联的一组接入节点服务是否允许所述第一接入节点向所述无线客户端提供服务的一条或多条规则。

6. 如权利要求1所述的方法,还包括存储标识出所述多个接入节点中的一个或多个接入节点属于一组接入节点的数据,其中所述组的成员资格是基于所述一个或多个接入节点的特性的。

7. 如权利要求1所述的方法,其中,所述第一接入策略至少部分包括关于基于描述在所述第一接入节点处多少带宽正被消耗的数据是否允许所述第一接入节点向所述无线客户端提供服务的一条或多条规则。

8. 如权利要求1所述的方法,还包括在所述接收所述请求的步骤之前,在所述多个接入节点中的两个或更多个接入节点中的每个处接收来自所述无线客户端的预认证消息,所述预认证消息请求在所述无线客户端和接收接入节点之间建立安全性关联。

9. 一种用于基于集中化信息平衡无线接入的装置,包括:

用于从多个接入节点中的第一接入节点接收请求向无线客户端提供服务的请求的装置,其中所述多个接入节点中的每个被配置为向一个或多个客户端提供无线服务;

用于从多个存储的策略中选择适用于所述第一接入节点的第一接入策略的装置;

用于基于所述第一接入策略确定是否允许所述第一接入节点向所述无线客户端提供服务的装置;

用于在确定出所述第一接入策略允许所述第一接入节点向所述无线客户端提供服务时,向所述第一接入节点发送指令所述第一接入节点向所述无线客户端提供服务的第一消息的装置;以及

用于在确定出所述第一接入策略不允许所述第一接入节点向所述无线客户端提供服务时,向所述第一接入节点发送指令所述第一接入节点拒绝服务所述无线客户端的第二消息的装置。

10. 如权利要求 9 所述的装置,还包括:

用于从所述多个接入节点中的第二接入节点接收请求向所述无线客户端提供服务的第二请求的装置;

用于从所述多个存储的策略中选择适用于所述第二接入节点的第二接入策略的装置;

用于基于所述第二接入策略确定是否允许所述第二接入节点向所述无线客户端提供服务的装置;

用于在确定出所述第二接入策略允许所述第二接入节点向所述无线客户端提供服务时,向所述第二接入节点发送指令所述第二接入节点向所述无线客户端提供服务的第三消息的装置;以及

用于在确定出所述第二接入策略不允许所述第二接入节点向所述无线客户端提供服务时,向所述第二接入节点发送指令所述第二接入节点拒绝服务所述无线客户端的第四消息的装置。

11. 如权利要求 9 所述的装置,其中,所述第一接入策略至少部分包括关于多少无线客户端能够被所述多个接入节点中的一个或多个服务的一条或多条规则。

12. 如权利要求 9 所述的装置,其中,所述请求包括客户端标识数据,并且其中所述第一接入策略至少部分包括关于基于所述客户端标识数据是否允许所述第一接入节点向所述无线客户端提供服务的一条或多条规则。

13. 如权利要求 9 所述的装置,其中,所述第一接入策略至少部分包括关于基于多少其他无线客户端正由与所述第一接入节点相关联的一组接入节点服务是否允许所述第一接入节点向所述无线客户端提供服务的一条或多条规则。

14. 如权利要求 9 所述的装置,还包括用于存储标识出所述多个接入节点中的一个或多个接入节点属于一组接入节点的数据的装置,其中所述组的成员资格是基于所述一个或多个接入节点的特性的。

15. 如权利要求 9 所述的装置,其中,所述用于选择所述第一接入策略的装置基于所述请求中包括的接入节点身份信息选择所述第一接入策略,并且其中所述接入节点身份信息标识所述第一接入节点。

16. 如权利要求 9 所述的装置, 其中, 所述第一接入策略至少部分包括关于基于描述在所述第一接入节点处多少带宽正被消耗的数据是否允许所述第一接入节点向所述无线客户端提供服务的一条或多条规则。

17. 如权利要求 9 所述的装置, 还包括用于在所述多个接入节点中的两个或更多个接入节点中的每个处接收来自所述无线客户端的预认证消息的装置, 其中所述预认证消息请求在所述无线客户端和接收接入节点之间建立安全性关联。

基于集中化信息平衡无线接入的方法和装置

技术领域

[0001] 本发明涉及对网络的无线接入进行负载平衡。

背景技术

[0002] 近些年来,利用无线连接接入网络由于其便利性而日益流行。利用无线连接接入网络的一种方法在 IEEE 802.11 规范中有所描述。根据该方法,客户端发送探测请求到在该客户端的范围内的一个或多个接入点。接入点 (AP) 是被配置为向一个或多个客户端提供无线服务的组件。典型的网络可能具有多个接入点。探测请求是从客户端发送到接入点的这样的消息,该消息用于确定该接入点是否能够向该客户端提供服务。

[0003] 在接入点接收到探测请求后,接入点发送探测响应给客户端。探测响应指示出发送该探测响应的接入点能够向接收客户端提供服务。

[0004] 由于一个客户端一般发送探测请求到多于一个接入点,所以客户端一般在返回中接收到多于一个探测响应。每个客户端遵循一定过程来确定该客户端应当尝试向哪个接入点请求服务。例如,客户端可以基于哪个接入点发送了具有最强信号的探测响应来确定该客户端应当尝试向哪个接入点请求服务。通过连接到发送了具有最强信号的探测响应的接入点,客户端从而提高了从接入点接收优质服务的可能性。

[0005] 在客户端选择了从其接收服务的特定接入点后,客户端发送对服务的请求到该特定的接入点。此后,该特定接入点向该客户端提供服务。

[0006] 每个接入点可以服务的客户端的数目可能是有限的。例如,随着更多的客户端连接到特定的接入点,对接入点的资源的需求也增加了。在某一时刻,在不使从接入点提供给客户端的服务质量下降的不可接受的水平的情况下,该接入点可能不能再服务额外的客户端。结果,如果对接入点的资源的需求超出了可接受的水平,接入点可能拒绝对请求服务的特定客户端提供服务。

[0007] 为了容纳尽可能多的客户端,无线网络的设计者基于断定的客户端数目和位置,确定接入点的数目和位置。例如,对于一家公司,接入点的数目和位置可以通过估计物理位置(例如,建筑、楼层或者办公建筑)中的客户端的数目来确定出。在这种情形中,由于客户端的数目和位置已知,所以可以容易地预测每个接入点的平均客户端数目。

