

IP ADDRESS ACQUISITION METHOD AND APPARATUS

[0001] The present application claims priority to Chinese Patent Application No. 201510764761.9, filed on November 11, 2015 and entitled "IP ADDRESS ACQUISITION METHOD AND APPARATUS", which is incorporated herein by
5 reference in its entirety.

TECHNICAL FIELD

[0002] The present application relates to the field of information technologies, and in particular, to an IP address acquisition method and apparatus.

BACKGROUND

10 [0003] With the development of the informational society, people are accustomed to using the Internet for social activities such as online shopping, online banking, and instant messaging. The exposure of online activities related to personal property attracts more attention of people (for example, a financial activity and a transaction activity). Therefore, people begin to monitor an Internet Protocol (IP) address of each
15 terminal in the network, so as to evaluate a degree of threat in the network, and to prevent any high potential threats from an IP address. If necessary, an access request of such an IP address can be rejected, so as to improve overall network security.

[0004] However, in an existing IP address acquisition method, when an IP address of a terminal is monitored, the IP address of the terminal is obtained only from a
20 request or a response message header transmitted using the Hypertext Transfer Protocol (HTTP). However, it is easy for a malicious actor to change IP address information included in the HTTP message header by installing a browser plug-in or hacker software or by using a proxy server. Consequently, an accurate and authentic IP address cannot be obtained.

25 [0005] It can be seen that, in the terminal IP address acquisition method in the prior art, authenticity and accuracy of an obtained IP address are relatively low, thereby reducing accuracy of other information processed based on the terminal IP

address.

SUMMARY

[0006] Embodiments of the present application provide an IP address acquisition method and apparatus, so as to resolve a prior-art problem that authenticity and accuracy of an IP address obtained by using only the HTTP request message header are relatively low.

[0007] An embodiment of the present application provides an IP address acquisition method, including:

receiving, by a network side device, a request message of a first protocol sent by a terminal;

returning a web page including scripting language code to the terminal based on the request message of the first protocol;

receiving a request message for establishing a communication connection sent by the terminal by running the scripting language code;

establishing a communication connection to the terminal based on the request message for establishing a communication connection; and

determining a first IP address of the terminal by using the communication connection.

[0008] An embodiment of the present application provides an IP address acquisition method, including:

sending, by a terminal, a request message of a first protocol to a network side device;

receiving a web page sent by the network side device based on the request message of the first protocol, where the web page includes scripting language code;

running the scripting language code, and sending, to the network side device based on the scripting language code, a request message for establishing a communication connection, so that the network side device establishes a communication connection to the terminal; and

sending a data packet to the network side device by using the communication connection, so that the network side device determines a first IP address of the terminal based on the data packet.

[0009] An embodiment of the present application provides an IP address

acquisition apparatus, including:

a first receiving module, configured to receive a request message of a first protocol sent by a terminal;

5 a returning module, configured to return a web page including scripting language code to the terminal based on the request message of the first protocol;

a second receiving module, configured to receive a request message for establishing a communication connection sent by the terminal by running the scripting language code;

10 a communication connection module, configured to establish a communication connection to the terminal based on the request message for establishing a communication connection; and

an acquisition module, configured to obtain a first IP address of the terminal by using the communication connection.

[0010] An embodiment of the present application provides an IP address acquisition apparatus, including:

15 a first sending module, configured to send a request message of a first protocol to a network side device;

20 a receiving module, configured to receive a web page sent by the network side device based on the request message of the first protocol, where the web page includes scripting language code;

a communication connection module, configured to: run the scripting language code, and send, to the network side device based on the scripting language code, a request message for establishing a communication connection, so that the network side device establishes a communication connection to the apparatus; and

25 a second sending module, configured to send a data packet to the network side device by using the communication connection, so that the network side device determines a first IP address of the apparatus based on the data packet.

[0011] The embodiments of the present application provide the IP address acquisition method and apparatus. In the method, the network side device receives the request message of the first protocol sent by the terminal, and returns the web page including the scripting language code to the terminal based on the request message, so that the terminal establishes the communication connection to the network side device by running the scripting language code, and determines the first IP address of the terminal by using the communication connection. In the IP address acquisition

method, the network side device can determine an authentic IP address of an access terminal, and improve the authenticity and accuracy of the determined authentic IP address, thereby improving accuracy of other information processing that needs to be performed based on a terminal IP address.

