

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 8 月 18 日 (18.08.2016)



(10) 国际公布号
WO 2016/127914 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01) H04L 29/08 (2006.01)
- (21) 国际申请号: PCT/CN2016/073507
- (22) 国际申请日: 2016 年 2 月 4 日 (04.02.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510080975.4 2015 年 2 月 13 日 (13.02.2015) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 王淑香 (WANG, Shuxiang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 高红亮 (GAO, Hongliang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

- 关于申请人有权申请并被授予专利(细则 4.17(ii))

本国际公布:

- 包括国际检索报告(条约第 21 条(3))。

(54) Title: REDIRECTION METHOD, APPARATUS, AND SYSTEM

(54) 发明名称: 一种用于重定向的方法、装置及系统

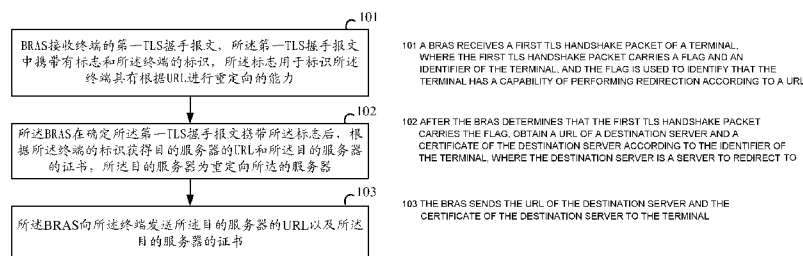


图 1

(57) Abstract: This application provides a redirection method, apparatus, and system, so as to improve a success rate of redirection. The method comprises: a broadband remote access server (BRAS) receiving a first transport layer security (TLS) handshake packet of a terminal, where the first TLS handshake packet carries a flag and an identifier of the terminal, and the flag is used to identify that the terminal has a capability of performing redirection according to a uniform resource locator (URL); after the BRAS determines that the first TLS handshake packet carries the flag, obtaining a URL of a destination server and a certificate of the destination server according to the identifier of the terminal, where the destination server is a server to redirect to; and the BRAS sending the URL of the destination server and the certificate of the destination server to the terminal. After determining that the URL of the destination server matches the certificate of the destination server, the terminal may output information used to prompt that access will be redirected.

(57) 摘要: 本申请提供了一种用于重定向的方法、装置及系统, 用以提高重定向的成功率。该方法中, 宽带远程接入服务器 BRAS 接收终端的第一传输层安全 TLS 握手报文, 第一 TLS 握手报文中携带有标志和所述终端的标识, 所述标志用于标识所述终端具有根据统一资源定位符 URL 进行重定向的能力; 所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后, 根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书, 所述目的服务器为重定向所述服务器; 所述 BRAS 向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书。所述终端在确定所述目的服务器的 URL 以及所述目的服务器的证书匹配后, 可输出用于提示访问将被重定向的信息。



WO 2016/127914 A1

一种用于重定向的方法、装置及系统

本申请要求于 2015 年 2 月 13 日提交中国专利局、申请号为 CN 201510080975.4、发明名称为“一种用于重定向的方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明涉及通信技术领域，尤其涉及一种用于重定向的方法、装置及系统。

10 背景技术

宽带远程接入服务器（Broadband Remote Access Server，BRAS）中，存在多种需要将终端的万维网（英文名称为 Web）页面访问重定向到运营商服务器的场景。

例如，终端访问任意的网站时，所述任意的网站目的地址不是运营商的 Web 服务器（英文名称为 Web Server），所述终端的访问被 BRAS 重定向到运营商的 Web 认证页面，即所述运营商的 Web Server 对所述终端进行 Web 认证。而目前，所述终端的访问被所述 BRAS 重定向到运营商的 Web 认证页面之前，所述终端会因为从所述 BRAS 获得的证书与所述终端所访问的网站不匹配，而输出用于提示证书有问题的告警信息，使得采用所述终端的用户关闭包括
15 所述告警信息的页面。这样，所述终端的访问无法被 BRAS 成功地重定向到运营商的 Web 认证页面，使得所述终端无法实现重定向对应的业务。
20

发明内容

本发明实施例提供一种用于重定向的方法、装置及系统，有助于提高重
25 定向的成功率。

本发明实施例提供的具体技术方案如下：

第一方面，提供了一种用于重定向的方法，包括：

BRAS 接收终端发送的第一传输层安全 (Transport Layer Security, TLS) 握手报文, 所述第一 TLS 握手报文中携带有标志和所述终端的标识, 所述标志用于标识所述终端具有根据统一资源定位符 (Uniform Resource Locator, URL) 进行重定向的能力;

- 5 所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后, 根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书, 所述目的服务器为重定向所达的服务器;

所述 BRAS 向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书。

- 10 在上述第一方面的第一种可能的实现方式中, 所述 BRAS 根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书包括:

所述 BRAS 根据所述终端的标识, 获得预先配置的表项, 所述表项包括所述终端的标识、所述目的服务器的 URL 和所述目的服务器的证书;

- 15 所述 BRAS 从所述表项中, 获得所述目的服务器的 URL 和所述目的服务器的证书。

结合上述第一方面或第一方面的第一种可能的实现方式, 还提供了第一方面的第二种可能的实现方式, 所述 BRAS 向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书包括:

- 20 所述 BRAS 向所述终端发送第二 TLS 握手报文, 所述第二 TLS 握手报文携带所述目的服务器的 URL 和所述目的服务器的证书。

结合上述第一方面或第一方面的第一种可能的实现方式, 还提供了第一方面的第三种可能的实现方式, 所述 BRAS 向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书包括:

- 25 所述 BRAS 向所述终端发送服务器重定向 Server Redirect 报文, 所述 Server Redirect 报文携带所述目的服务器的 URL;

所述 BRAS 向所述终端发送服务器认证 Server Certificate 报文, 所述 Server Certificate 报文携带所述目的服务器的证书。

结合上述第一方面、第一方面的第一种可能的实现方式、第一方面的第二种可能的实现方式或第一方面的第三种可能的实现方式，还提供了第一方面的第四种可能的实现方式，还包括：

所述 BRAS 接收所述终端发送第一 HTTPS 报文，所述第一 HTTPS 报文用于向所述 BRAS 请求重定向的信息，所述第一 HTTPS 报文包括所述终端的标识；

所述 BRAS 根据所述终端的标识，获得所述第二服务器的 URL；

所述 BRAS 向终端发送第二 HTTPS 报文，所述第二 HTTPS 报文包括所述第二服务器的 URL。

第二方面，提供了一种用于重定向的方法，包括：

终端向 BRAS 发送第一 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于标识所述终端具有根据 URL 进行重定向的能力；

所述终端接收所述 BRAS 发送的目的服务器的 URL 和所述目的服务器的证书，所述目的服务器为重定向所达的服务器；

所述终端判断所述目的服务器的 URL 与所述目的服务器的证书是否匹配；

若所述目的服务器的 URL 与所述目的服务器的证书匹配，则所述终端输出第一提示信息，所述第一提示信息用于提示访问将被重定向，所述访问为所述终端对所请求的服务器的访问。

在上述第二方面的第一种可能的实现方式中，还包括：

若所述目的服务器的 URL 与所述目的服务器的证书不匹配，则所述终端输出第二提示信息，所述第二提示信息用于提示所述目的服务器的证书错误。

结合上述第二方面或第二方面的第一种可能的实现方式，还提供了第二方面的第二种可能的实现方式，所述终端接收所述 BRAS 发送的目的服务器的 URL 和所述目的服务器的证书包括：

所述终端接收所述 BRAS 发送的第二 TLS 握手报文，所述第二 TLS 握手

报文中携带所述目的服务器的 URL 和所述目的服务器的证书;

所述终端从所述第二 TLS 握手报文中获得所述目的服务器的 URL 和所述目的服务器的证书。

结合上述第二方面或第二方面的第一种可能的实现方式中, 还提供了第二方面的第三种可能的实现方式, 所述终端接收所述 BRAS 发送的目的服务器的 URL 和所述目的服务器的证书包括:

所述终端接收所述 BRAS 发送的服务器重定向 Server Redirect 报文, 所述 Server Redirect 报文携带所述目的服务器的 URL;

所述终端从所述 Server Redirect 报文获得所述目的服务器的 URL;

所述终端接收所述 BRAS 发送服务器认证 Server Certificate 报文, 所述 Server Certificate 报文携带所述目的服务器的证书;

所述终端从所述 Server Certificate 报文获得所述目的服务器的证书。

结合上述第二方面、第二方面的第一种可能的实现方式、第二方面的第二种可能的实现方式或第二方面的第三种可能的实现方式, 还提供了第二方面的第四种可能的实现方式, 还包括:

所述终端向所述 BRAS 发送第一 HTTPS 报文, 所述第一 HTTPS 报文用于向所述 BRAS 请求重定向的信息, 所述第一 HTTPS 报文包括所述终端的标识;

所述终端接收所述 BRAS 发送的第二 HTTPS 报文, 所述第二 HTTPS 报文包括所述第二服务器的 URL;

所述终端在获得用于指示进行重定向的指令后, 根据所述第二服务器的 URL 访问所述第二服务器。

第三方面, 提供了一种 BRAS, 所述 BRAS 包括:

接收模块, 用于接收终端发送的第一 TLS 握手报文, 所述第一 TLS 握手报文中携带有标志和所述终端的标识, 所述标志用于标识所述终端具有根据 URL 进行重定向的能力, 所述目的服务器为重定向所达的服务器;