[0008] 但是,存在难以预先确定多少个客户端将需要接入网络的情形。例如,在会议、记者招待会、热点和其他非常规事件期间,就难以确定多少个客户端将需要接入。在这种情形中,由于在该位置中对可用接入点的需求太大,所以客户端可能不能获得对网络的接入。如果请求无线接入的客户端具有特殊的接入需要,例如,客户端可能在要求无线接入的会议期间参与进行陈述,该问题就尤其麻烦。

[0009] 此外,即使对于例如会议之类的非常规事件,额外的接入点被添加到物理位置,客户端可能仍不能获得它们所要求的服务。由于客户端一般采用相同或类似的过程来确定向哪个接入点请求服务,所以可能即使许多接入点被添加来支持特定的位置,但是该位置中的每个客户端可能仍尝试向相同接入点请求服务,例如,每个客户端将尝试向以最强信号

对探测请求的作出响应的接入点请求服务。因此,位于同一位置的大部分客户端将尝试向单个接入点请求服务,即使有其他接入点可用也是如此。该接入点最终将由于来自客户端的请求而过载,导致该接入点所提供的服务质量降低。此外,由于客户端一般采用相同或类似的过程来确定向哪个接入点请求服务,所以被一个接入点拒绝服务的每个客户端将可能尝试连接到第二接入节点,这也可能超过第二接入节点的容量。

[0010] 因此,期望提供一种方法,该方法用于在不招致现有方法的缺点的情况下,提供对网络的负载平衡的无线接入。在本部分中描述的方法是可能被实现的方法,但是不一定是先前已被设想出或者实现的方法。因此,除非另行指出,不应当仅由于该部分中所述的任何方法被包括在该部分中而假定它们是现有技术。

发明内容

[0011] 一种机器实现的方法,包括:从多个接入节点中的第一接入节点接收请求向无线客户端提供服务的请求,其中所述多个接入节点中的每个被配置为向一个或多个客户端提供无线服务;从多个存储的策略中选择适用于所述第一接入节点的第一接入策略;基于所述第一接入策略确定是否允许所述第一接入节点向所述无线客户端提供服务;在确定出所述第一接入策略允许所述第一接入节点向所述无线客户端提供服务时,向所述第一接入节点发送指令所述第一接入节点向所述无线客户端提供服务的第一消息;以及在确定出所述第一接入策略不允许所述第一接入节点向所述无线客户端提供服务时,向所述第一接入节点发送指令所述第一接入节点拒绝服务所述第二消息。

[0012] 一种计算机装置,包括:用于从多个接入节点中的第一接入节点接收请求向无线客户端提供服务的请求的装置,其中所述多个接入节点中的每个被配置为向一个或多个客户端提供无线服务;用于从多个存储的策略中选择适用于所述第一接入节点的第一接入策略的装置;用于基于所述第一接入策略确定是否允许所述第一接入节点向所述无线客户端提供服务的装置;用于在确定出所述第一接入策略允许所述第一接入节点向所述无线客户端提供服务时,向所述第一接入节点发送指令所述第一接入节点向所述无线客户端提供服务的第一消息的装置;以及用于在确定出所述第一接入策略不允许所述第一接入节点向所述无线客户端提供服务时,向所述第一接入节点发送指令所述第一接入节点拒绝服务所述第二消息的装置。

附图说明

[0013] 在附图中,作为示例而不是作为限制示出了这里所述的实施例,其中相似的标号指示类似的元素,其中:

[0014] 图 1 是示出了其中可以实现一个实施例的示例网络布置的框图;

[0015] 图 2 是示出了一个实施例的功能步骤的流程图;

[0016] 图 3 是示出了说明性实施例的功能组件的框图;以及

[0017] 图 4 是示出了其上可以实现一个实施例的计算机系统的框图。

具体实施方式

[0018] 在下面的描述中,为了说明目的,阐述了很多具体细节,以便于充分理解这里所述

的实施例。但是,没有这些具体细节也可以实施这里所述的实施例,这是很明显的。在其他实例中,以框图形式示出了公知的结构和设备,以避免不必要地模糊了这里所述的实施例。

[0019] 功能概述

[0020] 公开了一种方法,用于基于集中化信息管理和平衡无线接入。根据一个实施例,请求向无线客户端提供服务的请求被集中化管理器从多个接入节点中的第一接入节点接收到。所述多个接入节点中的每个接入节点被配置为向一个或多个客户端提供服务。所述集中化管理器在一个实施例中可由 AAA 服务器实现。

[0021] 集中化管理器从多个存储的策略中选择适用于所述第一接入节点的接入策略。集中化管理器基于所选接入策略来确定是否允许第一接入节点向无线客户端提供服务。

[0022] 在确定出所选接入策略允许第一接入节点向无线客户端提供服务时,指令第一接入节点向该无线客户端提供服务的消息被发送到第一接入节点。但是,在确定出所选接入策略不允许第一接入节点向该无线客户端提供服务时,指令第一接入节点拒绝服务该无线客户端的消息被发送到第一接入节点。

[0023] 有利地是,实施例允许基于接入节点外存储的集中化信息确定特定的接入节点是否应当向特定的客户端提供服务。集中化信息可以被实现为在集中化管理器处存储的一组策略。在集中化管理器处存储的策略可以包括多种规则,例如多少无线客户端或者哪些无线客户端能够被一个接入节点服务。例如,该组策略可以包括仅允许可配置数目的客户端连接到特定接入节点的规则(例如,仅 10 个无线客户端可连接到接入节点 2)或者仅允许特定客户端(例如,与公司的 CEO 相关联的客户端)连接到特定接入节点的规则。

[0024] 体系结构概述

[0025] 图 1 是示出了其中可以实现一个实施例的示例无线网络布置的框图。用户 102 与客户端 104 相关联,客户端 104 通信耦合到公共网络 106 并且间接通信耦合到企业网络 110。公共网络 106 或企业网络 110 都可以是无线网络。

