(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0045974**

(51)[2020.01] **H04L 29/06**; H04L 29/12

(13) **B**

(21) 1-2021-07738

(22) 01/12/2021

(30) 202011410695.2 04/12/2020 CN

(45) 26/05/2025 446

(43) 27/06/2022 411A

(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P. R. China

(72) ZHUANG, Shunwan (CN); WANG, Haibo (CN); GU, Yunan (CN); HUANG, Mingqing (CN); XIA, Zhongqi (CN); YAN, Gang (CN).

(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) THIẾT BỊ VÀ PHƯƠNG PHÁP KIỂM TRA CẶP HỆ THỐNG TỰ TRỊ

(21) 1-2021-07738

(57) Sáng chế đề cập đến lĩnh vực kỹ thuật mạng máy tính và bộc lộ phương pháp và thiết bị kiểm tra cặp hệ thống tự trị (AS). Phương pháp này có thể tránh được việc xác định không chính xác cặp AS trong thông tin đường truyền của đường truyền AS trong quá trình kiểm tra của đường truyền AS, và cải thiện độ chính xác của việc kiểm tra đường truyền AS. Phương pháp này được áp dụng với thiết bị mạng. Phương pháp này bao gồm: thu nhận thông tin đường truyền bao gồm cặp AS; xác định thông tin vùng của vùng mà cặp AS trong thông tin đường truyền thuộc về; và kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về, trong đó cặp AS trong thông tin đường truyền bao gồm hai số AS liền kề trong thông tin đường truyền.

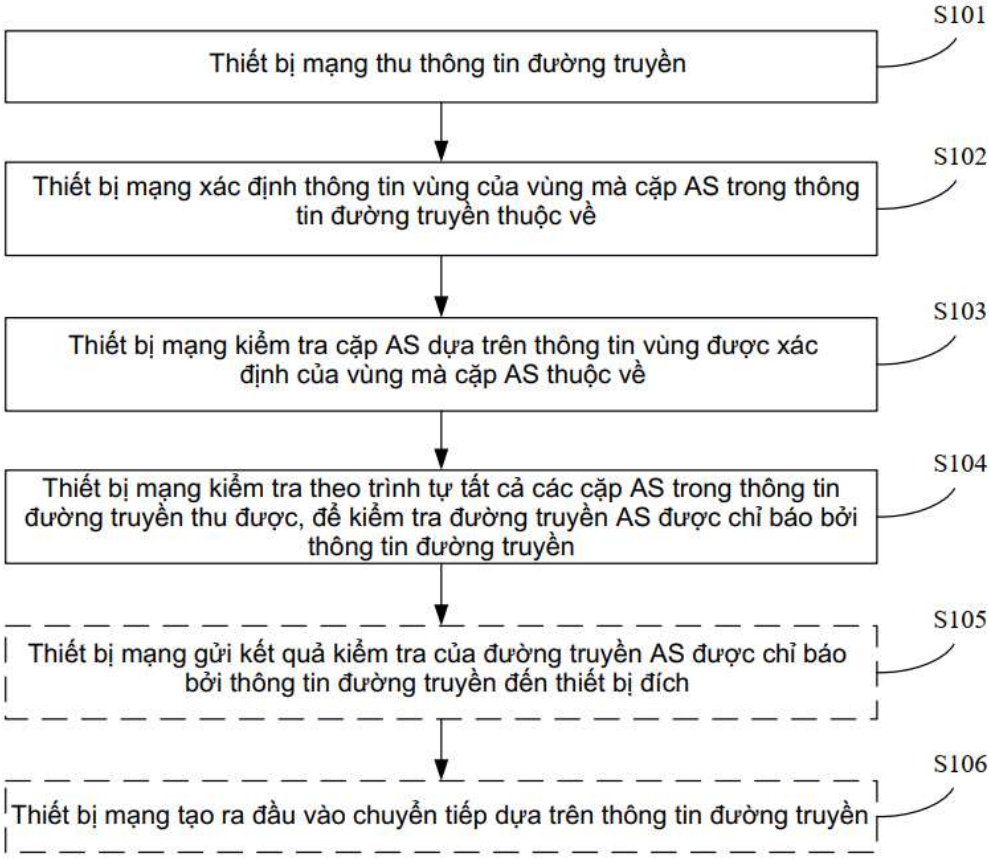

FIG. 5

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực kỹ thuật mạng máy tính, và cụ thể là đến cơ cấu, thiết bị và phương pháp kiểm tra cặp hệ thống tự trị (autonomous system, AS).