获得模块, 用于在确定所述第一 TLS 握手报文携带所述标志后, 根据所

述终端的标识获得目的服务器的 URL 和所述目的服务器的证书，所述目的服务器为重定向所达的服务器；

发送模块，用于向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书。

- 5 在上述第三方面的第一种可能的实现方式中，所述获得模块具体用于根据所述终端的标识，获得预先配置的表项，所述表项包括所述终端的标识、所述目的服务器的 URL 和所述目的服务器的证书；

所述获得模块具体用于从所述表项中，获得所述目的服务器的 URL 和所述目的服务器的证书。

- 10 结合上述第三方面或第三方面的第一种可能的实现方式，还提供了第三方面的第二种可能的实现方式，所述发送模块具体用于向所述终端发送第二 TLS 握手报文，所述第二 TLS 握手报文中携带所述目的服务器的 URL 和所述目的服务器的证书。

- 15 结合上述第三方面或第三方面的第一种可能的实现方式，还提供了第三方面的第三种可能的实现方式，所述发送模块具体用于向所述终端发送服务器重定向 Server Redirect 报文，所述 Server Redirect 报文携带所述目的服务器的 URL；

所述发送模块具体用于向所述终端发送服务器认证 Server Certificate 报文，所述 Server Certificate 报文携带所述目的服务器的证书。

- 20 结合上述第三方面、第三方面的第一种可能的实现方式、第三方面的第二种可能的实现方式或第三方面的第三种可能的实现方式，还提供了第三方面的第四种可能的实现方式，

- 所述接收模块还用于接收所述终端发送第一 HTTPS 报文，所述第一 HTTPS 报文用于向所述 BRAS 请求重定向的信息，所述第一 HTTPS 报文包
25 括所述终端的标识；

所述获得模块还用于根据所述终端的标识，获得所述第二服务器的 URL；
所述发送模块还用于向终端发送第二 HTTPS 报文，所述第二 HTTPS 报

文包括所述第二服务器的 URL。

第四方面，提供了一种终端，包括：

发送模块，用于向 BRAS 发送第一 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于标识所述终端具有根据
5 URL 进行重定向的能力；

接收模块，用于接收所述 BRAS 发送的目的服务器的 URL 和所述目的服务器的证书，所述目的服务器为重定向所达的服务器；

判断模块，用于判断所述目的服务器的 URL 与所述目的服务器的证书是否匹配；

10 输出模块，用于在所述判断模块确定所述目的服务器的 URL 与所述目的服务器的证书匹配，输出第一提示信息，所述第一提示信息用于提示访问将被重定向，所述访问为所述终端对所请求的服务器的访问。

在上述第四方面的第一种可能的实现方式中，所述输出模块还用于在所述判断模块确定所述目的服务器的 URL 与所述目的服务器的证书不匹配，输出
15 第二提示信息，所述第二提示信息用于提示所述目的服务器的证书有问题。

结合上述第四方面或第四方面的第一种可能的实现方式，还提供了第四方面的第二种可能的实现方式，所述接收模块具体用于接收所述 BRAS 发送的第二 TLS 握手报文，所述第二 TLS 握手报文中携带所述目的服务器的 URL 和所述目的服务器的证书。

20 结合上述第四方面或第四方面的第一种可能的实现方式，还提供了第四方面的第三种可能的实现方式，所述接收模块具体用于接收所述 BRAS 发送的服务器重定向 Server Redirect 报文，所述 Server Redirect 报文携带所述目的服务器的 URL；

所述接收模块具体用于接收所述 BRAS 发送服务器认证 Server Certificate
25 报文，所述 Server Certificate 报文携带所述目的服务器的证书。

结合上述第四方面、第四方面的第一种可能的实现方式、第四方面的第二种可能的实现方式或第四方面的第三种可能的实现方式，还提供了第四方

面的第四种可能的实现方式，还包括：重定向模块；

所述发送模块还用于向所述 BRAS 发送第一 HTTPS 报文，所述第一 HTTPS 报文用于向所述 BRAS 请求重定向的信息，所述第一 HTTPS 报文包括所述终端的标识；

5 所述接收模块还用于接收所述 BRAS 发送的第二 HTTPS 报文，所述第二 HTTPS 报文包括所述第二服务器的 URL；

所述重定向模块还用于在获得用于指示进行重定向的指令后，根据所述第二服务器的 URL 访问所述第二服务器。

第五方面，提供了一种用于重定向的系统，包括：上述第三方面或第三
10 方面的任意一种可能的实现方式所提供的 BRAS 和上述第四方面或第四方面的任意一种可能的实现方式所提供的终端。

基于上述技术方案，本发明实施例中，BRAS 通过判断终端的第一 TLS 握手报文中是否携带标志；所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后，确定所述标志对应的所述终端支持 URL 的重定向功能；所述 BRAS 可在
15 确定所述标志对应的所述终端支持 URL 的重定向功能后，向所述终端发送与所述终端对应的目的服务器的 URL 以及所述目的服务器的证书。所述终端在确定所述目的服务器的 URL 以及所述目的服务器的证书匹配后，获取并输出第一提示信息，从而避免了终端将该重定向所达的服务器的证书与所请求访问的服务器的 URL 进行匹配，所述终端输出安全告警页面而误导用户关闭页
20 面，提高了重定向的成功率。

附图说明

图 1 为本发明实施例中用于重定向的方法流程图；

图 2 为本发明实施例中用于重定向的方法流程图；

25 图 3 为本发明实施例中 HTTPS 重定向过程示意图；

图 4 为本发明实施例中另一 HTTPS 重定向过程示意图；

图 5 为本发明实施例中 BRAS 结构示意图；

图 6 为本发明实施例中另一 BRAS 结构示意图；

图 7 为本发明实施例中终端结构示意图；

图 8 为本发明实施例中另一终端结构示意图；

图 9 为本发明实施例中用于重定向的系统的示意图。

5

具体实施方式

以超文本传输协议（Hypertext Transfer Protocol, HTTP）实现重定向的过程为例进行说明。

终端，如个人电脑（Personal Computer, PC），向 BRAS 发送访问请求，
10 所述访问请求的目的地址是所述终端请求访问的服务器的地址。所述终端请求访问的服务器可以不是运营商的 Web Server。所述 BRAS 可代替所述终端所请求访问的服务器，与所述终端建立传输控制协议（Transmission Control Protocol, TCP）连接。所述 BRAS 在收到所述终端的 GET HTTP 报文或 POST HTTP 报文后，向所述终端发送重定向报文（英文名称为 Redirect Packet）。所
15 述 GET HTTP 报文用于从指定的资源请求数据。所述 POST HTTP 报文用于向指定的资源提交数据。所述 Redirect Packet 中携带的目的服务器的 URL 为 Web Server 的 URL。所述目的服务器为重定向所达的服务器。

若所述 Web Server 和所述终端之间采用基于安全套接层（Secure Socket Layer, SSL）的超文本传输安全协议（Hypertext Transfer Protocol Secure, HTTPS），则所述 BRAS 可接收所述终端发送的传输层安全（Transport Layer Security, TLS）报文。所述 BRAS 可与所述终端完成 TLS 握手，并在完成所述 TCP 握手和 TLS 握手后，接收所述终端发送的加密的 Get HTTPs 报文或 Post HTTPs 报文。所述 BRAS 可向所述终端发送加密后的 Redirect Packet。所述 BRAS 与所述终端进行 TLS 握手的过程中，发送给所述终端的证书是所述
25 Web Server 的证书，即所述目的服务器为所述 Web Server。这样，所述终端在 TLS 握手阶段检查证书合法性时，会因为所述 Web Server 的证书与请求访问的网站域名不匹配而输出告警提示信息，使得终端无法显示正确的认证业务

或欠费重定向等相关业务页面。

针对上述问题，提出了有助于提高重定向的成功率的解决方法。该解决方法是 BRAS 接收终端发送的第一 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于标识所述终端具有根据 URL 进行重定向的能力；所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后，根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书，所述目的服务器为重定向所达的服务器；所述 BRAS 向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书。所述终端可在所述目的服务器的 URL 以及所述目的服务器的证书匹配后，输出用于提示重定向的提示信息。

本发明的实施例中，所述终端请求访问的服务器为第一服务器，第二服务器为重定向所达的服务器，所述第一服务器和所述第二服务器是不同的服务器。在所述终端满足重定向的条件时，所述终端对所述第一服务器的访问请求可被重定向为访问所述第二服务器，所述重定向的条件可以是 Web 认证或欠费提醒等运营商提供的与 Web 有关的业务。BRAS 可预配置有与所述终端对应的第二服务器的 URL 以及与所述终端对应的所述第二服务器的证书，比如 BRAS 可存储有与重定向相关的表项，所述与重定向相关的表项包括所述终端的标识、所述第二服务器的 URL 和所述第二服务器的证书。所述 BRAS 可以从认证、授权和计费（Authentication, Authorization and Accounting, AAA）服务器获得所述第二服务器的 URL 以及所述终端的标识。所述 BRAS 可从 AAA 服务器或其它网络设备获得所述第二服务器的证书，或所述 BRAS 可以根据 AAA 服务器或其它网络设备提供的用于生成证书的信息，生成所述第二服务器的证书，所述第二服务器的证书可包括所述第二服务器的 URL。所述 BRAS 可在获得所述第二服务器的 URL、所述第二服务器的证书和所述终端的标识后，生成或更新所述与重定向相关的表项。

本发明的实施例中，BRAS 中可以按照终端所属的认证域，为用户所采用的终端配置相应的第二服务器的 URL 以及所述第二服务器的证书。例如：Web 认证可包括认证前域和认证域。需要进行 Web 认证的终端可在所述认证前域