[0026] 无线网络可以使用 802.1x 无线通信协议,并且通常使用某种形式的用户认证协议。例如,可以使用 IETF RFC 2284 中定义的可扩展认证协议(EAP)。在描述 EAP 的 RFC 的术语中,客户端系统被称作“请求者(supplicant)”,并且在本文中客户端 104 就是这样的请求者。客户端 104 例如可以执行可从 Microsoft 获得的 802.1x 请求者。

[0027] 接入节点,例如接入节点 108A 和 108B,与集中化管理器 120 协作,控制对企业网络 110 的接入。如这里所使用的,接入节点指接入点(AP)。接入节点 108A 和 108B 可各自被称为 AAA 客户端,因为集中化管理器 120 为接入节点 108A 和 108B 的认证请求服务。接入节点 108A 和 108B 在一个实施例中各自可以是配置为执行接入控制功能的网络路由器。一个示例是可从 San Jose, California 的 Cisco Systems 公司购得的 Cisco Access Server AS5300。这里所述的遵循 EAP 的实施例可以利用任何具有 EAP 能力的平台实现,所述平台包括交换机、路由器、支持 VPN 的网络元件、无线网关、防火墙等。尽管在图 1 中仅示出了两个接入节点,即,接入节点 108A 和 108B,但是本领域技术人员应当理解可以采用任何数目的接入节点。

[0028] 客户端 104 是能够接收来自接入节点的无线服务的任何功能组件。客户端的非限制性的说明性示例包括个人计算机、工作站和无线设备。网络 106 可以是任何局域网、广域网、或者一个或多个互连网。企业网络 110 是容纳了客户端 104 寻求接入的一个或多个网

络资源 140 的任何网络,包括 WLAN。在某些实施例中,网络 106 和 110 可以是相同的;因此,图 1 欲广泛包括任何网络布置,其中非受信客户端 104 正寻求接入到容纳在安全网络中的资源 140。

[0029] 集中化管理器 120 是服务器类计算机,其被配置为安全地存储诸如用户名和口令之类的用户认证信息,并且执行认证协议、算法和支持过程,例如,一次口令 (OTP) 确认、加密和解密、消息摘要评价等。集中化管理器 120 可由执行例如由 AAA 服务器提供的认证、授权和记账服务的服务器实现。集中化管理器 120 的商业示例是来自 Cisco Systems 公司的 CiscoSecure Access Control Server。

[0030] 在一个实施例中,集中化管理器 120 利用安全协议与接入节点 108A 和 108B 通信,其中该安全协议是针对在认证中使用优化过的。适当的协议的一个示例是 RADIUS。

[0031] 集中化管理器 120 还可以执行图 2 的步骤,这些步骤在下面将被详细描述。

[0032] 可选地,策略服务器 130 被通信耦合到网络 110 和 / 或集中化管理器 120,或者被与集中化管理器集成。策略服务器 130 提供认证策略的仓库,集中化管理器 120 可以参考该仓库来确定如何与客户端 104 交互。例如,策略服务器 130 可以指定客户端 104 必须能够用于认证的最低要求认证方法,除了完成成功的认证外客户端必须给出的特定种类的证书,等等。

[0033] 在这种布置中,客户端 104 必须向与集中化管理器 120 协作的特定接入节点 (例如接入节点 108A) 成功地认证其自身,以获得对资源 140 的接入。可以使用若干种认证协议中的任何认证协议来执行认证。适当的认证协议的一个示例是 PEAP,该协议是作为在客户端 104 和接入节点 108A 之间建立 PPP 连接的一部分而被执行的遵循 EAP 的协议。在面向对象的环境中,定义作为认证协议的一部分执行的消息和动作的逻辑可以被构造为客户端 104 利用应用编程接口 (API) 114A 访问或调用的认证方法 112A。兼容的认证方法 112B 可由集中化管理器 120 利用 API 114B 调用。

[0034] 一般而言,根据 EAP,当客户端 104 尝试利用接入节点 108A 接入企业网络 110 时,接入节点 108A 与该客户端接触,并且请求身份信息,客户端在响应中提供该信息。因此,客户端 104 和接入节点 108A 建立了逻辑连接 130A。接入节点 108A 然后将认证协议中所包括的并且由客户端 104 发出的所有后续消息都传递给集中化管理器 120,并且将相关消息从认证服务器转发到该客户端。因此,客户端 104 和集中化管理器 120 实际上建立了逻辑连接 130B,直到认证协议终止为止。结果,集中化管理器 120 可以利用认证方法 112B 来确定其认证行为,因为其代表了认证协议会话的逻辑端点。

[0035] 平衡无线接入

[0036] 图 2 是示出了一个实施例的功能步骤的流程图。通过执行图 2 的步骤,基于在接入节点外存储的集中化信息确定出特定的接入节点是否应当向特定的客户端提供服务。在一个实施例中,集中化信息被存储在集中化管理器处。图 2 的步骤将在下面参考图 3 说明,图 3 是示出了一个实施例的功能组件的框图。

[0037] 最初,在步骤 210 中,请求向无线客户端提供服务的请求被接收到。步骤 210 的请求可以是响应于接入节点从无线客户端接收对服务的请求而从该接入节点 (在这里称作“请求接入节点”) 发送的。集中化管理器可以接收步骤 210 的请求。

[0038] 例如,图 3 示出了多个客户端 (客户端 310、312、314 和 316)、多个接入节点 (接入

节点 320、322、324 和 326) 以及集中化管理器 330。步骤 210 可由从接入节点 322 接收到请求向客户端 310 提供服务的请求的集中化管理器 330 执行。在执行了步骤 210 后,处理前进到步骤 220。

[0039] 在步骤 220 中,适用于第一接入节点的接入策略被选出。集中化管理器 330 可以通过从存储在集中化管理器 330 处或者集中化管理器 330 可访问的多个策略中选出一个接入策略(“被选接入策略”)来执行步骤 220 的选择。例如,如图 3 所示,集中化管理器 330 包括存储的策略 340,存储的策略 340 可以包含任何数目的策略。另外,被选接入策略也可以是从一组存储的策略中选出的,该组策略可以全部或部分存储在可由集中化管理器 330 访问的策略服务器(图 3 中未示出)处。

[0040] 策略的目的是定义一条或多条规则,这些规则可用来确定是否允许接入节点向无线客户端提供服务。如果一条策略有助于确定是否允许特定的接入节点向无线客户端提供服务,则该策略适用于该特定接入节点,例如,该策略可能包含与该策略适用于的特定接入节点相关联的一条或多条规则。