Tình trạng kỹ thuật của sáng chế

Hệ thống tự trị (autonomous system, AS) là mạng giao thức internet (Internet Protocol, IP) được quản lý bởi một thực thể và có chính sách định tuyến thống nhất. Hệ số an toàn không được xem xét trong thiết kế ban đầu của giao thức cổng biên (Border Gateway Protocol, BGP). Do đó, khi thông tin định tuyến BGP được truyền giữa các AS lân cận có quan hệ kinh doanh được thiết lập trước, sự rò rỉ thông tin định tuyến dễ xảy ra. Sự rò rỉ thông tin định tuyến thường khiến lưu lượng di chuyển trên đường truyền dài hơn, và do đó làm tăng độ trễ truyền lưu lượng. Ngoài ra, sự rò rỉ thông tin định tuyến nguy hiểm có thể còn gây ra các rủi ro an ninh như gián đoạn truy nhập tuyến bất thường, theo dõi lưu lượng, tấn công xen giữa, và tấn công giả mạo.

Để ngăn ngừa việc rò rỉ tuyến, AS thông thường có thể kiểm tra tất cả các cặp AS (AS pairs) trong thông tin đường truyền của đường truyền AS (AS path) trong thông tin định tuyến BGP thu được theo nguyên tắc thung lũng tự do (valley free) bằng cách sử dụng cơ chế hạ tầng khóa công khai tài nguyên (resource public key infrastructure, RPKI), để xác định hiệu lực của đường truyền AS, và còn xác định an ninh của tuyến BGP. Tuy nhiên, khi AS kiểm tra thông tin đường truyền thu được của đường truyền AS bằng cách sử dụng kỹ thuật thông thường, AS có thể xác định không chính xác cặp AS trong thông tin đường truyền của đường truyền AS. Kết quả là, kết quả kiểm tra của đường truyền AS là không chính xác.

Dựa trên điều này, làm thế nào để tránh được việc xác định không chính xác cặp AS trong thông tin đường truyền của đường truyền AS trong quá trình

kiểm tra của đường truyền AS là vấn đề kỹ thuật cần được giải quyết khẩn cấp trong kỹ thuật thông thường.

Bản chất kỹ thuật của sáng chế

Các phương án của sáng chế đề xuất cơ cấu, thiết bị, và phương pháp kiểm tra cặp AS. Phương pháp này có thể tránh được việc xác định không chính xác cặp AS trong thông tin đường truyền của đường truyền AS trong quá trình kiểm tra của đường truyền AS, và cải thiện độ chính xác của việc kiểm tra đường truyền AS.

Theo khía cạnh thứ nhất, phương án của sáng chế đề xuất phương pháp kiểm tra cặp AS, và phương pháp có thể được áp dụng với thiết bị mạng. Phương pháp này bao gồm các bước: thu nhận thông tin đường truyền bao gồm cặp AS; xác định thông tin vùng của vùng mà cặp AS trong thông tin đường truyền thuộc về; và sau đó kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về. Cặp AS trong thông tin đường truyền bao gồm hai số AS liền kề trong thông tin đường truyền.

Khi cặp AS được kiểm tra bằng cách sử dụng phương pháp kiểm tra cặp AS được đề xuất trong phương án này của sáng chế, thông tin vùng của vùng mà cặp AS thuộc về được đưa ra để kiểm tra cặp AS. Điều này có thể tránh được trường hợp trong đó quan hệ kinh doanh được xác định không chính xác do cùng cặp AS có các quan hệ kinh doanh khác nhau trong các vùng khác nhau trong quá trình kiểm tra của cặp AS trong thông tin đường truyền. Ngoài ra, cặp AS có thể được kiểm tra chính xác, và khi hiệu lực của đường truyền tương ứng với thông tin đường truyền bao gồm cặp AS được kiểm tra theo nguyên tắc thung lũng tự do, độ chính xác kiểm tra được cải thiện tương ứng.

Theo cách thức thực hiện khả thi, việc kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về bao gồm: kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền.