中被配置 Web 认证服务器的 URL。所述需要进行 Web 认证的终端先通过所述认证前域上线，BRAS 会将所述终端的 HTTP 访问重定向到所述 Web 认证服务器的 URL 对应的 Web 认证服务器。若用户在终端显示的由 Web 认证服务器提供的网页上输入用户名和密码，则所述终端就会通过所述认证域上线，

5 所述终端的 HTTP 访问不会被重定向。或者，AAA 服务器检测到该终端需要进行 URL 重定向的业务，例如需要欠费提醒，所述 AAA 服务器将该终端对应的第二服务器的 URL 以及所述第二服务器的证书发送给所述 BRAS，由 BRAS 进行与所述终端相关的重定向处理。

本发明实施例中所涉及的重定向可以为：所述终端通过所述 BRAS 访问

10 所述第一服务器时，所述 BRAS 在确定所述终端满足重定向的条件后，向所述终端发送所述第二服务器的 URL 和所述第二服务器的证书，以便所述终端访问所述第二服务器，完成与所述重定向的条件对应的业务。

本发明实施例中的终端可以是装设于手机、PC 或移动终端等设备上的浏览器或客户端，在此不再对终端进行逐一举例说明。

15 图 1 对应的实施例是从 BRAS 侧对用于重定向的方法进行说明。如图 1 所示，本发明实施例中用于重定向的方法如下：

101：BRAS 接收终端的第一 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于标识所述终端具有根据 URL 进行重定向的能力。

20 举例说明，所述终端具有根据 URL 进行重定向的能力可以为所述终端具有解析携带 URL 的报文的能力以及具有采用所述报文中的 URL 进行重定向的能力。比如，所述终端发送给所述 BRAS 的所述第一 TLS 握手报文中携带有所述标志，这就表示所述终端支持 HTTPS 重定向功能。

举例说明，所述终端发送给所述 BRAS 的第一 TLS 握手报文为 Client

25 Hello，该 Client Hello 中可包括扩展项，所述扩展项可用于携带所述标志。具体地，所述终端获得的 Client Hello 的净荷部分可携带所述标志，例如，在 Client Hello 净荷部分中用于扩展的部分增加扩展项，该扩展项携带所述标志。

举例说明，所述终端的标识可以是所述终端的媒体接入控制（Media Access Control, MAC）地址、互联网协议（Internet Protocol, IP）地址等用于标识所述终端的信息。

102: 所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后，根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书，所述目的服务器为重定向所述服务器。

举例说明，所述目的服务器可以为第二服务器。所述 BRAS 上可预先配置有与重定向相关的表项。所述与重定向相关的表项包括所述终端的标识、所述第二服务器的 URL 和所述第二服务器的证书。所述第二服务器的证书可包括所述第二服务器的 URL。

举例说明，所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后，确定所述终端支持重定向。所述 BRAS 可根据所述终端的标识进行本地查找，比如所述 BRAS 可查询是否存在包括所述终端的标识的与重定向相关的表项，若存在，则所述 BRAS 可从所述与重定向相关的表项中获得所述第二服务器 URL 和所述第二服务器的证书。所述第二服务器的证书可以是第二服务器向证书颁发中心（英文名称为 certificate authority，英文缩写为 CA）申请的证书。所述第二服务器的证书的生成方法可采用通常的证书生成方法，在此不再赘述。

举例说明，所述 BRAS 配置有所述终端的标识和所述第二服务器的 URL 之间的对应关系。所述 BRAS 可根据所述终端的标识和与所述终端的标识对应的所述第二服务器的 URL，生成或从其它网络设备获得所述第二服务器的证书。所述 BRAS 可根据所述第一 TLS 握手报文中携带的所述终端的标识，获得所述第二服务器 URL。所述 BRAS 生成所述第二服务器的证书的方式可采用通常的证书生成方式，在此不再赘述。

举例说明，所述 BRAS 根据所述终端的标识查找获得与重定向对应的表项的过程可以为所述 BRAS 确定所述终端满足重定向的条件，所述重定向的条件对应的业务为所述第二服务器提供的业务，比如 Web 认证业务或欠费提

醒业务。

103: 所述 BRAS 向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书。

举例说明, 所述 BRAS 可以是在向所述终端发送所述第二服务器的 URL 的同时, 发送所述第二服务器的证书, 比如: 所述 BRAS 向所述终端发送第二 TLS 握手报文, 该第二 TLS 握手报文可以为 Server Hello 报文, 所述 Server Hello 中携带所述第二服务器的 URL 以及所述第二服务器的证书。或者, 所述 BRAS 也可以向所述终端发送所述第二服务器的 URL 之后, 向所述终端发送所述第二服务器的证书, 比如: 所述 BRAS 向所述终端发送携带所述第二服务器的 URL 的服务器重定向 (英文名称为 Server Redirect) 报文, 然后向所述终端发送携带所述第二服务器的证书的服务器认证 (英文名称为 Server Certificate) 报文。

为了能够兼容通常的重定向过程, 103 之后, 本发明实施例提供的方法还可包括: 所述 BRAS 接收所述终端发送的第一 HTTPS 报文, 所述第一 HTTPS 报文用于向所述 BRAS 请求重定向的信息, 所述第一 HTTPS 报文可为 Get HTTPS 报文或 Post HTTPS 报文, 所述第一 HTTPS 报文包括所述终端的标识; 所述 BRAS 向终端发送第二 HTTPS 报文, 所述第二 HTTPS 报文可携带重定向的信息, 所述重定向的信息可包括所述第二服务器的 URL, 所述第二 HTTPS 报文可以为 Redirect HTTPS 报文。所述 BRAS 在与所述终端的 TLS 握手结束后, 可通过所述第二 HTTPS 报文, 向所述终端发送所述重定向的信息, 有助于所述终端根据该重定向的信息访问所述第二服务器。

举例说明, 所述终端也可在与所述 BRAS 的 TLS 握手后, 根据 TLS 握手过程中从所述 BRAS 获得的所述第二服务器 URL 访问所述第二服务器, 省略向所述 BRAS 发送所述第一 HTTPS 报文的过程。

举例说明, 如果所述第二服务器提供的业务为 Web 认证业务, 则所述第二 HTTPS 报文中的重定向的信息还可包括用于完成 Web 认证的信息, 所述用于完成 Web 认证的信息可以包括用户的 MAC 地址、用户物理位置信息等。

所述终端可根据所述重定向的信息访问所述第二服务器，将所述用于完成 Web 认证的信息发送给所述第二服务器，有助于所述第二服务器根据所述用于完成 Web 认证的信息对所述终端进行 Web 认证。

该实施例中，BRAS 通过判断终端发送的第一 TLS 握手报文中是否携带标识，所述标识用于标识所述终端具有根据 URL 进行重定向的能力，所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后，向所述终端发送与所述终端对应的目的服务器的 URL 以及与所述终端对应的目的服务器的证书，有助于终端根据该目的服务器的 URL 以及目的服务器的证书进行匹配的成功率，有助于提高重定向的成功率。

图 2 对应的实施例是从终端侧对用于重定向的方法进行说明。如图 2 所示，本发明实施例中用于重定向的方法如下：

201：终端向 BRAS 发送第一 TLS 握手报文，该第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于标识所述终端具有根据 URL 进行重定向的能力。

举例说明，所述终端具有根据 URL 进行重定向的能力可以为所述终端具有解析携带 URL 的报文的能力以及具有采用所述报文中的 URL 进行重定向的能力。比如，所述终端发送给所述 BRAS 的所述第一 TLS 握手报文中携带有所述标志，可表明所述终端支持 HTTPS 重定向功能。本发明实施例中的终端的标识可以与图 1 对应的实施例中的终端的标识相同，在此不再赘述。本发明实施例中的第一 TLS 握手报文可以与图 1 对应的实施例中的第一 TLS 握手报文相同，在此不再赘述。

举例说明，所述终端向所述 BRAS 发送所述第一 TLS 握手报文的目的是请求访问第一服务器。

202：所述终端接收 BRAS 发送的目的服务器的 URL 以及所述目的服务器的证书，所述目的服务器为重定向所达的服务器。

举例说明，所述目的服务器可以为第二服务器。所述第二服务器的 URL 以及所述第二服务器的证书可以为图 1 对应的实施例中的相应内容，在此不

再赘述。

举例说明，所述终端接收 BRAS 发送的目的服务器的 URL 以及所述目的服务器的证书包括：所述终端接收所述 BRAS 发送的 Server Redirect 报文，所述 Server Redirect 报文携带所述第二服务器的 URL；所述终端从所述 Server Redirect 报文获得所述第二服务器的 URL；所述终端接收所述 BRAS 发送的 Server Certificate 报文，所述 Server Certificate 报文携带所述第二服务器的证书；所述终端从所述 Server Certificate 报文获得所述第二服务器的证书。

举例说明，所述终端接收 BRAS 发送的目的服务器的 URL 以及所述目的服务器的证书包括：所述终端接收所述 BRAS 发送的第二 TLS 握手报文，所述第二 TLS 握手报文为 Server Hello 报文，所述 Server Hello 报文中携带所述第二服务器的 URL 以及所述第二服务器的证书；所述终端从所述 Server Hello 报文中获得所述第二服务器的 URL 以及所述第二服务器的证书。