[0041] 选择被选接入策略可以基于在步骤 210 中接收到的请求中包含的接入节点身份信息而执行。接入节点身份信息是标识出发送了步骤 210 的请求的接入节点的信息。例如,在上述示例中,接入节点身份信息会标识出接入节点 322,因为接入节点 322 将步骤 210 的请求发送给集中化管理器 330。

[0042] 如图 3 所示,集中化管理器 330 存储 N 条策略(其中 N 是任何数目)。步骤 220 可由集中化管理器 330 选择策略 2 服务从接入节点 322 发送来的请求来执行。集中化管理器 330 在本示例中可能选择策略 2 是因为策略 2 可能包含与接入节点 322 相关联的一条或多条规则。集中化管理器 330 可以基于所存储的策略中的哪些与由接入节点身份信息标识出的接入节点相关联来选择策略。在执行了步骤 220 后,处理前进到步骤 230。

[0043] 在步骤 230 中,基于在步骤 220 中选出的被选接入策略来确定是否允许请求接入节点向无线客户端提供服务。在上述示例中,集中化管理器 330 可以通过基于在步骤 220 中选出的策略 2 确定是否允许接入节点 322 向无线客户端 310 提供服务来执行步骤 230。

[0044] 每个策略可以包括一条或多条规则,这些规则基于一组标准描述一个或多个接入节点是否被允许向一个或多个无线客户端提供服务。每个策略所考虑的标准集合可能变化。例如,标准集合可能是基于无线客户端的用户特性或者基于环境因素的。

[0045] 在一个实施例中,策略至少部分可以包括关于有多少无线客户端能够被一个或多个接入节点服务的一条或多条规则。例如,可以建立这样一条策略,其中一个特定的接入节点仅可以服务 10 个无线客户端。一旦该特定接入节点正服务 10 个客户端,则来自该特定接入节点的请求向额外的客户端提供服务的任何接收到的请求都将被该策略拒绝。在这种策略中,可由一个接入节点服务的无线客户端的数目可以是可配置的数目,例如,集中化管理器 330 的管理员可以对该策略进行配置来改变允许一个特定接入节点服务的无线客户端的数目。

[0046] 在另一个实施例中,策略至少部分可以包括关于哪些无线客户端可以被一个或多个无线接入节点服务的一条或多条规则。例如,可以建立这样一条策略,其中仅与特定个人(例如,公司的 CEO) 相关联的特定无线客户端可以被特定的接入节点所服务。

[0047] 关于客户端的用户或者客户端自身的信息可以被包含在在步骤 210 中接收到的

请求内包含的客户端标识数据中。客户端标识数据是标识出关于向接入节点请求服务的无线客户端或者该无线客户端的用户的一个或多个特性的数据。策略可以基于在客户标识数据中标识出的一个或多个特性,判定是否允许特定的接入节点向无线客户端提供服务。例如,策略可以基于在客户端标识数据中标识出的下面的特征中的一个或多个,判定是否允许特定接入节点向无线客户端提供服务,上述特征包括:用户的身份、与无线客户端的用户相关联的位置、或者与无线客户端的用户相关联的组织群组。

[0048] 在另一个实施例中,策略至少部分可以包括关于多个无线客户端中的一个或多个何时能够被一个或多个接入节点服务的一条或多条规则。例如,可以建立这样一条策略,其中一个或多个接入节点仅在周一到周五的9AM到5PM之间被允许服务客户端。可以对特定接入节点建立任何时间限制。

[0049] 在另一个实施例中,接入节点可以在逻辑上被组合到一起成为一个群组。标识一个或多个接入节点属于一个群组的数据可以被存储,例如,集中化管理器330可以存储标识一个或多个接入节点属于一个群组的群组数据。接入节点的群组可以是基于该群组中的接入节点的特性的。例如,一个群组中的每个接入节点可能物理位置彼此接近,可能每个被指派了特定的任务或功能,或者每个可能都共享类似的功能能力。策略可以被配置为包括考虑了该群组数据的一条或多条规则。

[0050] 例如,策略可以至少部分包括关于基于多少其他无线客户端正被与第一接入节点相关联的群组中的接入节点服务来判定是否允许第一接入节点向无线客户端提供服务的一条或多条规则。如果第一接入节点正接近但尚未达到峰值能力,并且在与第一接入节点相关联的群组中存在能够向在步骤210中接收到的请求中标识出的无线客户端提供的其他接入节点,则基于该群组中的其他接入节点之一将向该无线客户端提供服务的假设,策略可以拒绝第一接入节点向该无线客户端提供服务。上述策略仅是说明性的,因为其他实施例可以采用包括关于基于关于请求接入节点的群组的其他考虑,判定是否允许该请求接入节点向无线客户端提供服务的一条或多条规则的其他策略。

[0051] 在另一个实施例中,策略可以至少部分包括关于基于描述在第一接入节点处正在消耗的带宽多少的数据来判定是否允许第一接入节点向无线客户端提供服务的一条或多条规则。例如,集中化管理器330可以存储对在多个接入节点中的每个处正被消耗的带宽多少进行描述的数据。每个接入节点可以将关于在该接入节点处正被消耗的带宽多少的信息发送给集中化管理器330。这种信息可以以多种格式获得,例如,其可以被包括在在步骤210中接收到的请求中,其可以由接入节点周期性地并且异步地发送到在步骤210中接收到的请求,或者集中化管理器330可以周期性地轮询每个接入节点。

[0052] 尽管上面描述了以各种策略为特征的若干实施例,但是本领域技术人员应当理解,这里所述的策略仅是说明性的,并且集中化管理器330可以采用任何策略来确定是否允许请求接入节点向与请求相关联的无线客户端提供服务。

[0053] 如果被选接入策略允许请求接入节点向与请求相关联的无线客户端提供服务,则处理前进到步骤240。但是,如果被选接入策略不允许请求接入节点向与请求相关联的无线客户端提供服务,则处理前进到步骤250。

[0054] 在步骤240中,确定出被选接入策略允许请求接入节点向无线客户端提供服务后,指令请求接入节点向无线客户端提供的消息从集中化管理器330发送到请求接入

节点。在请求接入节点接收到该消息后,第一接入节点就可以向无线客户端提供服务。在上述示例中,步骤 240 可通过集中化管理器 330 向接入节点 322 发送指令接入节点 322 向客户端 310 提供服务的消息来执行。