Theo cách thức thực hiện khả thi khác, việc kiểm tra cặp AS dựa trên

thông tin vùng được xác định của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền bao gồm: khi cơ sở dữ liệu đầu vào cấp quyền bao gồm đầu vào cấp quyền mà bao gồm cặp AS và ký hiệu nhận dạng vùng tương ứng với thông tin vùng của vùng mà cặp AS thuộc về, xác định rằng cặp AS được kiểm tra thành công.

Theo cách thức thực hiện khả thi khác, việc kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền bao gồm: khi cơ sở dữ liệu đầu vào cấp quyền không bao gồm đầu vào cấp quyền mà bao gồm cặp AS và ký hiệu nhận dạng vùng tương ứng với thông tin vùng của vùng mà cặp AS thuộc về, xác định rằng cặp AS không được kiểm tra.

Theo các cách thức thực hiện khả thi nêu trên, do cơ sở dữ liệu đầu vào cấp quyền bao gồm ký hiệu nhận dạng vùng của vùng mà cặp AS thuộc về, nên khi cặp AS được kiểm tra từ cơ sở dữ liệu đầu vào cấp quyền dựa trên thông tin vùng của vùng mà cặp AS thuộc về, không chỉ cặp AS giống như cặp AS cần được kiểm tra cần được so khớp từ cơ sở dữ liệu đầu vào cấp quyền, mà việc liệu ký hiệu nhận dạng vùng của cặp AS giống như cặp AS cần được kiểm tra có so khớp với thông tin vùng của vùng mà cặp AS cần được kiểm tra thuộc về cần được xác định từ cơ sở dữ liệu đầu vào cấp quyền.

Điều này có thể tránh được trường hợp trong đó quan hệ kinh doanh được xác định không chính xác do cùng cặp AS có các quan hệ kinh doanh khác nhau trong các vùng khác nhau trong quá trình kiểm tra của cặp AS trong thông tin đường truyền. Ngoài ra, cặp AS có thể được kiểm tra chính xác, và khi hiệu lực của đường truyền tương ứng với thông tin đường truyền bao gồm cặp AS được kiểm tra theo nguyên tắc thung lũng tự do, độ chính xác kiểm tra được cải thiện tương ứng.

Theo cách thức thực hiện khả thi khác, việc xác định thông tin vùng của vùng mà cặp AS trong thông tin đường truyền thuộc về bao gồm: xác định, từ thông tin định tuyến bao gồm thông tin đường truyền, thông tin vùng của vùng

mà cặp AS thuộc về; hoặc xác định, dựa trên tiền tố trong thông tin định tuyến, thông tin vùng của vùng mà cặp AS thuộc về.

Theo cách thức thực hiện khả thi này, thông tin vùng của vùng mà cặp AS trong thông tin đường truyền thuộc về có thể thu được. Theo cách này, thiết bị mạng có thể kiểm tra cặp AS trong cơ sở dữ liệu đầu vào cấp quyền dựa trên thông tin vùng. Điều này cải thiện độ chính xác của việc kiểm tra cặp AS.

Lưu ý rằng trong phương án này của sáng chế, thông tin vùng của vùng mà cặp AS thuộc về có thể thu được theo cách bất kỳ mà có thể được sử dụng để thu nhận thông tin vùng.

Theo cách thức thực hiện khả thi khác, trước khi việc kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền, phương pháp này còn bao gồm: thu nhận cơ sở dữ liệu đầu vào cấp quyền.

Theo cách thức thực hiện khả thi khác, cơ sở dữ liệu đầu vào cấp quyền bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ nhất; và bước thu nhận cơ sở dữ liệu đầu vào cấp quyền bao gồm: thu bản tin đơn vị dữ liệu giao thức (protocol data unit, PDU) từ máy chủ, trong đó bản tin PDU bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước và ký hiệu nhận dạng vùng của vùng mà cặp AS có quan hệ kinh doanh được thiết lập trước thuộc về; và sau đó tạo cơ sở dữ liệu đầu vào cấp quyền thứ nhất dựa trên bản tin PDU thu được.

Theo cách thức thực hiện khả thi khác, cơ sở dữ liệu đầu vào cấp quyền còn bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ hai; và bước thu nhận cơ sở dữ liệu đầu vào cấp quyền bao gồm: tạo cơ sở dữ liệu đầu vào cấp quyền thứ hai dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng, trong đó bảng định tuyến mạng và/hoặc dữ liệu mạng bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước và thông tin vùng của vùng mà cặp AS có quan hệ kinh doanh được thiết lập trước thuộc về.