203：所述终端判断所述目的服务器的 URL 与所述目的服务器的证书是否匹配，若所述目的服务器的 URL 与所述目的服务器的证书匹配，则执行 204。

举例说明，所述第二服务器的证书至少携带所述第二服务器的 URL，若所述第二服务器的证书中所携带的所述第二服务器的 URL 与所述终端接收到的所述第二服务器的 URL 相同，则所述终端确定所述第二服务器的证书与所述第二服务器的 URL 匹配。若所述第二服务器的证书中所携带的所述第二服务器的 URL 与所述终端接收到的所述第二服务器的 URL 不相同，则所述终端确定所述第二服务器的证书与所述第二服务器的 URL 不匹配。

204：所述终端输出第一提示信息，所述第一提示信息用于提示访问将被重定向，所述访问为所述终端对所请求的服务器的访问。

举例说明，所述终端所请求访问的服务器为第一服务器。所述访问为对所述第一服务器的访问。

举例说明，所述终端若确定所述第二服务器的 URL 与所述第二服务器的证书匹配，则所述终端可生成所述第一提示信息。所述终端可向用户输出所述第一提示信息。其中，所述终端向用户输出所述第一提示信息的方式包括：

所述终端生成包含所述第一提示信息的页面，所述终端显示所述包含所述第一提示信息的页面。

203 之后，本发明实施例提供的方法还包括：若所述目的服务器的 URL 与所述目的服务器的证书不匹配，则所述终端输出第二提示信息，所述第二
5 提示信息用于提示所述目的服务器的证书错误。

举例说明，所述终端若确定所述第二服务器的 URL 与所述第二服务器的证书不匹配，则所述终端可生成所述第二提示信息。所述终端可向用户输出所述第二提示信息。其中，所述终端向用户输出所述第二提示信息的方式包
括：所述终端生成包含所述第二提示信息的页面，所述终端显示所述包含所
10 述第二提示信息的页面。

204 之后，本发明实施例提供的方法还包括：所述终端在获取用户根据所述
第一提示信息输入的指示后，完成与所述 BRAS 的 TLS 握手过程，所述用
户输入的指示用于确认继续访问所述第二服务器的 URL；所述终端在 TLS 握
手过程后，向所述 BRAS 发送第一 HTTPS 报文，所述第一 HTTPS 报文用于
15 向所述 BRAS 请求重定向的信息，所述第一 HTTPS 报文包括所述终端的标识；
所述终端接收所述 BRAS 发送的第二 HTTPS 报文，所述第二 HTTPS 报文包
括所述重定向的信息，所述重定向的信息包括第二服务器的 URL；所述终端
根据所述重定向的信息，访问所述第二服务器的 URL 对应的服务器。

204 之后，本发明实施例提供的方法还包括：所述终端在获取用户根据所
20 述第一提示信息输入的指示后，所述指示用于确认继续访问所述第二服务器
的 URL，所述终端结束与所述 BRAS 的 TLS 握手过程；所述终端向所述 BRAS
发送所述第一 HTTPS 报文；所述终端接收到所述 BRAS 发送的所述第二
HTTPS 报文；所述终端根据所述重定向信息，访问所述第二服务器的 URL 对
应的服务器。

25 举例说明，本发明实施例提供的方法还包括：所述终端未接收到所述
BRAS 发送的所述第二 HTTPS 报文，结束重定向。

该实施例中，终端在向 BRAS 发送的第一 TLS 握手报文中携带标志，使

得 BRAS 根据该标志确定该终端具有根据 URL 进行重定向的能力，终端接收 BRAS 发送的目的服务器的证书以及目的服务器的 URL，根据该目的服务器的证书和该目的服务器的 URL 进行匹配，从而避免了终端检查所述目的服务器的证书合法性时，由于所述目的服务器的证书与所述终端请求访问的服务器的 URL 不匹配而导致重定向失败，有助于提高重定向的成功率。

以下通过两个实施例对本发明实施例中 HTTPS 重定向的过程进行详细说明如下：

第一实施例提供的进行 HTTPS 重定向的过程如图 3 所示：

终端，比如装设于终端的浏览器，在生成的 Client Hello 报文中携带名称为 redirect_url_enable 的扩展项和所述终端的标识，该扩展项的内容用于表示所述终端具有解析携带 URL 的报文的能力以及具有采用所述报文中的 URL 进行重定向的能力。

BRAS 接收到所述终端的 Client Hello 报文后，若确定所述 Client Hello 报文中携带名称为 redirect_url_enable 的扩展项，向所述终端发送 Server Hello 报文，所述 Server Hello 用于所述 BRAS 与所述终端协商确定加密方式等信息。所述 BRAS 根据所述 Client Hello 报文中携带的所述终端的标识，获得所述终端对应的第二服务器的 URL 和所述第二服务器的证书。所述 BRAS 向所述终端发送 Server Redirect 报文，所述 Server Redirect 报文携带所述第二服务器的 URL；所述 BRAS 向所述终端发送 Server Certificate 报文，所述 Server Certificate 报文包括所述第二服务器的证书。

所述终端收到所述 BRAS 发送的所述 Server Redirect 报文，从所述 Server Redirect 报文获得所述第二服务器的 URL。所述终端收到所述 BRAS 发送的所述 Server Certificate 报文，从所述 Server Certificate 报文获得所述第二服务器的 URL。所述终端判断所述第二服务器的证书与所述第二服务器的 URL 是否匹配，若所述第二服务器的证书与所述第二服务器的 URL 匹配，则所述终端生成并输出第一提示页面，所述第一提示页面用于提示访问将被重定向至所述第二服务器。若所述第二服务器的证书与所述第二服务器的 URL 不匹配，

则所述终端生成并输出第二提示页面，所述第二提示页面用于提示证书错误的告警页面。

若所述终端获取所述用户访问所述第二服务器的指示后，与所述 BRAS 完成 TLS 握手交互后，向 BRAS 发送 Get HTTPS 报文或 Post HTTPS 报文。

5 所述 Get HTTPS 报文或所述 Post HTTPS 报文可携带所述终端的标识。

所述 BRAS 与所述终端完成 TLS 握手交互后，在收到所述 Get HTTPS 报文或所述 Post HTTPS 报文后，根据获得的所述终端的标识，向所述终端发送 Redirect HTTPS 报文，所述 Redirect HTTPS 报文中至少携带所述第二服务器的 URL。

10 若终端收到所述 Redirect HTTPS 报文，则所述终端启动访问所述第二服务器的流程，即根据所述 Redirect HTTPS 报文中的所述第二服务器的 URL，访问所述第二服务器。若所述终端未收到所述 Redirect HTTPS 报文或者所述 Redirect HTTPS 报文所携带的 URL 与 Server Redirect 报文所携带的 URL 不相同，则所述终端不会访问所述第二服务器。

15 第二具体实施例中进行 HTTPS 重定向的过程如图 4 所示，与第一具体实施例的不同之处在于：

所述终端获取所述用户访问所述第二服务器的指示后，终止与所述 BRAS 的 TLS 握手过程，并且所述终端不再向所述 BRAS 发送 Get HTTPS 报文或 Post HTTPS 报文。所述终端可采用 TLS 握手过程中从所述 BRAS 获得的所述
20 第二服务器的 URL，访问所述第二服务器。

以上两个具体实施例中，Client Hello 报文中名称为 redirect_url_enable 的扩展项可表示为：

```
enum{  
    redirect_url_enable  
25 }Extension Type;
```

其中，redirect_url_enable 可作为标识使用，不携带数据。

以上两个具体实施例中，所述第二服务器的 URL 可携带在 Server Redirect

报文的净荷中。所述 Server Redirect 报文结构体可表示为：

```
struct{  
    unit8 urllength;  
    opaque string<0-255>;  
5    }Server Redirect.
```

其中，unit8 urllength 可携带所述第二服务器的 URL 的长度；opaque string 可携带所述第二服务器的 URL。

本发明实施例还提供了一种 BRAS，该 BRAS 可采用上述方法实施例部分中 BRAS 所采用的方法，重复之处不再赘述，如图 5 所示，该 BRAS 包括：

10 接收模块 501 用于接收终端的第一 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于标识所述终端具有根据 URL 进行重定向的能力。所述终端具有根据 URL 进行重定向的能力可以为所述终端具有解析携带 URL 的报文的能力以及具有采用所述报文中的 URL 进行重定向的能力。

15 获得模块 502 用于在确定所述第一 TLS 握手报文携带所述标志后，根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书，所述目的服务器为重定向所达的服务器。所述目的服务器可以为图 1、图 2、图 3 或图 4 对应的实施例中的第二服务器。

20 发送模块 503 用于向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书。

举例说明，所述发送模块 503 具体用于向所述终端发送携带所述目的服务器的 URL 的 Server Redirect 报文；所述发送模块具体用于向所述终端发送携带所述目的服务器的证书的 Server Certificate 报文。

25 举例说明，所述发送模块 503 具体用于向所述终端发送第二 TLS 握手报文，该第二 TLS 握手报文为 Server Hello 报文，所述 Server Hello 报文携带所述目的服务器的 URL 以及所述目的服务器的证书。

该实施例中，BRAS 通过判断终端发送的第一 TLS 握手报文中是否携带

标识, 所述标识用于标识所述终端具有根据 URL 进行重定向的能力, 所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后, 向所述终端发送与所述终端对应的目的服务器的 URL 以及与所述终端对应的目的服务器的证书, 有助于终端根据该目的服务器的 URL 以及目的服务器的证书进行匹配的成功率, 有助于提高重定向的成功率。

本发明实施例还提供了一种 BRAS, 该 BRAS 可采用上述方法实施例部分中 BRAS 所采用的方法, 重复之处不再赘述, 如图 6 所示, 该 BRAS 包括处理器 601、存储器 602 和通信接口 603, 处理器 601、存储器 602、通信接口 603 通过总线 604 相互连接; 总线 604 可以是外设部件互连标准(peripheral component interconnect, 简称 PCI)总线或扩展工业标准结构(extended industry standard architecture, 简称 EISA)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示, 图 6 中用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。