5

BRIEF DESCRIPTION OF DRAWINGS

[0012] The accompanying drawings described herein are intended to provide a further understanding of the present application, and constitute a part of the present application. The example embodiments of the present application and descriptions thereof are intended to explain the present application, and do not constitute an improper limitation on the present application. In the accompanying drawings:

10

[0013] FIG. 1 is an IP address acquisition process according to an embodiment of the present application;

[0014] FIG. 2 is an IP address acquisition process corresponding to FIG. 1 according to an embodiment of the present application;

15

[0015] FIG. 3 is a detailed flowchart illustrating risk control according to an embodiment of the present application;

[0016] FIG. 4 is a first schematic structural diagram illustrating an IP address acquisition apparatus according to an embodiment of the present application; and

[0017] FIG. 5 is a second schematic structural diagram illustrating an IP address acquisition apparatus according to an embodiment of the present application.

20

DESCRIPTION OF EMBODIMENTS

[0018] In an existing IP address acquisition method, an IP address of a terminal is obtained by using an HTTP request message, and the IP address of the terminal is determined based on an HTTP request message header. Consequently, in this method, the IP address of the terminal is easily masqueraded and tampered with by using a browser plug-in, a proxy server, etc, and therefore, authenticity and accuracy of the obtained IP address of the terminal are relatively low. To improve authenticity and accuracy of the obtained IP address, a communication connection needs to be established in this embodiment of the present application. The communication connection is established to enable a network side device to obtain an authentic IP

25

30

address of the terminal. Therefore, the communication connection is not used for normal communication (for example, a video communication connection is established, but video data is not transmitted between the terminal and the network side device), and establishing the communication connection is a superficial operation.

5 Because the authentic IP address of the terminal needs to be obtained when establishing the communication connection, the network side device can obtain the authentic IP address of the terminal by using the communication connection. In this embodiment of the present application, the network side device returns a web page including scripting language code to the terminal that sends a request message of a
10 first protocol, so that the terminal establishes a communication connection to the network side device by running the scripting language code, and determines a first IP address of the terminal by using the communication connection. Therefore, the IP address of the terminal is not only determined by using an IP address included in the HTTP request message header, but also is determined by using the established
15 communication connection. In this case, a malicious actor is effectively prevented from modifying or masquerading the IP address in the HTTP request message header, thereby improving the accuracy and authenticity of the IP address of the terminal obtained by the network side device. This improves reliability of the obtained IP address of the terminal (a degree reflecting that the obtained IP address is the
20 authentic IP address) and further improves accuracy of other information processing that needs to be performed based on the IP address.

[0019] To meet the objectives, technical solutions, and advantages of the present application, the following describes the technical solutions of the present application with reference to specific embodiments of the present application and corresponding
25 accompanying drawings. Apparently, the described embodiments are merely some rather than all of the embodiments of the present application. Other embodiments obtained by a person of ordinary skill in the art based on the embodiments of the present application without creative efforts shall fall within the protection scope of the present application.

30 **[0020]** FIG. 1 is an IP address acquisition process according to an embodiment of the present application. The IP address acquisition process includes the following steps.

[0021] S101: A network side device receives a request message of a first protocol sent by a terminal.

5 [0022] In this embodiment of the present application, in actual application, because the terminal usually needs to pass through a gateway of a server of a website before accessing the server, the network side device in step S101 can be a gateway, and the gateway receives the request message of the first protocol sent by the terminal.

10 [0023] Or the network side device in the present application can be a server, and the server receives the request message of the first protocol sent by the terminal. In addition, the gateway in the present application can be a separate device independent of the server, or can be a device integrated with the server. The present invention sets no special limitation here.

[0024] In addition, the first protocol can be HTTP. Because a request/response mode is used in HTTP, the request message in the present application can be a request message sent by the terminal based on HTTP, and the HTTP request message includes an access request address (an address of the server), an IP address of the terminal, etc.

15 [0025] The terminal in this embodiment of the present application can be various terminals such as a mobile phone, a personal computer (PC), and a tablet computer.

[0026] The following uses an example in which the network side device is a gateway for description.

20 [0027] For example, if Jack is to access an online bank website of a bank by using a terminal and operate his own account, Jack needs to enter an address of the online bank website in a browser address bar, and the terminal generates and sends an HTTP request message based on the address, so as to access the online bank website. Because a server corresponding to the online bank website is provided with a gateway, the gateway receives the HTTP request message sent by the terminal.