[0055] 在步骤 250 中,确定出被选接入策略不允许请求接入节点向无线客户端提供服务后,指令请求接入节点拒绝服务该无线客户端的消息从集中化管理器 330 被发送到请求接入节点。在请求接入节点接收到该消息后,请求接入节点发送第二消息到请求服务的无线客户端,向该无线客户端指示服务被拒绝。在上述示例中,步骤 250 可通过集中化管理器 330 向接入节点 322 发送指令接入节点 322 拒绝服务客户端 310 的消息来执行。

[0056] 在一个实施例中,一旦对无线客户端的服务被特定接入节点拒绝,该无线客户端就存储标识出特定接入节点拒绝了服务的数据。所存储的数据可由无线设备在确定该无线设备接下来应当尝试连接哪个接入节点时使用。无线设备使用算法来确定要连接到哪个接入节点,但是忽略已拒绝服务该无线设备的任何接入节点,以确保该无线设备不继续尝试相同的接入节点。一旦无线设备确定出接下来将尝试连接到哪个接入节点(“第二接入节点”),则无线设备可以发送请求服务的请求到该第二接入节点。第二接入节点可以发送请求向该无线客户端提供服务的请求到集中化管理器 330。集中化管理器 330 然后重复图 2 的功能步骤来处理来自第二接入节点的请求。

[0057] 有利地是,实施例允许基于在接入节点外存储的集中化信息来确定特定的接入节点是否应当向特定的客户端提供服务。利用本发明的实施例,网络管理员可以定义用于无线网络的负载平衡和服务质量(QoS)策略。因此,除了传统的AAA策略,例如,认证、授权和记账外,集中化管理器的存储的策略可以基于负载平衡或QoS考虑。

[0058] 预认证消息

[0059] IEEE 802.11i 安全性标准已定义了称作“预认证(pre-authentication)”的可选关联阶段。预认证被设计为允许请求者在建立到特定接入节点的直接关联之前,建立与多个接入节点的安全性关联。预认证有利地提高了在移动环境中将请求者重关联到新的接入节点的性能,因为新的接入节点无需执行请求者的完整重认证的全部协议开销。

[0060] 这里所使用的“预认证消息”指从客户端发送到一个或多个接入节点的用于在发送客户端和接收接入节点之间建立安全性关联的请求。例如,200个人可能位于特定的区域内开会。这200个人中的每个人都可能试图利用无线设备连接到网络。200个无线设备中的每个可能发送预认证消息到5个不同的接入节点。

[0061] 当特定的接入节点接收到预认证消息时,该特定的接入节点与集中化管理器 120 通信,以告知集中化管理器 120 该特定节点接收到了预认证消息。集中化管理器 120 进而可以基于一个或多个策略来确定如何处理该特定接入节点接收到的预认证消息。在一个实施例中,集中化管理器 120 可以基于在该集中化管理器处存储的或者该集中化管理器可访问的考虑了关于在多个接入节点处接收到的预认证消息的信息的一个或多个策略,确定如何处理由该特定节点接收到的预认证消息。在集中化管理器 120 基于该一个或多个策略确定了如何处理预认证请求后,集中化管理器 120 将该判决传输到接收了预认证消息的特定接入节点。

[0062] 如上所述,集中化管理器 120 在对从接入节点发送来的请求向客户端提供服务的请求进行处理时,可以参考一个或多个策略。当处理请求向客户端提供服务的请求时,集中

化管理器 120 可以参考一个或多个策略,这些策略包括考虑了关于在多个接入节点处接收到的预认证消息的信息的一条或多条规则。

[0063] 本发明的实施例可以采用这样的集中化管理器 120,该集中化管理器 120 选择包括考虑了由多个接入节点接收到的预认证消息的一条或多条规则的接入策略。例如,可以建立这样的策略,该策略通过对已在一个接入节点处接收到的一组预认证消息进行评估,并且尝试基于在多个接入节点处接收到的预认证消息的集合来均匀分布已被授权或预授权在特定节点处接收服务的客户端的量,从而使网络上的负载最小化。在上述包括 200 个人的示例中,如果 200 个无线客户端中的每个发送预认证消息到 5 个不同的接入节点,并且此后集中化管理器 120 接收来自一组接入节点的关于已接收到 1000 (200×5) 个预认证消息的通知,则集中化管理器 120 可以向该组接入节点传达:5 个特定接入节点可预认证 40 个无线客户端。其他实施例可以采用考虑了由多个接入节点接收到的预认证消息的其他策略,这些实施例尝试基于由多个接入节点接收到的预认证消息,最优地准予或拒绝从某个接入点服务客户端。

[0064] 实现机构

[0065] 客户端 104、接入节点 108A 和 108B、集中化管理器 120 和策略服务器 130 在一个实施例中每个都可以被实现在计算机系统上。图 4 是示出了其上可以实现一个实施例的计算机系统 400 的框图。计算机系统 400 包括总线 402 或其他通信机构用于传输信息,以及与总线 402 耦合用于处理信息的处理器 404。计算机系统 400 还包括耦合到总线 402 用于存储信息和要被处理器 404 执行的指令的主存储器 406,例如,随机存取存储器 (RAM) 或者其他动态存储器件。主存储器 406 还可以用于在执行要由处理器 404 执行的指令期间存储临时变量或其他中间信息。计算机系统 400 还包括耦合到总线 402 用于存储静态信息和用于处理器 404 的指令的只读存储器 (ROM) 408 或其他静态存储器件。存储设备 410 例如磁盘或光盘被提供并且耦合到总线 402 用于存储信息和指令。

[0066] 计算机系统 400 可以经由总线 402 耦合到显示器 412,例如,阴极射线管 (CRT),用于向计算机用户显示信息。包括字母数字和其他按键的输入设备 414 被耦合到总线 402 用于向处理器 404 传输信息和命令选择。另一类用户输入设备是光标控制设备 416,例如,鼠标、跟踪球、或者光标方向键,用于向处理器 404 传输方向信息和命令选择,以及用于控制光标在显示器 412 上移动。这种输入设备一般具有在两个轴 (第一轴,例如, x ;和第二轴,例如, y) 上的两个自由度,其允许该设备指定平面中的位置。