Theo các cách thức thực hiện khả thi nêu trên, thiết bị mạng có thể xây dựng theo cách cục bộ, theo các cách khác nhau, cơ sở dữ liệu đầu vào cấp

quyền mà bao gồm ký hiệu nhận dạng của vùng mà cặp AS thuộc về. Theo cách này, cặp AS có thể được kiểm tra chính xác dựa trên cơ sở dữ liệu đầu vào cấp quyền được xây dựng và thông tin vùng của vùng mà cặp AS cần được kiểm tra thuộc về. Điều này cải thiện độ chính xác của việc kiểm tra đường truyền tương ứng với thông tin đường truyền bao gồm cặp AS.

Theo cách thức thực hiện khả thi khác, việc kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền bao gồm: kiểm tra cặp AS dựa trên thông tin vùng của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền thứ nhất; và nếu cặp AS không được kiểm tra, kiểm tra cặp AS dựa trên thông tin vùng của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Theo cách thức thực hiện khả thi này, thiết bị mạng đầu tiên có thể kiểm tra cặp AS dựa trên thông tin vùng của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền thứ nhất thu được từ máy chủ. Khi cặp AS không được kiểm tra, thiết bị mạng có thể kiểm tra lại cặp AS dựa trên thông tin vùng của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền thứ hai thu được bằng cách phân tích bảng định tuyến mạng và/hoặc dữ liệu mạng. Theo cách này, khi dữ liệu cấp quyền của máy chủ không đủ toàn diện, cặp AS cần được kiểm tra có thể còn được kiểm tra bằng cách sử dụng dữ liệu cấp quyền thu được bằng cách phân tích bảng định tuyến mạng và/hoặc dữ liệu mạng. Điều này còn làm giảm tỷ lệ xác định không chính xác trong quá trình kiểm tra của cặp AS.

Theo cách thức thực hiện khả thi khác, việc kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền bao gồm: kiểm tra cặp AS dựa trên thông tin vùng của vùng mà cặp AS thuộc về và đầu vào cấp quyền đích mà ở trong cơ sở dữ liệu đầu vào cấp quyền và tương ứng với tiền tố trong thông tin đường truyền, trong đó phiên bản IP của cặp AS trong đầu vào cấp quyền đích là giống như phiên bản IP trong tiền tố trong thông tin đường truyền.

Cách thức thực hiện khả thi này loại bỏ tác động gây ra cho việc kiểm tra

cặp AS trong thông tin đường truyền do các AS sử dụng các phiên bản IP khác nhau.

Theo cách thức thực hiện khả thi khác, thông tin đường truyền bao gồm các số AS được bố trí theo thứ tự thiết lập trước, và các số AS được sử dụng để chỉ báo đường truyền tương ứng với thông tin đường truyền; và phương pháp này còn bao gồm: kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền, để kiểm tra đường truyền tương ứng với thông tin đường truyền.

Theo cách thức thực hiện khả thi này, cặp AS được kiểm tra bằng cách sử dụng phương pháp được đề xuất trong phương án này của sáng chế. Điều này có thể tránh được trường hợp trong đó quan hệ kinh doanh được xác định không chính xác do cùng cặp AS có các quan hệ kinh doanh khác nhau trong các vùng khác nhau trong quá trình kiểm tra của cặp AS trong thông tin đường truyền. Theo cách này, cặp AS có thể được kiểm tra chính xác, và khi hiệu lực của đường truyền tương ứng với thông tin đường truyền bao gồm cặp AS được kiểm tra theo nguyên tắc thung lũng tự do, độ chính xác kiểm tra được cải thiện tương ứng.

Theo cách thức thực hiện khả thi khác, phương pháp này còn bao gồm: khi cặp AS trong thông tin đường truyền không được kiểm tra trong lần đầu tiên, đảo ngược cặp AS mà chưa được kiểm tra trong thông tin đường truyền; và sau đó kiểm tra cặp AS được đảo ngược, để hoàn thành việc kiểm tra của đường truyền tương ứng với thông tin đường truyền.