25 [0028] S102: Return a web page including scripting language code to the terminal based on the request message of the first protocol.

30 [0029] In this embodiment of the present application, if the terminal accesses a network by using a device such as a router or a proxy server, a source IP address included in a message header of the request message of the first protocol is an IP address of the router or the proxy server instead of an authentic IP address of the terminal. If a malicious actor tampers with the source IP address included in the message header of the request message of the first protocol, the source IP address is not the authentic IP address of the terminal either. Therefore, because the source IP address included in the message header of the request message of the first protocol

cannot be determined as the authentic IP address of the terminal in this case, the authentic IP address of the terminal needs to be further determined in the method provided in the present application.

[0030] When the authentic IP address of the terminal is further determined, if the network side device receiving the HTTP request message is a gateway, the gateway can forward, to a server, the HTTP request message sent by the terminal. After receiving the request message, the server returns a corresponding web page, and the web page includes a predetermined scripting language code. The gateway can return the web page including the scripting language code to the terminal. The scripting language code is used to enable the terminal to run the scripting language code, so that the terminal can obtain the authentic IP address of the terminal and send the authentic IP address to the gateway. If the network side device receiving the HTTP request message is a server, the server can directly return the web page including the scripting language code to the terminal based on the HTTP request message.

[0031] In addition, in the present application, the network side device may not directly return the web page including the scripting language code, but provides an address for downloading the scripting language code in a web page code corresponding to the web page, so that after subsequently parsing the web page code, the terminal can download the scripting language code from another network side device (for example, the server) and run the scripting language code.

[0032] The scripting language code includes but is not limited to the JavaScript code. The JavaScript code can be used to enable the terminal to run the JavaScript code, so that the terminal can obtain the authentic IP address of the terminal and send the authentic IP address to the network side device.

[0033] In the previous example, after the gateway of the online bank receives the HTTP request message sent by the Jack's terminal, the gateway forwards the HTTP request message to the server, so that the server returns a corresponding web page. Then, the gateway sends, to the terminal, the web page returned by the server based on the HTTP request message, and the web page includes the JavaScript code.

[0034] S103: Receive a request message for establishing a communication connection sent by the terminal by running the scripting language code.

[0035] S104: Establish a communication connection to the terminal based on the request message for establishing a communication connection.

[0036] S105: Determine a first IP address of the terminal by using the

communication connection.

[0037] In this embodiment of the present application, after receiving the web page sent by the network side device, the terminal needs to parse the web page code corresponding to the web page. Because the web page includes the scripting language code, the terminal loads and runs the scripting language code when parsing the web page code.

[0038] In addition, a function of the scripting language code in this embodiment of the present application is to enable the terminal to send, to the network side device, the request message for establishing a communication connection, so that the network side device establishes the communication connection to the terminal, and obtains the authentic IP address of the terminal by using the communication connection. Therefore, after the terminal runs the scripting language code, the terminal sends, to the network side device, the request message for establishing a communication connection, and in step S103, the network side device receives the request message for establishing a communication connection.

[0039] In step S104, after receiving the request message for establishing a communication connection sent by the terminal, the network side device can establish the communication connection to the terminal. Further, the communication connection in the present application can be the Web Real-Time Communication (WebRTC) connection, and WebRTC is based on Simple Traversal of User Datagram Protocol through Network Address Translators (STUN). When STUN specifies that such a communication connection as WebRTC is to be used, both parties that establish the communication connection need to use respective authentic IP addresses to establish the connection (the two parties that establish the communication connection need to obtain the authentic IP addresses of each other), and User Datagram Protocol (UDP) "hole punching" needs to be performed when the authentic IP address of the terminal is being determined. Therefore, in the present application, a method for determining the first IP address of the terminal by using the communication connection in step S105 is actually to determine the authentic IP address of the terminal by means of UDP "hole punching". A specific process can be as follows:

[0040] First, the network side device monitors a data packet of a second protocol sent by the terminal, and the data packet of the second protocol is sent by the terminal by running the JavaScript code. The second protocol can be UDP. In addition, because the communication connection in the present application can be WebRTC, the

network side device receives, by using WebRTC, a UDP data packet sent by the terminal.

[0041] Secondly, the network side device can determine a source IP address of the UDP data packet.