[0067] 本发明涉及使用用于实现这里所述技术的计算机系统 400。根据本发明的一个实施例,这些技术由计算机 400 响应于处理器 404 执行主存储器 406 中包含的一条或多条指令的一个或多个序列而被执行。这些指令可以从另一机器可读介质例如存储设备 410 读入到主存储器 406 中。执行主存储器 406 中包含的指令的序列致使处理器 404 执行这里所述的过程步骤。在替换实施例中,硬连线电路可以被用来替换软件指令或者与软件指令结合来实现本发明。因此,本发明的实施例不限于硬件电路和软件的任何特定组合。

[0068] 这里所使用的术语“机器可读介质”指参与提供致使机器以特定方式操作的数据的任何介质。在利用计算机系统 400 实现的一个实施例中,各种机器可读介质被包括来例如向处理器 404 提供指令以执行。这种介质可以采取任何形式,包括但不限于非易失性介质、易失性介质和传输介质。非易失性介质包括例如光盘或磁盘,例如,存储设备 410。易失

性介质包括动态存储器,例如主存储器 406。传输介质包括同轴电缆、铜缆和光纤,包括包含总线 402 在内的线路。传输介质也可以采取声波或光波的形式,例如,在无线电波和红外数据通信期间产生的那些。

[0069] 机器可读介质的常见形式包括例如软盘、柔性盘、硬盘、磁带、或者任何其他磁介质, CD-ROM、任何其他光介质,穿孔卡、纸带、具有孔图案的任何其他物理介质, RAM、PROM、EPROM、FLASH-EPROM、任何其他存储器芯片或带盒,后面所述的载波,或者计算机可读取的任何其他介质。

[0070] 计算机可读介质的各种形式可以用来传送一条或多条指令的一个或多个序列到处理器 404 用于执行。例如,指令最初可承载在远程计算机的磁盘上。该远程计算机可以将指令载入到其动态存储器中,然后利用调制解调器通过电话线发送这些指令。计算机系统 400 本地的调制解调器可以在电话线上接收数据,然后利用红外发射器将该数据转换成红外信号。红外检测器可以接收红外信号中携带的数据,并且适当的电路可以将数据放置到总线 402 上。总线 402 将数据传送到主存储器 406,处理器 404 从总线 406 提取指令并且执行这些指令。可选地,由主存储器 406 接收到的指令可以在被处理器 404 执行之前或之后被存储在存储设备 410 上。

[0071] 计算机系统 400 还可以包括耦合到总线 402 的通信接口 418。通信接口 418 提供耦合到被连接到本地网络 422 的网络链路 420 的双向数据通信。例如,通信接口 418 可以是提供到相应类型的电话线的数据通信连接的综合业务数字网 (ISDN) 卡或者调制解调器。又例如,通信接口 418 可以是提供到兼容 LAN 的数据通信连接的局域网 (LAN) 卡。也可以实现无线链路。在任何这种实现方式中,通信接口 418 发送和接收携带代表各种类型信息的数字数据流的电、电磁或光信号。

[0072] 网络链路 420 一般通过一个或多个网络提供到其他数据设备的数据通信。例如,网络链路 420 可以通过本地网络 422 提供到主机计算机 424 或者到由因特网提供商 (ISP) 426 操作的数据设备的连接。ISP 426 进而通过现在通常称作“因特网”428 的全球分组数据通信网络提供数据通信服务。本地网络 422 和因特网 428 都使用携带数字数据流的电、电磁或光信号。通过各种网络的信号和网络链路 420 上的并且通过通信接口 418 的信号(其携带着去往和来自计算机系统 400 的数字数据)都是传输信息的载波的示例性形式。

[0073] 计算机系统 400 可以通过(一个或多个)网络、网络链路 420 和通信接口 418 发送消息和接收数据,其中包括程序代码。在因特网示例中,服务器 430 可以通过因特网 428、ISP 426、本地网络 422 和通信接口 418 发送针对应用程序的所请求代码。

[0074] 所接收到的代码可以在其被接收到时由处理器 404 执行,并且/或者被存储在存储设备 410 或者其他非易失性存储设备中以便以后执行。这样,计算机系统 400 可以以载波形式获得应用代码。

[0075] 在前面的说明中,已结合可能随实现方式而变的许多特定细节描述了本发明的实施例。因此,本发明的内容以及申请人期望的本发明的内容的唯一并且排他的指示存在于通过本申请而授权的授权形式(包括任何后续补正)的权利要求中。这里明确给出的对包含在这种权利要求中的术语的定义应当约束这种术语在权利要求中使用时的含义。因此,未在权利要求中明确记载的限制、元素、特性、特征、优点和属性不应当以任何方式限制这