Theo cách thức thực hiện khả thi này, khi cơ sở dữ liệu đầu vào cấp quyền được xây dựng, chỉ cơ sở dữ liệu bao gồm quan hệ kinh doanh đơn cần được xây dựng. Điều này cải thiện hiệu quả xây dựng cơ sở dữ liệu đầu vào cấp quyền. Do chỉ cặp C2P AS, cặp P2C AS, và cặp P2P AS thường được bao gồm trong quá trình kiểm tra của thông tin đường truyền, nên cơ sở dữ liệu đầu vào cấp quyền bao gồm chỉ cặp C2P AS có thể được xây dựng, hoặc cơ sở dữ liệu đầu vào cấp quyền bao gồm chỉ cặp P2C AS có thể được xây dựng. Khi cặp AS không được kiểm tra trong lần đầu tiên, chỉ cặp AS mà chưa được kiểm tra cần được đảo

ngược sau đó. Khi đường truyền có hiệu lực, cùng cặp AS có thể được tìm thấy thông qua việc so khớp từ cơ sở dữ liệu đầu vào cấp quyền cho cặp AS được đảo ngược, sao cho việc kiểm tra có thể được thực hiện trôi chảy.

Theo cách thức thực hiện khả thi khác, phương pháp này còn bao gồm: nếu thông tin đường truyền bao gồm nhiều nhất một cặp AS mà không được kiểm tra, xác định rằng đường truyền tương ứng với thông tin đường truyền được kiểm tra thành công.

Theo cách thức thực hiện khả thi khác, phương pháp này còn bao gồm: tạo đầu vào chuyển tiếp thứ nhất dựa trên thông tin đường truyền.

Theo hai cách thức thực hiện khả thi, thiết bị mạng tạo ra đầu vào chuyển tiếp dựa trên thông tin đường truyền tương ứng với đường truyền mà được kiểm tra thành công. Do đường truyền tương ứng với đầu vào chuyển tiếp được kiểm tra thành công, đầu vào chuyển tiếp là đầu vào chuyển tiếp an toàn. Theo cách này, khi chuyển tiếp bản tin sau đó, thiết bị mạng có thể sử dụng đầu vào chuyển tiếp an toàn, mà không gây ra sự rò rỉ tuyến. Điều này đảm bảo sự an toàn của dữ liệu được truyền.

Theo cách thức thực hiện khả thi khác, phương pháp này còn bao gồm: nếu thông tin đường truyền bao gồm ít nhất hai cặp AS mà không được kiểm tra, xác định rằng đường truyền tương ứng với thông tin đường truyền không được kiểm tra.

Theo cách thức thực hiện khả thi khác, phương pháp này còn bao gồm: tạo đầu vào chuyển tiếp thứ hai dựa trên thông tin đường truyền; và sau đó đánh dấu thông tin cụ thể cho đầu vào chuyển tiếp thứ hai, trong đó thông tin cụ thể được sử dụng để chỉ báo liệu đầu vào chuyển tiếp thứ hai là đầu vào chuyển tiếp rủi ro cao hay đầu vào chuyển tiếp ưu tiên thấp.

Theo hai cách thức thực hiện khả thi, thiết bị mạng có thể tạo ra đầu vào chuyển tiếp dựa trên thông tin đường truyền tương ứng với đường truyền mà không được kiểm tra. Do đường truyền tương ứng với đầu vào chuyển tiếp không được kiểm tra, nghĩa là, đầu vào chuyển tiếp là đầu vào chuyển tiếp

không an toàn, nên khi bản tin được chuyển tiếp bằng cách sử dụng đầu vào chuyển tiếp, sự rò rỉ tuyến có thể xảy ra, và sự rò rỉ dữ liệu bị gây ra. Ngoài ra, thông tin cụ thể được đánh dấu cho các đầu vào chuyển tiếp không an toàn này, để nhắc nhở thiết bị mạng xem xét toàn diện rủi ro mang lại bởi các đầu vào chuyển tiếp trong quá trình sử dụng các đầu vào chuyển tiếp này. Ví dụ, các đầu vào chuyển tiếp không được sử dụng để chuyển tiếp bản tin dữ liệu có yêu cầu an toàn tương đối cao. Nói cách khác, thiết bị mạng có thể sử dụng các đầu vào chuyển tiếp này dựa trên tình hình thực tế. Điều này cải thiện tính linh hoạt của việc sử dụng đầu vào chuyển tiếp bởi thiết bị mạng.