5 **[0042]** Thirdly, the network side device writes the source IP address to a UDP response packet. The network side device can write the source IP address to the UDP response packet as content of the UDP response packet instead of a source IP address of the UDP response packet, and then return the UDP response packet including the source IP address to the terminal.

10 **[0043]** Then, after the terminal receives the UDP response packet, the terminal uses the authentic IP address of the terminal as the first IP address and sends the first IP address to the network side device. There are many methods for sending the first IP address. The first IP address can be written to another UDP packet and sent to the network side device by using WebRTC, or the first IP address can be written to
15 content of another HTTP message and sent to the network side device by using the HTTP message. It should be noted that, a method for sending the first IP address can be selected based on a specific implementation situation, and is not specifically limited in the present application.

[0044] Finally, in this embodiment of the present application, if the first IP
20 address of the terminal is included in the UDP data packet and is sent to the network side device by using WebRTC, after receiving the UDP data packet sent by the terminal and that includes the first IP address, the network side device can obtain the first IP address of the terminal, that is, the authentic IP address of the terminal.

[0045] In the previous process of determining the first IP address of the terminal
25 by using the communication connection, the network side device performs second-protocol (UDP) "hole punching" by using the established communication connection (WebRTC) and the protocol (STUN) used for the communication connection, so that the network side device eventually obtains the first IP address of the terminal (the authentic IP address of the terminal).

30 **[0046]** In the previous example, the gateway of the online bank receives a request message for establishing WebRTC sent by the Jack's terminal, and establishes WebRTC with the terminal based on the request message. The gateway receives a UDP data packet sent by the terminal, and determines that a source IP address for sending the data packet is 206.128.127.25. The gateway writes the source IP address

to a UDP response packet returned to the terminal, so that the terminal uses an authentic IP address (for example, 118.168.200.18) of the terminal as a first IP address based on the source IP address included in the received UDP response packet, writes the first IP address to content of the HTTP message, and sends the HTTP message to the gateway. After receiving the HTTP request message, the gateway parses the first IP address of the terminal from the content of the HTTP request message. The gateway eventually determines that the first IP address of the terminal is 118.168.200.18.

[0047] In addition, in this embodiment of the present application, the network side device may further determine a second IP address of the terminal by receiving the request message of the first protocol sent by the terminal in step S101. When the first protocol is HTTP, the network side device can obtain the source IP address included in the message header of the request message of the first protocol, and use the source IP address as the second IP address of the terminal. Because the network side device further obtains the first IP address of the terminal in step S105, the network side device can perform risk control processing based on the two IP addresses, or send the two IP addresses to a device (for example, a server in a risk control system) for risk control processing. A specific device for risk control processing is not limited in the present application.

[0048] Risk control processing can be as follows: the two IP addresses of the terminal are obtained by using different methods (separately based on the HTTP request message header and WebRTC), if the first IP address and the second IP address of the terminal obtained by the network side device are inconsistent, it can be considered that the terminal sends the HTTP request message by using at least a proxy server. In addition, the IP address of the terminal may be maliciously tampered with for illegal activities. Therefore, a monitoring level of a subsequent activity of the first IP address corresponding to the terminal needs to be raised. Because the obtained first IP address of the terminal is the authentic IP address of the terminal, a historical activity record of the first IP address can be further checked, to determine whether the first IP address is involved in an illegal activity in past.

[0049] In the previous example, the gateway obtains the HTTP request message in step S101. If the gateway determines the source IP address included in the message header as the second IP address of the terminal, such as 206.128.127.25, after the gateway obtains the first IP address of the terminal in step S105, the gateway can send

the obtained first IP address and the obtained second IP address of the Jack's terminal to the risk control system for risk control processing. Because the obtained first IP address (118.168.200.18) is not the same as the second IP address (206.128.127.25), the risk control system considers the first IP address (118.168.200.18) as a key monitoring target, so as to prevent an activity of the IP address from threatening security of the online bank.

[0050] According to the IP address acquisition method shown in FIG. 1, the network side device can obtain the authentic IP address of the terminal by establishing a masqueraded communication connection, and the IP address obtained by using the masqueraded communication connection is more authentic than the IP address obtained by using the HTTP request message header. In the IP address acquisition method in FIG. 1, the network side device can effectively determine an authentic IP address of an access terminal, and authenticity and accuracy of the authentic IP address obtained by the network side device are relatively high, thereby improving accuracy of other information processing that needs to be performed based on a terminal IP address.