些权利要求的范围。因此,说明书和附图应当被认为是说明性的而非限制性的。

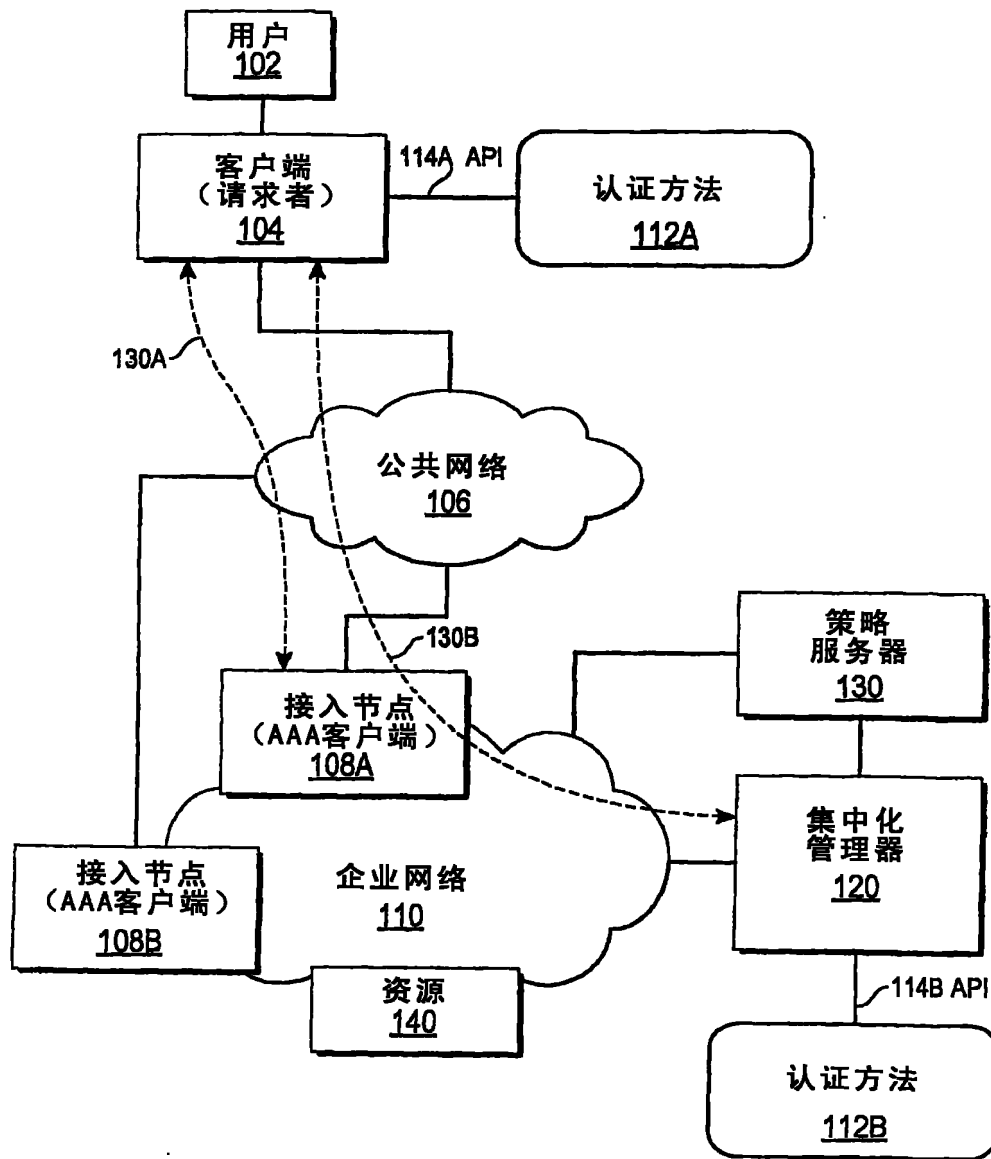


图 1

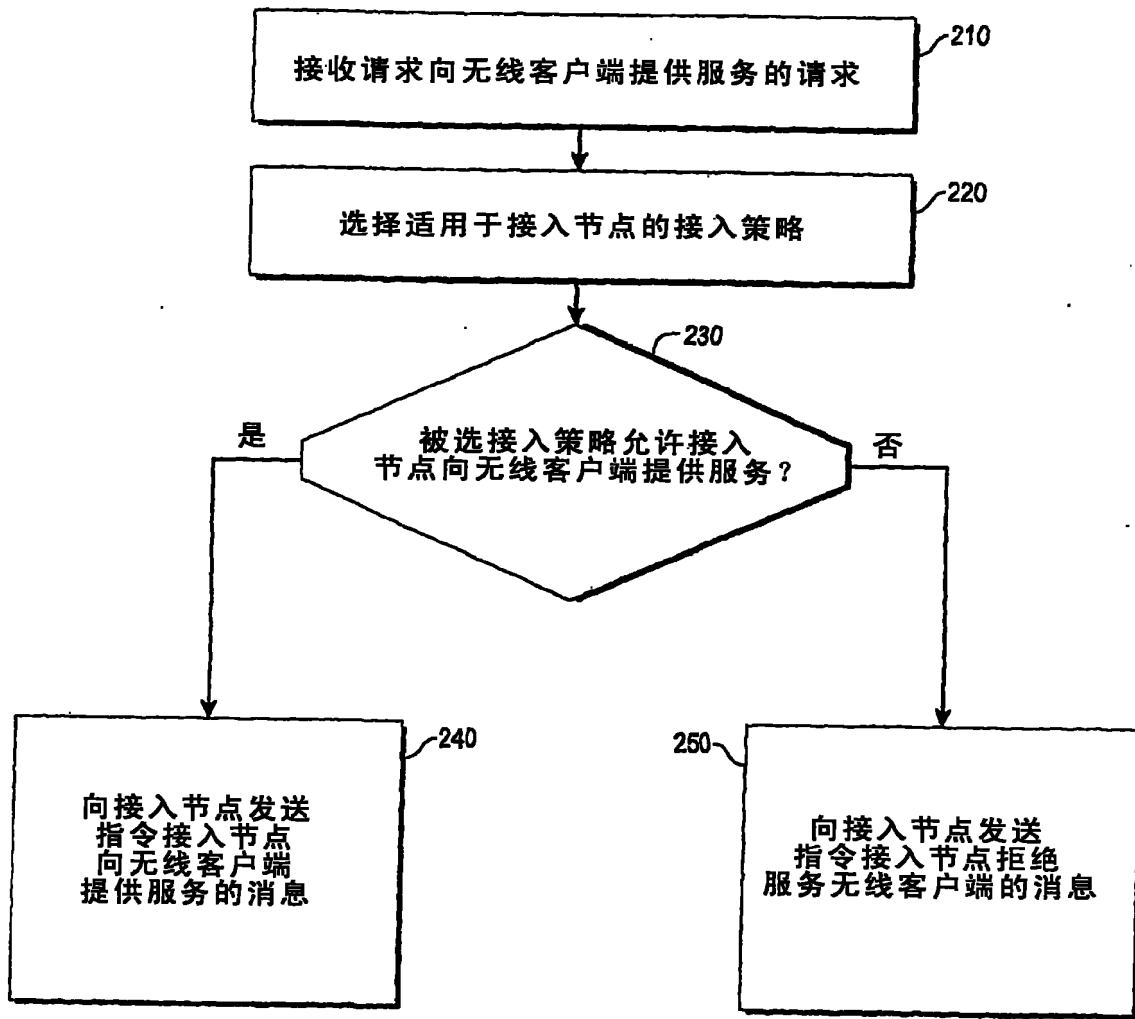