Theo cách thức thực hiện khả thi khác, nếu thiết bị mạng là thiết bị mạng trong AS thứ nhất, phương pháp này còn bao gồm: gửi kết quả kiểm tra của đường truyền tương ứng với thông tin đường truyền đến thiết bị đích, trong đó thiết bị đích là thiết bị mà ở trong AS thứ nhất và được kết nối với thiết bị mạng để truyền thông.

Theo cách thức thực hiện khả thi này, sau khi thu bản tin cập nhật BGP bao gồm thông tin đường truyền, thiết bị đích có thể xử lý thông tin đường truyền dựa trên kết quả kiểm tra, mà không kiểm tra thông tin đường truyền. Việc này làm giảm các tài nguyên được sử dụng của thiết bị đích, và cải thiện hiệu quả của thiết bị đích.

Theo cách thức thực hiện khả thi khác, "thu nhận thông tin đường truyền bao gồm cặp AS" bao gồm: thu nhận bản tin cập nhật giao thức cổng biên (border gateway protocol, BGP), trong đó bản tin cập nhật BGP bao gồm thông tin đường truyền.

Theo cách thức thực hiện khả thi khác, phương pháp này còn bao gồm: sau khi thu bản tin cập nhật BGP, kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra đường truyền tương ứng với thông tin đường truyền; hoặc trước khi gửi bản tin cập nhật BGP, kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra đường truyền tương ứng với thông tin đường truyền.

Theo cách thức thực hiện khả thi này, dịp mà trong đó thiết bị mạng kiểm tra đường truyền tương ứng với thông tin đường truyền bao gồm cặp AS là tương đối linh hoạt. Cụ thể, thiết bị mạng có thể kiểm tra đường truyền sau khi thu thông tin đường truyền, hoặc có thể kiểm tra đường truyền trước khi gửi thông tin đường truyền và sau khi thu thông tin đường truyền hoặc tạo thông tin đường truyền. Điều này chỉ báo rằng phương pháp được đề xuất trong phương án này của sáng chế có thể áp dụng được với nhiều kịch bản, và do đó làm tăng phạm vi ứng dụng của phương pháp theo phương án này của sáng chế.

Theo khía cạnh thứ hai, phương án của sáng chế đề xuất thiết bị kiểm tra cặp hệ thống tự trị (autonomous system, AS), và thiết bị này được áp dụng với thiết bị mạng. Thiết bị này bao gồm: bộ thu nhận, được cấu hình để thu nhận thông tin đường truyền, trong đó thông tin đường truyền bao gồm cặp AS, và cặp AS bao gồm hai số AS liền kề trong thông tin đường truyền; và bộ xử lý, được cấu hình để: xác định thông tin vùng của vùng mà cặp AS thuộc về; và kiểm tra cặp AS dựa trên thông tin vùng.

Theo cách thức thực hiện khả thi, bộ xử lý được cấu hình cụ thể để kiểm tra cặp AS dựa trên thông tin vùng và cơ sở dữ liệu đầu vào cấp quyền.

Theo cách thức thực hiện khả thi khác, bộ xử lý được cấu hình cụ thể để: khi cơ sở dữ liệu đầu vào cấp quyền bao gồm đầu vào cấp quyền mà bao gồm cặp AS và ký hiệu nhận dạng vùng tương ứng với thông tin vùng, xác định rằng cặp AS được kiểm tra thành công.

Theo cách thức thực hiện khả thi khác, bộ xử lý được cấu hình cụ thể để: khi cơ sở dữ liệu đầu vào cấp quyền không bao gồm đầu vào cấp quyền mà bao gồm cặp AS và ký hiệu nhận dạng vùng tương ứng với thông tin vùng, xác định rằng cặp AS không được kiểm tra.

Theo cách thức thực hiện khả thi khác, bộ xử lý còn được cấu hình để: xác định, từ thông tin định tuyến bao gồm thông tin đường truyền, thông tin vùng của vùng mà cặp AS thuộc về; hoặc xác định, dựa trên tiền tố trong thông tin định tuyến, thông tin vùng của vùng mà cặp AS thuộc về.

Theo cách thức thực hiện khả thi khác, bộ thu nhận còn được cấu hình để thu nhận cơ sở dữ liệu đầu vào cấp quyền.