[0051] Based on the IP address acquisition process executed by the network side device shown in FIG. 1, as shown in FIG. 2, an embodiment of the present application further provides an IP address acquisition process executed by a terminal.

[0052] FIG. 2 is an IP address acquisition process corresponding to FIG. 1 according to an embodiment of the present application. The IP address acquisition process includes the following steps.

[0053] S201: A terminal sends a request message of a first protocol to a network side device.

[0054] In this embodiment of the present application, if the terminal is to access a website, the terminal needs to first send an access request message to the website. The access request message is the request message of the first protocol. The first protocol can be HTTP, and the request message of the first protocol is an HTTP request message in this case. Because the network side device receiving the HTTP request message sent by the terminal can obtain a second IP address of the terminal by using an HTTP request message header, the terminal sends the HTTP request message to the network side device, so that the network side device can determine the second IP address of the terminal based on the HTTP request message.

[0055] S202: Receive a web page sent by the network side device based on the

request message of the first protocol, where the web page includes scripting language code.

[0056] In this embodiment of the present application, the network side device determines the second IP address of the access terminal in step S201. However, if the
5 second IP address of the access terminal is obtained from the HTTP request message header, when the terminal changes an IP address in the message header of the HTTP request message by installing a browser plug-in or hacker software or by using a proxy server, the network side device obtains a forged and false terminal IP address. In this case, the IP address obtained by the network side device is neither authentic
10 nor accurate. Therefore, the present application further needs to enable the network side device to obtain an authentic IP address of the terminal, so that the network side device can also obtain the authentic IP address of the terminal when the terminal forges the IP address of the terminal.

[0057] When the network side device is a gateway, after the terminal sends the
15 request message of the first protocol to the gateway, the gateway sends the request message of the first protocol to a server, and the server returns a corresponding web page to the gateway based on the request message. The gateway returns the web page to the terminal, and the terminal receives the web page returned by the gateway. The web page includes the scripting language code (the scripting language code can be the
20 JavaScript code). When the terminal parses a web page code of the web page, the terminal loads and runs the JavaScript code. The JavaScript code is used to enable the terminal to run the JavaScript code to obtain the authentic IP address of the terminal, and send the authentic IP address to the corresponding gateway.

[0058] S203: Run the scripting language code, and send, to the network side
25 device based on the scripting language code, a request message for establishing a communication connection, so that the network side device establishes a communication connection to the terminal.

[0059] S204: Send a data packet to the network side device by using the
30 communication connection, so that the network side device determines a first IP address of the terminal based on the data packet.

[0060] In this embodiment of the present application, after running the JavaScript code, based on the JavaScript code, the terminal sends, to the network side device that sends the web page, the request message for establishing a communication connection. The communication connection can be WebRTC. Because of the reason in step S103

to step S105, based on WebRTC, the network side device needs to perform UDP "hole punching" to enable the terminal to obtain the authentic IP address of the terminal and send the authentic IP address to the network side device, the terminal sends the authentic IP address of the terminal to the network side device in the subsequent step

5 S204.

[0061] Therefore, after the terminal establishes WebRTC with the network side device, in step S204, the terminal can first send a data packet of a second protocol to the network side device that sends the HTTP request message in step S201. The second protocol can be UDP, in the present application, the terminal sends a UDP data
10 packet to the network side device after establishing WebRTC with the network side device. The UDP data packet can be a null data packet without any content, so that network resources can be saved, and pressure of the network side device can be relieved.

[0062] After receiving the UDP data packet, the network side device can
15 determine a source IP address for sending the UDP data packet, and add the source IP address to a UDP response packet that is returned to the terminal. In this case, after receiving the UDP response packet returned by the network side device, the terminal can parse content of the UDP response packet, and obtain the source IP address of the terminal that is included in the UDP response packet.

[0063] After obtaining the source IP address included in the UDP response packet,
20 the terminal can compare the source IP address with the authentic IP address of the terminal. If the two are consistent, the terminal uses the source IP address or the authentic IP address of the terminal as the first IP address, and sends the first IP address to the network side device; if the two are inconsistent, the terminal uses the
25 authentic IP address of the terminal as the first IP address, and sends the first IP address to the network side device. The first IP address is sent to the network side device by writing the first IP address to content of the HTTP request message or by writing the first IP address to another UDP data packet. A specific method for sending the first IP address to the network side device is not limited in the present application.