存储器 602, 用于存放程序。具体地, 程序可以包括程序代码, 所述程序代码包括计算机操作指令。存储器 602 可能包含随机存取存储器(random access memory, 简称 RAM), 也可能还包括非易失性存储器(non-volatile memory), 例如至少一个磁盘存储器。

通信接口 603 用于与其他设备进行通信。

其中, 处理器 601 获取存储器 602 中程序, 按照该程序执行以下过程:

通过通信接口 603 接收终端的第一 TLS 握手报文, 所述第一 TLS 握手报文中携带有标志和所述终端的标识, 所述标志用于标识所述终端具有根据 URL 进行重定向的能力;

在确定所述第一 TLS 握手报文携带所述标志后, 根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书, 所述目的服务器为重定向所达的服务器;

通过通信接口 603 向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书。

举例说明，所述终端具有根据 URL 进行重定向的能力可以为所述终端具有解析携带 URL 的报文的能力以及具有采用所述报文中的 URL 进行重定向的能力。

5 举例说明，处理器 601 通过通信接口 603 向所述终端发送携带所述目的服务器的 URL 的 Server Redirect 报文，向所述终端发送携带所述目的服务器的证书的 Server Certificate 报文。

举例说明，所述处理器 601 通过所述通信接口 603 向所述终端发送第二 TLS 握手报文，该第二 TLS 握手报文为 Server Hello 报文，所述 Server Hello 报文中携带所述目的服务器的 URL 以及所述目的服务器的证书。

10 该实施例中，BRAS 通过判断终端发送的第一 TLS 握手报文中是否携带标识，所述标识用于标识所述终端具有根据 URL 进行重定向的能力，所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后，向所述终端发送与所述终端对应的目的服务器的 URL 以及与所述终端对应的目的服务器的证书，有助于终端根据该目的服务器的 URL 以及目的服务器的证书进行匹配的成功率，有助于提高重定向的成功率。
15

本发明实施例还提供了一种终端，该终端可采用上述方法实施例部分中终端所采用的方法，重复之处不再赘述，如图 7 所示，该终端包括：

发送模块 701 用于向 BRAS 发送第一 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于标识所述终端具有根据
20 URL 进行重定向的能力。所述终端具有根据 URL 进行重定向的能力可以为所述终端具有解析携带 URL 的报文的能力以及具有采用所述报文中的 URL 进行重定向的能力。

接收模块 702 用于接收所述 BRAS 返回的目的服务器的 URL 以及所述目的服务器的证书，所述目的服务器为重定向所达的服务器。

25 判断模块 703，用于判断所述目的服务器的 URL 与所述目的服务器的证书是否匹配。

输出模块 704，用于在所述判断模块 703 确定所述目的服务器的 URL 与

所述目的服务器的证书匹配，输出第一提示信息，所述第一提示信息用于提示对所请求的服务器的访问将被重定向。

可选地，所述输出模块 704 还用于在所述判断模块 703 确定所述目的服务器的 URL 与所述目的服务器的证书不匹配，输出第二提示信息，所述第二
5 提示信息用于提示所述目的服务器的证书有问题。

举例说明，所述接收模块 702 具体用于接收所述 BRAS 发送的第二 TLS 握手报文，所述第二 TLS 握手报文中携带所述目的服务器的 URL 和所述目的服务器的证书。所述接收模块 702 可从所述第二 TLS 握手报文中获得所述目的服务器的 URL 和所述目的服务器的证书，或者所述判断模块 703 可从所述
10 接收模块 702 接收到的所述第二 TLS 握手报文，获得所述目的服务器的 URL 和所述目的服务器的证书。

举例说明，所述接收模块 702 具体用于接收所述 BRAS 发送的 Server Redirect 报文，所述 Server Redirect 报文携带所述目的服务器的 URL，并接收所述 BRAS 发送 Server Certificate 报文，所述 Server Certificate 报文携带所述
15 目的服务器的证书。所述接收模块 702 或所述判断模块 703 可从所述 Server Redirect 报文获得所述目的服务器的 URL，所述接收模块 702 或所述判断模块 703 可从所述 Server Certificate 报文获得所述目的服务器的证书。

该实施例中，终端在向 BRAS 发送的第一 TLS 握手报文中携带标志，使得 BRAS 根据该标志确定该终端具有根据 URL 进行重定向的能力，终端接收
20 BRAS 发送的目的服务器的证书以及目的服务器的 URL，根据该目的服务器的证书和该目的服务器的 URL 进行匹配，从而避免了终端检查所述目的服务器的证书合法性时，由于所述目的服务器的证书与所述终端请求访问的服务器的 URL 不匹配而导致重定向失败，有助于提高重定向的成功率。

本发明实施例还提供了一种终端，该终端的可采用上述方法实施例部分
25 中终端所采用方法，重复之处不再赘述，如图 8 所示，该终端包括处理器 801、存储器 802 和通信接口 803，处理器 801、存储器 802、通信接口 803 通过总线 804 相互连接；总线 804 可以是外设部件互连标准（peripheral component

interconnect, 简称 PCI) 总线或扩展工业标准结构 (extended industry standard architecture, 简称 EISA) 总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示, 图 8 中用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。

5 存储器 802, 用于存放程序。具体地, 程序可以包括程序代码, 所述程序代码包括计算机操作指令。存储器 802 可能包含随机存取存储器 (random access memory, 简称 RAM), 也可能还包括非易失性存储器 (non-volatile memory), 例如至少一个磁盘存储器。

通信接口 803 用于与其他设备进行通信。

10 其中, 处理器 801 用于获取存储器 802 中程序, 按照该程序执行以下过程:

通过通信接口 803 向 BRAS 发送第一 TLS 握手报文, 所述第一 TLS 握手报文中携带有标志和所述终端的标识, 所述标志用于标识所述终端具有根据 URL 进行重定向的能力;

15 通过通信接口 803 接收所述 BRAS 发送的目的服务器的 URL 以及所述目的服务器的证书, 所述目的服务器为重定向所达的服务器;

判断所述目的服务器的 URL 与所述目的服务器的证书是否匹配, 在确定所述目的服务器的 URL 与所述目的服务器的证书匹配后, 输出第一提示信息, 所述第一提示信息用于提示对所请求的服务器的访问将被重定向。

20 可选地, 处理器 801 若确定所述目的服务器的 URL 与所述目的服务器的证书不匹配, 输出第二提示信息, 所述第二提示信息用于提示所述目的服务器的证书有问题。

举例说明, 处理器 801 在获取用户根据第一提示信息输入的指示后, 通过通信接口 803 向所述 BRAS 发送第一 HTTPS 报文, 所述指示用于确认继续
25 访问所述目的服务器的 URL, 所述第一 HTTPS 报文携带所述终端的标识, 所述第一 HTTPS 用于向所述 BRAS 请求重定向的信息; 所述处理器 801 通过通信接口 803 接收所述 BRAS 发送的第二 HTTPS 报文, 所述第二 HTTPS 报文

携带所述重定向的信息；若所述处理器 801 通过通信接口 803 接收到所述 BRAS 发送的所述第二 HTTPS 报文，则所述处理器 801 根据所述重定向的信息访问所述目的服务器 URL 对应的服务器；若所述处理器 801 通过通信接口 803 未接收到所述 BRAS 发送的所述第二 HTTPS 报文，所述终端不再对所述目的服务器进行访问。

可选地，所述处理器 801 可在通过通信接口 803 向所述 BRAS 发送所述第一 HTTPS 报文前，终止与所述 BRAS 的 TLS 握手过程。

举例说明，所述处理器 801 通过通信接口 803 接收所述 BRAS 发送的第二 TLS 握手报文，所述第二 TLS 握手报文中携带所述目的服务器的 URL 和所述目的服务器的证书。

举例说明，所述处理器 801 通过通信接口 803 接收所述 BRAS 发送的服务器重定向 Server Redirect 报文，所述 Server Redirect 报文携带所述目的服务器的 URL，并接收所述 BRAS 发送服务器认证 Server Certificate 报文，所述 Server Certificate 报文携带所述目的服务器的证书。

该实施例中，终端在向 BRAS 发送的第一 TLS 握手报文中携带标志，使得 BRAS 根据该标志确定该终端具有根据 URL 进行重定向的能力，终端接收 BRAS 发送的目的服务器的证书以及目的服务器的 URL，根据该目的服务器的证书和该目的服务器的 URL 进行匹配，从而避免了终端检查所述目的服务器的证书合法性时，由于所述目的服务器的证书与所述终端请求访问的服务器的 URL 不匹配而导致重定向失败，有助于提高重定向的成功率。

图 9 为本发明实施例中用于重定向的系统的示意图。图 9 所示的系统可包括 BRAS901 和终端 902。所述 BRAS 可以为图 5 或图 6 对应的实施例提供的 BRAS，在此不再赘述。所述可以为图 7 或图 8 对应的实施例提供的终端，在此不再赘述。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个

其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

5 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

10 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

15 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

20 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种用于重定向的方法，其特征在于，所述方法包括：

宽带远程接入服务器 BRAS 接收终端发送的第一传输层安全 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于
5 标识所述终端具有根据统一资源定位符 URL 进行重定向的能力；

所述 BRAS 在确定所述第一 TLS 握手报文携带所述标志后，根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书，所述目的服务器为重定向所述服务器；