Theo cách thức thực hiện khả thi khác, cơ sở dữ liệu đầu vào cấp quyền bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ nhất, và thiết bị còn bao gồm bộ thu, được cấu hình để thu bản tin đơn vị dữ liệu giao thức (PDU) từ máy chủ, trong đó bản tin PDU bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước và ký hiệu nhận dạng vùng của vùng mà cặp AS có quan hệ kinh doanh được thiết lập trước thuộc về; và bộ xử lý còn được cấu hình để tạo ra cơ sở dữ liệu đầu vào cấp quyền thứ nhất dựa trên bản tin PDU.

Theo cách thức thực hiện khả thi khác, cơ sở dữ liệu đầu vào cấp quyền còn bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ hai; và bộ xử lý còn được cấu hình để tạo ra cơ sở dữ liệu đầu vào cấp quyền thứ hai dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng. Bảng định tuyến mạng và/hoặc dữ liệu mạng bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước và thông tin vùng của vùng mà cặp AS có quan hệ kinh doanh được thiết lập trước thuộc về.

Theo cách thức thực hiện khả thi khác, bộ xử lý còn được cấu hình riêng để: kiểm tra cặp AS dựa trên thông tin vùng và cơ sở dữ liệu đầu vào cấp quyền thứ nhất; và nếu cặp AS không được kiểm tra, kiểm tra cặp AS dựa trên thông tin vùng và cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Theo cách thức thực hiện khả thi khác, bộ xử lý còn được cấu hình riêng để kiểm tra cặp AS dựa trên thông tin vùng và đầu vào cấp quyền đích mà ở trong cơ sở dữ liệu đầu vào cấp quyền và tương ứng với tiền tố trong thông tin đường truyền, trong đó phiên bản giao thức internet (IP) của cặp AS trong đầu vào cấp quyền đích là giống như phiên bản IP trong tiền tố trong thông tin đường truyền.

Theo cách thức thực hiện khả thi khác, thông tin đường truyền bao gồm các số AS được sắp xếp theo thứ tự thiết lập trước, và các số AS được sử dụng để chỉ báo đường truyền tương ứng với thông tin đường truyền; và bộ xử lý còn được cấu hình để kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường

truyền, để kiểm tra đường truyền tương ứng với thông tin đường truyền.

Theo cách thức thực hiện khả thi khác, bộ xử lý còn được cấu hình để: khi cặp AS trong thông tin đường truyền không được kiểm tra trong lần đầu tiên, đảo ngược cặp AS mà chưa được kiểm tra trong thông tin đường truyền; và kiểm tra cặp AS được đảo ngược, để hoàn thành việc kiểm tra đường truyền tương ứng với thông tin đường truyền.

Theo cách thức thực hiện khả thi khác, bộ xử lý còn được cấu hình để: nếu thông tin đường truyền bao gồm nhiều nhất một cặp AS mà không được kiểm tra, xác định rằng đường truyền tương ứng với thông tin đường truyền được kiểm tra thành công.

Theo cách thức thực hiện khả thi khác, bộ xử lý còn được cấu hình để tạo ra đầu vào chuyển tiếp thứ nhất dựa trên thông tin đường truyền.

Theo cách thức thực hiện khả thi khác, bộ xử lý còn được cấu hình để: nếu thông tin đường truyền bao gồm ít nhất hai cặp AS mà không được kiểm tra, xác định rằng đường truyền tương ứng với thông tin đường truyền không được kiểm tra.

Theo cách thức thực hiện khả thi khác, bộ xử lý còn được cấu hình để: tạo ra đầu vào chuyển tiếp thứ hai dựa trên thông tin đường truyền; và đánh dấu thông tin cụ thể cho đầu vào chuyển tiếp thứ hai, trong đó thông tin cụ thể được sử dụng để chỉ báo liệu đầu vào chuyển tiếp thứ hai là đầu vào chuyển tiếp rủi ro cao hoặc đầu vào chuyển tiếp ưu tiên thấp.

Theo cách thức thực hiện khả thi khác, nếu thiết bị mạng là thiết bị mạng trong AS thứ nhất, thiết bị còn bao gồm: bộ gửi, được cấu hình để gửi kết quả kiểm tra đường truyền tương ứng với thông tin đường truyền đến thiết bị đích, trong đó thiết bị đích là thiết bị mà ở trong AS thứ nhất và được kết nối với thiết bị mạng để truyền thông.