[0064] In addition, when the source IP address is consistent with the authentic IP
30 address of the terminal, acknowledgment information can be returned instead of the first IP address, so that the network side device determines, based on the acknowledgment information, that the source IP address obtained by the network side device is the authentic IP address of the terminal.

[0065] Further, after obtaining the first IP address of the terminal, the network side device can perform risk control based on the first IP address and the second IP address obtained in step S202.

5 [0066] As shown in FIG. 3, FIG. 3 is a detailed flowchart illustrating risk control according to an embodiment of the present application.

[0067] S301: A terminal sends a request message of a first protocol to a gateway.

[0068] S302: The gateway determines a second IP address of the terminal based on the request message of the first protocol.

10 [0069] S303: The gateway forwards the request message of the first protocol to a server.

[0070] S304: The server returns a web page including scripting language code to the gateway.

[0071] S305: The gateway forwards the web page including the scripting language code to the terminal.

15 [0072] S306: The terminal receives the web page returned by the gateway, parses a web page code of the web page, and loads and runs the scripting language code included in the web page.

[0073] S307: The terminal sends a data packet of a second protocol to the gateway.

20 [0074] S308: The gateway receives the data packet of the second protocol sent by the terminal, and determines a source IP address of the terminal.

[0075] S309: The gateway sends a response packet of the second protocol including the source IP address of the terminal to the terminal.

25 [0076] S310. The terminal sends an authentic IP address of the terminal to the gateway based on the received response packet of the second protocol.

[0077] S311: The gateway receives the authentic IP address sent by the terminal, and uses the authentic IP address as a first IP address of the terminal.

[0078] S312: The gateway sends the first IP address and the second IP address of the terminal to a risk control system.

30 [0079] S313: The risk control system performs risk control processing based on the received first IP address and the received second IP address of the terminal.

[0080] The IP address acquisition method provided in the embodiment of the present application is described above. Based on the same idea, as shown in FIG. 4 and FIG. 5, an embodiment of the present application further provides a corresponding

IP address acquisition apparatus.

[0081] FIG. 4 is a first schematic structural diagram illustrating an IP address acquisition apparatus according to an embodiment of the present application. The IP address acquisition apparatus includes:

5 a first receiving module 401, configured to receive a request message of a first protocol sent by a terminal;

a returning module 402, configured to return a web page including scripting language code to the terminal based on the request message of the first protocol;

10 a second receiving module 403, configured to receive a request message for establishing a communication connection sent by the terminal by running the scripting language code;

a communication connection module 404, configured to establish a communication connection to the terminal based on the request message for
15 establishing a communication connection; and

an acquisition module 405, configured to determine a first IP address of the terminal by using the communication connection.

[0082] The acquisition module 405 is configured to: receive a data packet of a second protocol sent by the terminal based on the scripting language code by using
20 the communication connection; determine a source IP address for sending the data packet of the second protocol; add the source IP address to a response packet of the second protocol, and return the response packet of the second protocol to the terminal; and receive an IP address returned by the terminal based on the source IP address included in the response packet of the second protocol, and use the returned IP
25 address as the first IP address of the terminal determined by using the communication connection.

[0083] The apparatus further includes a risk control module 406, configured to: determine a second IP address of the terminal based on the request message of the first protocol, and perform risk control processing on the terminal based on the first IP
30 address and the second IP address.

[0084] In the IP address acquisition apparatus, the first protocol includes the Hypertext Transfer Protocol (HTTP), the scripting language code includes the JavaScript code, the communication connection includes the Web Real-Time Communication (WebRTC) connection, and the second protocol includes the User

Datagram Protocol UDP.

[0085] The IP address acquisition apparatus shown in FIG. 4 can be located in gateways of various websites or can be located on a server.

[0086] FIG. 5 is a second schematic structural diagram illustrating an IP address acquisition apparatus according to an embodiment of the present application. The IP address acquisition apparatus includes:

a first sending module 501, configured to send a request message of a first protocol to a network side device;

a receiving module 502, configured to receive a web page sent by the network side device based on the request message of the first protocol, where the web page includes scripting language code;

a communication connection module 503, configured to: run the scripting language code, and send, to the network side device based on the scripting language code, a request message for establishing a communication connection, so that the network side device establishes a communication connection to the apparatus; and

a second sending module 504, configured to send a data packet to the network side device by using the communication connection, so that the network side device determines a first IP address of the apparatus based on the data packet.