所述 BRAS 向所述终端发送所述目的服务器的 URL 以及所述目的服务器
10 的证书。

2、如权利要求 1 所述的方法，其特征在于，所述 BRAS 根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书包括：

所述 BRAS 根据所述终端的标识，获得预先配置的表项，所述表项包括所述终端的标识、所述目的服务器的 URL 和所述目的服务器的证书；

15 所述 BRAS 从所述表项中，获得所述目的服务器的 URL 和所述目的服务器的证书。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述 BRAS 向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书包括：

20 所述 BRAS 向所述终端发送第二 TLS 握手报文，所述第二 TLS 握手报文携带所述目的服务器的 URL 和所述目的服务器的证书。

4、如权利要求 1 或 2 所述的方法，其特征在于，所述 BRAS 向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书包括：

所述 BRAS 向所述终端发送服务器重定向 Server Redirect 报文，所述 Server Redirect 报文携带所述目的服务器的 URL；

25 所述 BRAS 向所述终端发送服务器认证 Server Certificate 报文，所述 Server Certificate 报文携带所述目的服务器的证书。

5、一种用于重定向的方法，其特征在于，所述方法包括：

终端向宽带远程接入服务器 BRAS 发送第一传输层安全 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于标识所述终端具有根据统一资源定位符 URL 进行重定向的能力；

5 所述终端接收所述 BRAS 发送的目的服务器的 URL 和所述目的服务器的证书，所述目的服务器为重定向所达的服务器；

所述终端判断所述目的服务器的 URL 与所述目的服务器的证书是否匹配；

若所述目的服务器的 URL 与所述目的服务器的证书匹配，则所述终端输出第一提示信息，所述第一提示信息用于提示访问将被重定向，所述访问为所述终端对所请求的服务器的访问。

6、如权利要求 5 所述的方法，其特征在于，所述方法还包括：

若所述目的服务器的 URL 与所述目的服务器的证书不匹配，则所述终端输出第二提示信息，所述第二提示信息用于提示所述目的服务器的证书错误。

15 7、如权利要求 5 或 6 所述的方法，其特征在于，所述终端接收所述 BRAS 发送的目的服务器的 URL 和所述目的服务器的证书包括：

所述终端接收所述 BRAS 发送的第二 TLS 握手报文，所述第二 TLS 握手报文中携带所述目的服务器的 URL 和所述目的服务器的证书；

20 所述终端从所述第二 TLS 握手报文中获得所述目的服务器的 URL 和所述目的服务器的证书。

8、如权利要求 5 或 6 所述的方法，其特征在于，所述终端接收所述 BRAS 发送的目的服务器的 URL 和所述目的服务器的证书包括：

所述终端接收所述 BRAS 发送的服务器重定向 Server Redirect 报文，所述 Server Redirect 报文携带所述目的服务器的 URL；

25 所述终端从所述 Server Redirect 报文获得所述目的服务器的 URL；

所述终端接收所述 BRAS 发送服务器认证 Server Certificate 报文，所述 Server Certificate 报文携带所述目的服务器的证书；

所述终端从所述 Server Certificate 报文获得所述目的服务器的证书。

9、一种宽带远程接入服务器 BRAS，其特征在于，所述 BRAS 包括：

接收模块，用于接收终端发送的第一传输层安全 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标志用于标识所述终端具有根据统一资源定位符 URL 进行重定向的能力，所述目的服务器为重定向所达的服务器；

获得模块，用于在确定所述第一 TLS 握手报文携带所述标志后，根据所述终端的标识获得目的服务器的 URL 和所述目的服务器的证书，所述目的服务器为重定向所达的服务器；

发送模块，用于向所述终端发送所述目的服务器的 URL 以及所述目的服务器的证书。

10、如权利要求 9 所述的 BRAS，其特征在于，所述获得模块具体用于根据所述终端的标识，获得预先配置的表项，所述表项包括所述终端的标识、所述目的服务器的 URL 和所述目的服务器的证书；

所述获得模块具体用于从所述表项中，获得所述目的服务器的 URL 和所述目的服务器的证书。

11、如权利要求 9 或 10 所述的 BRAS，其特征在于，

所述发送模块具体用于向所述终端发送第二 TLS 握手报文，所述第二 TLS 握手报文中携带所述目的服务器的 URL 和所述目的服务器的证书。

12、如权利要求 9 或 10 所述的 BRAS，其特征在于，

所述发送模块具体用于向所述终端发送服务器重定向 Server Redirect 报文，所述 Server Redirect 报文携带所述目的服务器的 URL；

所述发送模块具体用于向所述终端发送服务器认证 Server Certificate 报文，所述 Server Certificate 报文携带所述目的服务器的证书。

13、一种终端，其特征在于，所述终端包括：

发送模块，用于向宽带远程接入服务器 BRAS 发送第一传输层安全 TLS 握手报文，所述第一 TLS 握手报文中携带有标志和所述终端的标识，所述标

志用于标识所述终端具有根据统一资源定位符 URL 进行重定向的能力;

接收模块, 用于接收所述 BRAS 发送的目的服务器的 URL 和所述目的服务器的证书, 所述目的服务器为重定向所达的服务器;

5 判断模块, 用于判断所述接收模块接收的所述目的服务器的 URL 与所述目的服务器的证书是否匹配;

输出模块, 用于在所述判断模块确定所述目的服务器的 URL 与所述目的服务器的证书匹配, 输出第一提示信息, 所述第一提示信息用于提示访问将被重定向, 所述访问为所述终端对所请求的服务器的访问。

14、如权利要求 13 所述的终端, 其特征在于,

10 所述输出模块还用于在所述判断模块确定所述目的服务器的 URL 与所述目的服务器的证书不匹配, 输出第二提示信息, 所述第二提示信息用于提示所述目的服务器的证书有问题。

15、如权利要求 13 或 14 所述的终端, 其特征在于,

15 所述接收模块具体用于接收所述 BRAS 发送的第二 TLS 握手报文, 所述第二 TLS 握手报文中携带所述目的服务器的 URL 和所述目的服务器的证书。

16、如权利要求 13 或 14 所述的终端, 其特征在于,

所述接收模块具体用于接收所述 BRAS 发送的服务器重定向 Server Redirect 报文, 所述 Server Redirect 报文携带所述目的服务器的 URL;

20 所述接收模块具体用于接收所述 BRAS 发送服务器认证 Server Certificate 报文, 所述 Server Certificate 报文携带所述目的服务器的证书。

17、一种用于重定向的系统, 其特征在于, 所述系统包括:

权利要求 9 至 12 任意一项所述的宽带远程接入服务器 BRAS 和权利要求 13 至 16 任意一项所述的终端。

1/6

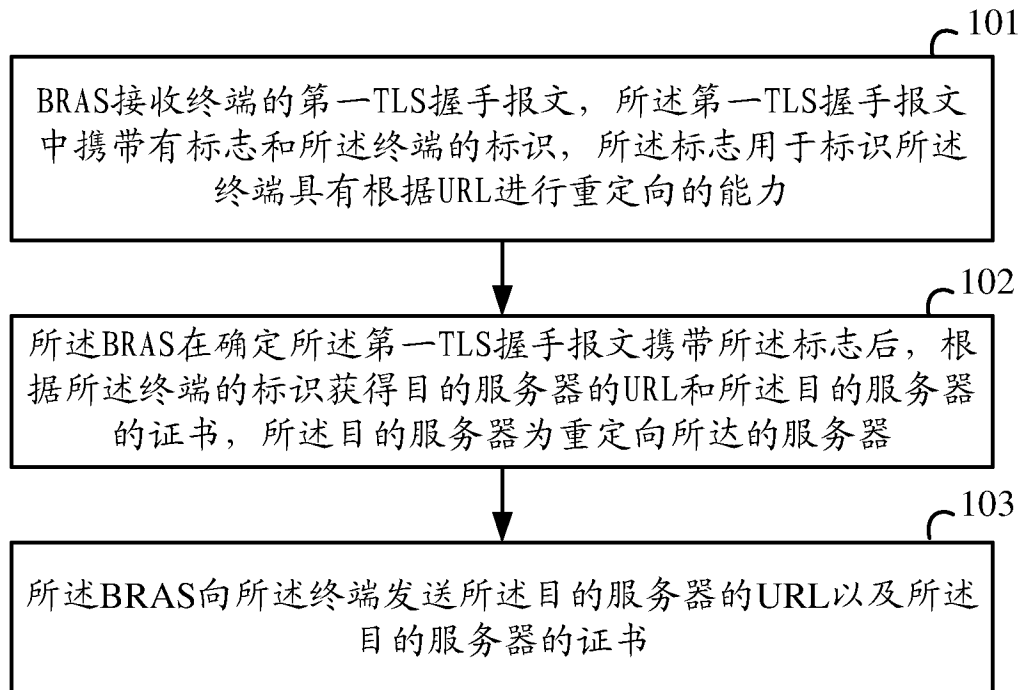


图 1

2/6

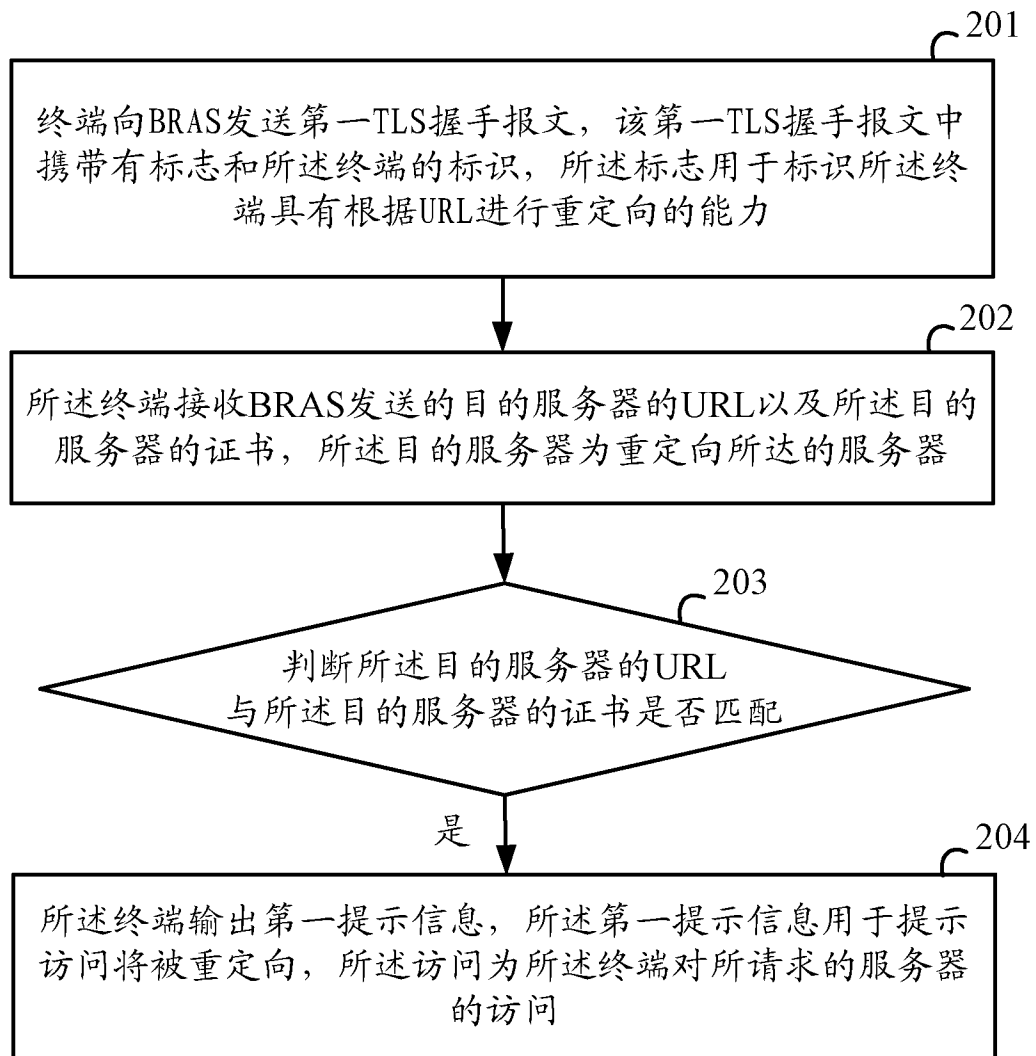


图 2

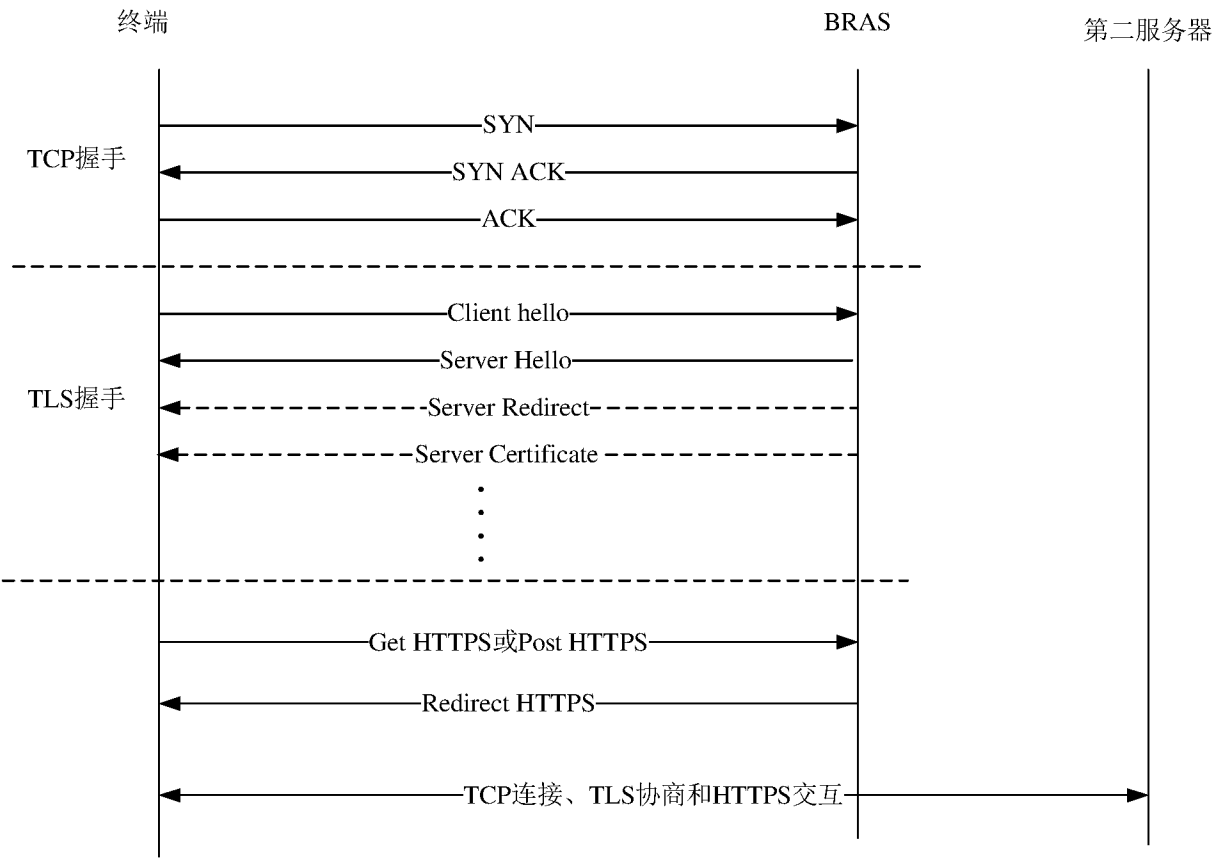


图 3

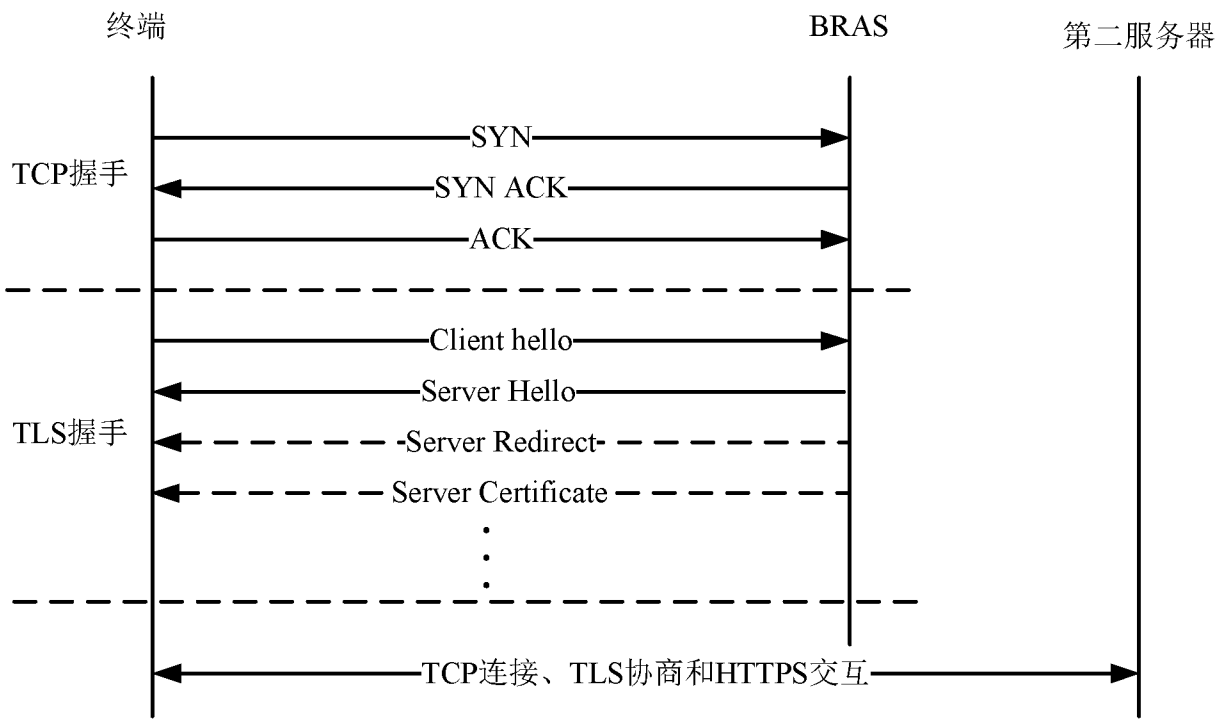


图 4

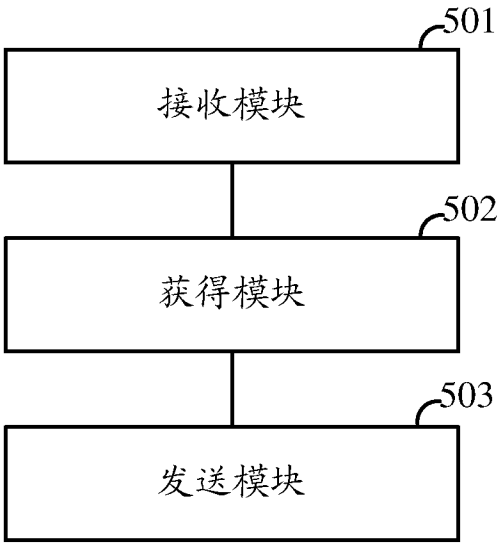


图 5

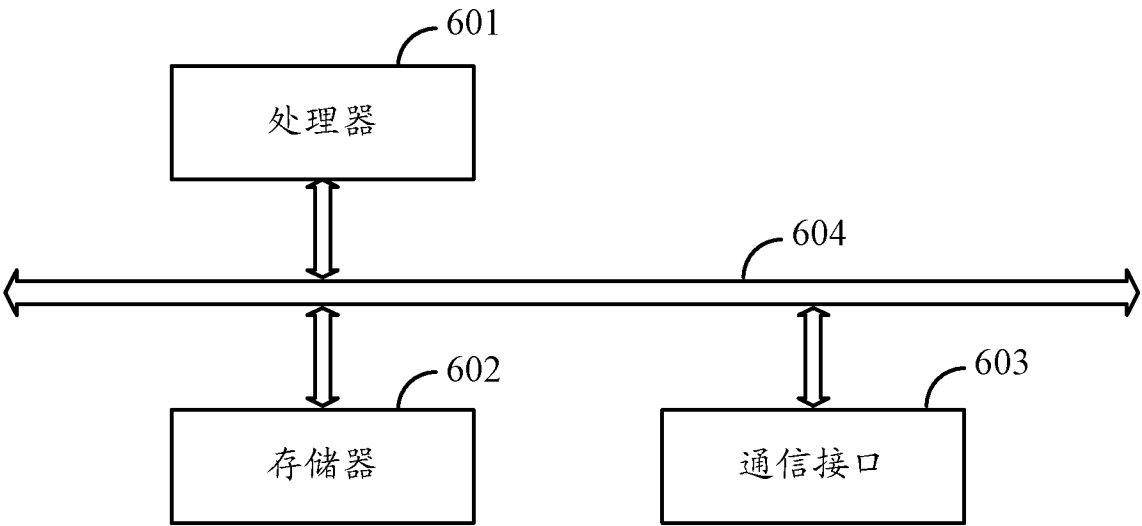


图 6

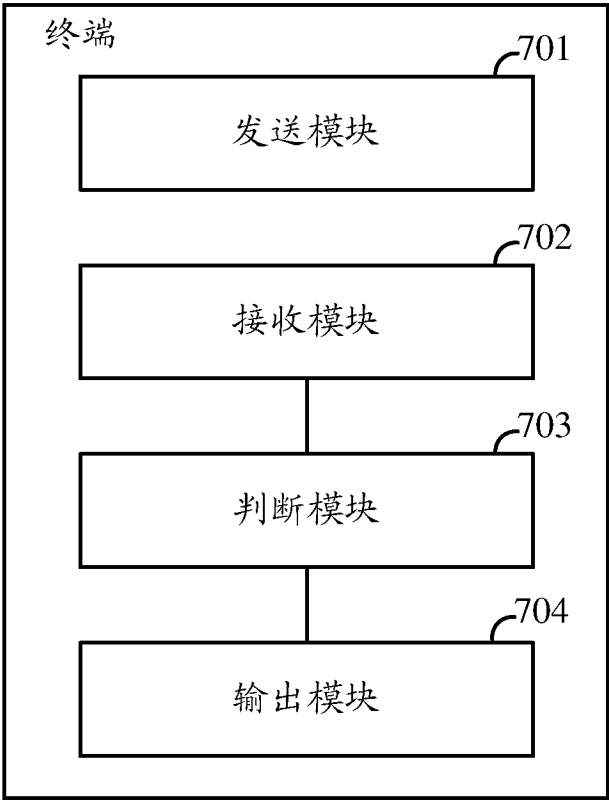


图 7

6/6

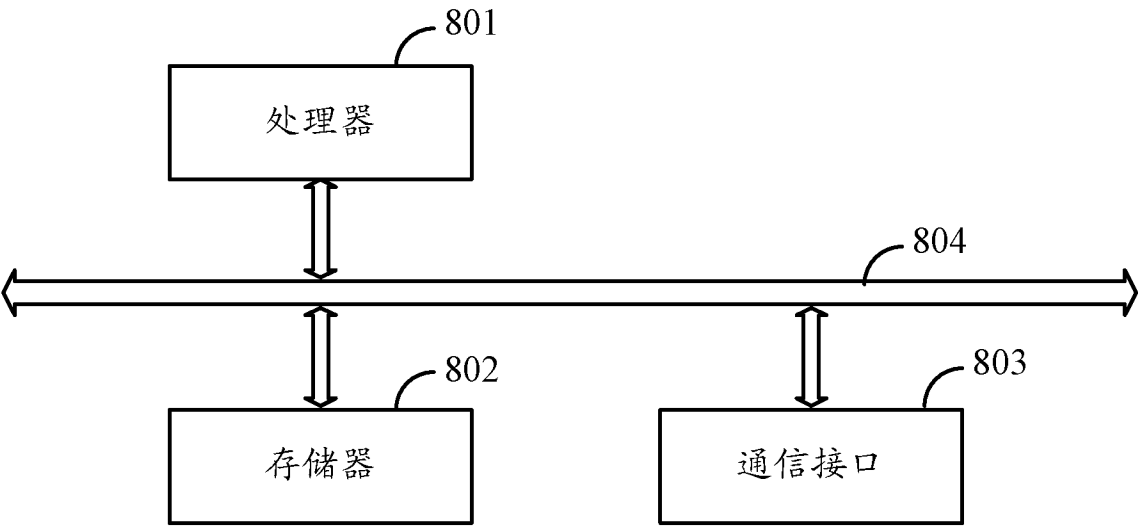


图 8

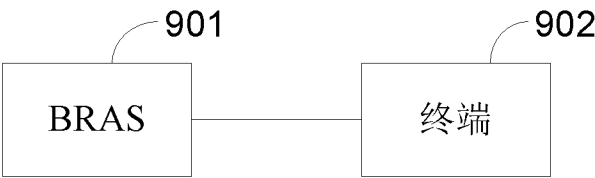


图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/073507

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 29/08 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC, GOOGLE: wang shuxiang, gao hongliang, ID, TLS, HTTPS, SSL, redirect+, server, match+, certificate, warning, identifier, sign, indication, access

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101360102 A (SYMANTEC CORP.) 04 February 2009 (04.02.2009) description, page 3, lines 13 to22	1-17
A	CN 102334311 A (MICROSOFT CORPORATION) 25 January 2012 (25.01.2012) the whole document	1-17
A	CN 103051626 A (HUAWEI TECHNOLOGIES CO., LTD.) 17 April 2013 (17.04.2013) the whole document	1-17
A	CN 103384993 A (HUAWEI TECHNOLOGIES CO., LTD.) 06 November 2013 (06.11.2013) the whole document	1-17

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&”document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 19 April 2016	Date of mailing of the international search report 27 April 2016
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer XING, Yunfeng Telephone No. (86-10) 62413374

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/073507

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101360102 A	04 February 2009	JP 2009038797 A	19 February 2009