图 2

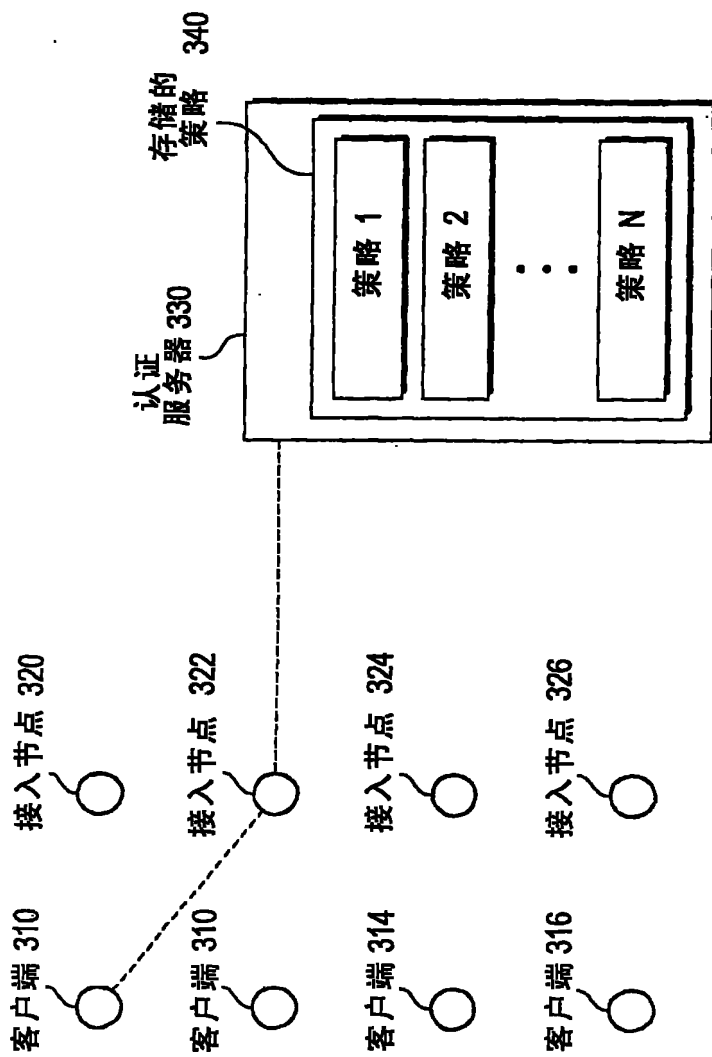


图3

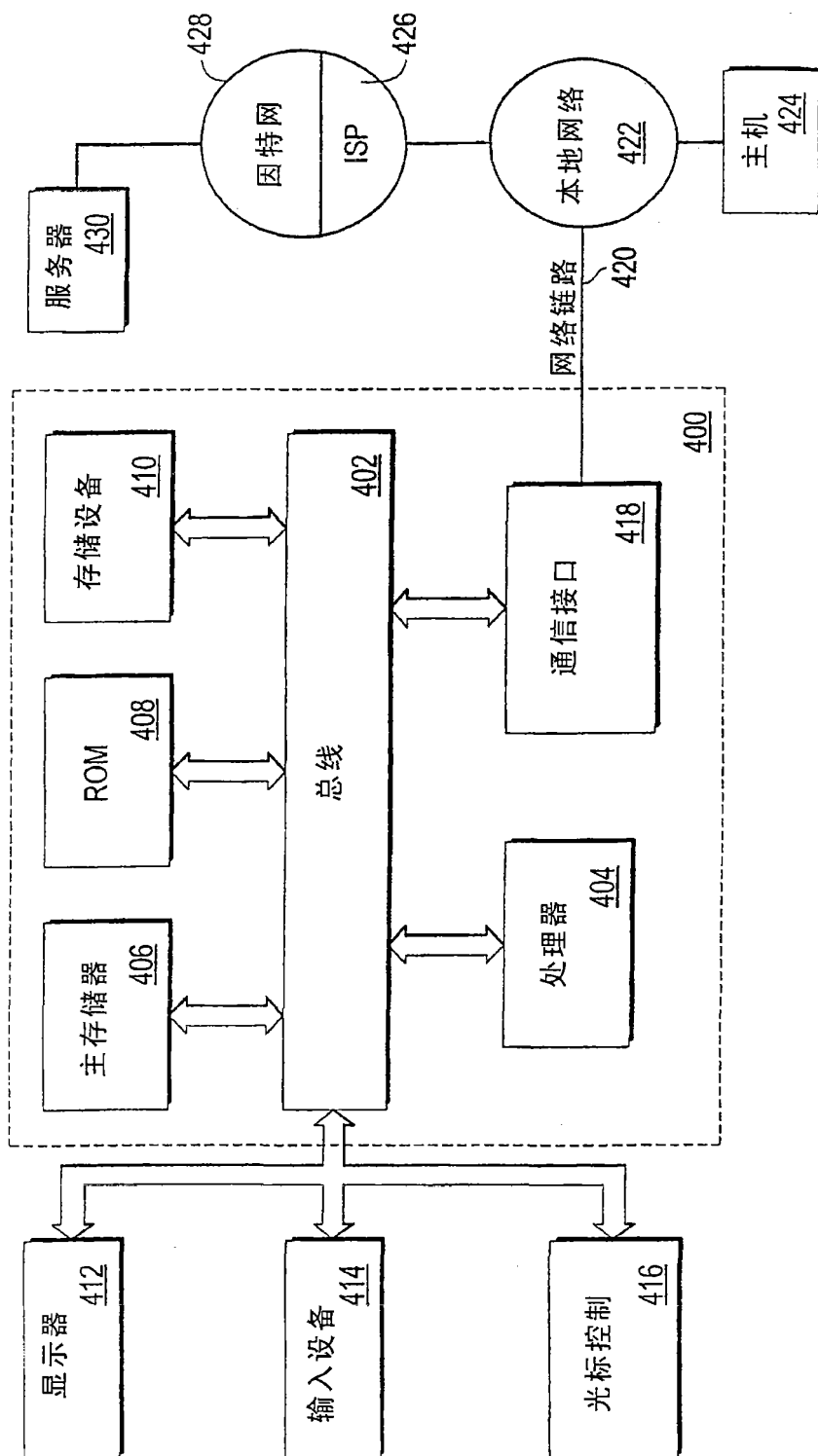


图4