[0087] The second sending module 504 is configured to: send a data packet of a second protocol to the network side device based on the scripting language code by using the communication connection, so that the network side device determines a source IP address for sending the data packet of the second protocol; receive a response packet of the second protocol, where the response packet of the second protocol is returned by the network side device and includes the source IP address; and determine an authentic IP address of the apparatus, use the authentic IP address as the first IP address of the apparatus, and send the first IP address of the apparatus to the network side device.

[0088] In the IP address acquisition apparatus, the first protocol includes the Hypertext Transfer Protocol (HTTP), the scripting language code includes the JavaScript code, the communication connection includes the Web Real-Time Communication (WebRTC) connection, and the second protocol includes the User Datagram Protocol UDP.

[0089] The IP address acquisition apparatus shown in FIG. 5 can be located in various terminals, and can be located in various terminals such as a mobile phone, a

PC, and a tablet computer.

[0090] In a typical configuration, a computing device includes one or more processors (CPU), an input/output interface, a network interface, and a memory.

5 **[0091]** The memory can include a non-persistent memory, a random access memory (RAM), a non-volatile memory, and/or another form that are/is in a computer readable medium, for example, a read-only memory (ROM) or a storage device (flash memory). The memory is an example of the computer readable medium.

10 **[0092]** The computer readable medium includes persistent, non-persistent, movable, and unmovable media that can store information by using any method or technology. The information can be a computer readable instruction, a data structure, a program module, or other data. The information can be a computer readable instruction, a data structure, a program module, or other data. Examples of a computer storage medium include but are not limited to: parameter random access memory (PRAM), static random access memory (SRAM), dynamic random access
15 memory (DRAM) or another type of random access memory (RAM), read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or another optical storage, a magnetic cassette, magnetic tape, magnetic tape, a magnetic disk memory or another
20 magnetic storage device, or any other non-transmission medium that can be used to store information that can be accessed by a computing device. According to a definition in this specification, the computer readable medium does not include computer-readable transitory media (transitory media) such as a modulated data signal and a carrier.

25 **[0093]** It should be further noted that, the terms "include", "contain", or their any other variant is intended to cover a non-exclusive inclusion, so that a process, a method, an article, or a device that includes a list of elements not only includes those elements but also includes other elements that are not expressly listed, or further includes elements inherent to such process, method, article, or device. An element
30 defined by "includes a ..." further includes, without more constraints, another identical element in the process, method, article, or device that includes the element.

[0094] A person skilled in the art should understand that the embodiments of the present application can be provided as a method, a system, or a computer program product. Therefore, the present application can use a form of hardware only

embodiments, software only embodiments, or embodiments with a combination of software and hardware. Moreover, the present application can use a form of a computer program product implemented on one or more computer-usable storage media (including but not limited to a magnetic disk memory, a CD-ROM, an optical memory, etc) that include computer usable program code.

[0095] The foregoing embodiments are merely embodiments of the present application, and are not intended to limit the present application. A person skilled in the art can make various modifications and changes to the present application. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of the present application shall fall within the scope of the claims of the present application.

CLAIMS

1. A computer-implemented method for Internet Protocol (IP) address acquisition, the method comprising:

receiving, by one or more processors, a request message from a terminal device, the request message requesting a service;

transmitting, by the one or more processors, computer code to the terminal device;

receiving, by the one or more processors, a communication connection request from the terminal device, the communication connection request being sent from the terminal device in response to running the computer code on the terminal device;

in response to receiving the communication connection request, establishing, by the one or more processors, a communication connection to the terminal device; and

determining, by the one or more processors, a first IP address associated with the terminal device based on one or more communications transmitted through the communication connection, wherein determining the first IP address comprises:

receiving, by the one or more processors, a data packet from the terminal device through the communication connection, the data packet being sent based on the computer code,

determining, by the one or more processors, a source IP address based on the data packet,

sending, by the one or more processors, a response data packet to the terminal device through the communication connection, the response data packet including the source IP address, and

determining, by the one or more processors, the first IP address based on a terminal IP address received from the terminal device, the terminal IP address being determined based on the source IP address.