		EP 2020798 A2	04 February 2009
		US 2009037997 A1	05 February 2009
CN 102334311 A	25 January 2012	US 2010218248 A1	26 August 2010
		WO 2010098960 A2	02 September 2010
		EP 2401842 A2	04 January 2012
		JP 2012519416 A	23 August 2012
CN 103051626 A	17 April 2013	None	
CN 103384993 A	06 November 2013	WO 2014089816 A1	19 June 2014

A. 主题的分类		
H04L 29/06 (2006.01) i; H04L 29/08 (2006.01) i		
按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域		
检索的最低限度文献 (标明分类系统和分类号)		
H04L		
包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))		
CNKI; CNPAT; WPI; EPDOC; GOOGLE: 王淑香, 高红亮, 重定向, 服务器, 匹配, 证书, ID, TLS, HTTPS, SSL, 告警, 警告, 标识, 标志, 接入, redirect+, server, match+, certificate, warning, identifier, sign, indication, access		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 101360102 A (赛门铁克公司) 2009年 2月 4日 (2009 - 02 - 04) 说明书第3页第13-22行	1-17
A	CN 102334311 A (微软公司) 2012年 1月 25日 (2012 - 01 - 25) 全文	1-17
A	CN 103051626 A (华为技术有限公司) 2013年 4月 17日 (2013 - 04 - 17) 全文	1-17
A	CN 103384993 A (华为技术有限公司) 2013年 11月 6日 (2013 - 11 - 06) 全文	1-17
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期		国际检索报告邮寄日期
2016年 4月 19日		2016年 4月 27日
ISA/CN的名称和邮寄地址		授权官员
中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088		邢雲峰
传真号 (86-10) 62019451		电话号码 (86-10) 62413374

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/073507

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	101360102	A	2009年 2月 4日	JP	2009038797	A	2009年 2月 19日
				EP	2020798	A2	2009年 2月 4日
				US	2009037997	A1	2009年 2月 5日
CN	102334311	A	2012年 1月 25日	US	2010218248	A1	2010年 8月 26日
				WO	2010098960	A2	2010年 9月 2日
				EP	2401842	A2	2012年 1月 4日
				JP	2012519416	A	2012年 8月 23日
CN	103051626	A	2013年 4月 17日	无			
CN	103384993	A	2013年 11月 6日	WO	2014089816	A1	2014年 6月 19日

表 PCT/ISA/210 (同族专利附件) (2009年7月)