2. The computer-implemented method of claim 1, wherein the first IP address is the terminal IP address.

3. The computer-implemented method of claim 1, wherein the request message is of Hypertext Transfer Protocol (HTTP), the computer code comprises JavaScript code, the communication connection comprises a Web Real-Time Communication (WebRTC)

connection, and at least one of the data packet and the response data packet is of User Datagram Protocol (UDP).

4. The computer-implemented method of claim 1, further comprising:
determining, by the one or more processors, a second IP address associated with the terminal device based on the request message; and
performing one or more risk control processes based on the first IP address and the second IP address.

5. The computer-implemented method of claim 4, wherein the one or more risk control processes comprises determining that the first IP address differs from the second IP address, and in response, assigning an alarm to the terminal device to monitor subsequent communications with the terminal device.

6. The computer-implemented method of claim 1, wherein the request message is of a first protocol, and the one or more communications transmitted through the communication connection are of a second protocol, the second protocol being different from the first protocol.

7. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to cause one or more processors to perform operations comprising:

receiving a request message from a terminal device, the request message requesting a service;

transmitting computer code to the terminal device;

receiving a communication connection request from the terminal device, the communication connection request being sent from the terminal device in response to running the computer code on the terminal device;

in response to receiving the communication connection request, establishing a communication connection to the terminal device; and

determining a first IP address associated with the terminal device based on one or more communications transmitted through the communication connection, wherein determining the first IP address comprises:

receiving a data packet from the terminal device through the communication

connection, the data packet being sent based on the computer code;

determining a source IP address based on the data packet;

sending a response data packet to the terminal device through the communication connection, the response data packet including the source IP address; and

determining the first IP address based on a terminal IP address received from the terminal device, the terminal IP address being determined based on the source IP address.

8. The non-transitory, computer-readable medium of claim 7, wherein the first IP address is the terminal IP address.

9. The non-transitory, computer-readable medium of claim 7, wherein the request message is of Hypertext Transfer Protocol (HTTP), the computer code comprises JavaScript code, the communication connection comprises a Web Real-Time Communication (WebRTC) connection, and at least one of the data packet and the response data packet is of User Datagram Protocol (UDP).

10. The non-transitory, computer-readable medium of claim 7, further comprising one or more instructions to:

determine, by the one or more processors, a second IP address associated with the terminal device based on the request message; and

perform one or more risk control processes based on the first IP address and the second IP address.

11. The non-transitory, computer-readable medium of claim 10, wherein the one or more risk control processes comprises determining that the first IP address differs from the second IP address, and in response, assigning an alarm to the terminal device to monitor subsequent communications with the terminal device.

12. The non-transitory, computer-readable medium of claim 7, wherein the request message is of a first protocol, and the one or more communications transmitted through the communication connection are of a second protocol, the second protocol being different from

the first protocol.

13. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

receiving a request message from a terminal device, the request message requesting a service;

transmitting computer code to the terminal device;

receiving a communication connection request from the terminal device, the communication connection request being sent from the terminal device in response to running the computer code on the terminal device;

in response to receiving the communication connection request, establishing a communication connection to the terminal device; and

determining a first IP address associated with the terminal device based on one or more communications transmitted through the communication connection, wherein determining the first IP address comprises:

receiving, by the one or more processors, a data packet from the terminal device through the communication connection, the data packet being sent based on the computer code;

determining, by the one or more processors, a source IP address based on the data packet;

sending, by the one or more processors, a response data packet to the terminal device through the communication connection, the response data packet including the source IP address; and

determining, by the one or more processors, the first IP address based on a terminal IP address received from the terminal device, the terminal IP address being determined based on the source IP address.

14. The computer-implemented system of claim 13, wherein the first IP address is the terminal IP address.

15. The computer-implemented system of claim 13, wherein the request message is of Hypertext Transfer Protocol (HTTP), the computer code comprises JavaScript code, the communication connection comprises a Web Real-Time Communication (WebRTC) connection, and at least one of the data packet and the response data packet is of User Datagram Protocol (UDP).

16. The computer-implemented system of claim 13, further comprising one or more operations to:

determine, by the one or more processors, a second IP address associated with the terminal device based on the request message; and

perform one or more risk control processes based on the first IP address and the second IP address.

17. The computer-implemented system of claim 16, wherein the one or more risk control processes comprises determining that the first IP address differs from the second IP address, and in response, assigning an alarm to the terminal device to monitor subsequent communications with the terminal device.