Theo cách thức thực hiện khả thi khác, bộ thu nhận được cấu hình cụ thể để thu nhận bản tin cập nhật giao thức cổng biên (border gateway protocol,

BGP), trong đó bản tin cập nhật BGP bao gồm thông tin đường truyền.

Theo cách thức thực hiện khả thi khác, bộ xử lý còn được cấu hình để: sau khi bản tin cập nhật BGP được thu, kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra đường truyền tương ứng với thông tin đường truyền; hoặc trước khi bản tin cập nhật BGP được gửi, kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra đường truyền tương ứng với thông tin đường truyền.

Sẽ được hiểu rằng các bộ phận/môđun chức năng thu được thông qua việc phân chia có thể được tích hợp vào một hoặc nhiều bộ phận/môđun. Đối với các phần mô tả của các giải pháp kỹ thuật khả thi được thực hiện bởi các bộ phận/môđun chức năng thu được thông qua việc phân chia và các phần mô tả hiệu quả có lợi, tham khảo các phần mô tả của các giải pháp kỹ thuật theo khía cạnh thứ nhất hoặc các cách thức thực hiện khả thi tương ứng của khía cạnh thứ nhất. Chi tiết không được mô tả lại ở đây.

Theo khía cạnh thứ ba, phương án của sáng chế đề xuất thiết bị kiểm tra cặp AS. Thiết bị kiểm tra cặp AS bao gồm bộ nhớ và một hoặc nhiều bộ xử lý. Bộ nhớ được ghép nối tới bộ xử lý. Bộ nhớ được cấu hình để lưu trữ các lệnh máy tính. Bộ xử lý được cấu hình để gọi ra các lệnh máy tính, để thực hiện phương pháp theo bất kỳ một trong số khía cạnh thứ nhất hoặc các cách thức thực hiện khả thi của khía cạnh thứ nhất.

Theo khía cạnh thứ tư, phương án của sáng chế đề xuất cơ cấu kiểm tra cặp AS. Cơ cấu là thiết bị mạng trong AS. Cơ cấu được cấu hình để thực hiện phương pháp theo bất kỳ một trong số khía cạnh thứ nhất hoặc các cách thức thực hiện khả thi của khía cạnh thứ nhất.

Theo khía cạnh thứ năm, phương án của sáng chế đề xuất phương tiện lưu trữ đọc được bởi máy tính, ví dụ, phương tiện lưu trữ đọc được bởi máy tính loại không tạm thời. Phương tiện lưu trữ đọc được bởi máy tính lưu trữ chương trình máy tính (hoặc các lệnh). Khi chương trình máy tính (hoặc các lệnh) được chạy trên thiết bị kiểm tra cặp AS, thiết bị kiểm tra cặp AS được cho phép thực hiện

phương pháp theo cách thức thực hiện bất kỳ của khía cạnh thứ nhất.

Theo khía cạnh thứ sáu, phương án của sáng chế đề xuất sản phẩm chương trình máy tính. Khi sản phẩm chương trình máy tính chạy trên thiết bị kiểm tra cặp AS, phương pháp theo cách thức thực hiện bất kỳ của khía cạnh thứ nhất được thực hiện.

Theo khía cạnh thứ bảy, phương án của sáng chế đề xuất hệ thống chip, bao gồm bộ xử lý. Bộ xử lý được cấu hình để gọi ra và chạy, từ bộ nhớ, chương trình máy tính được lưu trữ trong bộ nhớ, để thực hiện phương pháp theo cách thức thực hiện bất kỳ của khía cạnh thứ nhất.

Có thể hiểu rằng bất kỳ một trong số thiết bị, phương tiện lưu trữ máy tính, sản phẩm chương trình máy tính, hệ thống chip, hoặc tương tự được đề xuất ở trên có thể được áp dụng với phương pháp tương ứng được đề xuất ở trên. Do đó, đối với các hiệu quả có lợi mà có thể đạt được bởi thiết bị, phương tiện lưu trữ máy tính, sản phẩm chương trình máy tính, hệ thống chip, hoặc tương tự, tham khảo các hiệu quả có lợi của phương pháp tương ứng. Chi tiết không được mô tả lại ở đây.

Trong các phương án của sáng chế, tên gọi của thiết bị kiểm tra cặp AS không tạo ra bất kỳ giới hạn nào với các thiết bị hoặc các môđun chức năng. Trong quá trình thực hiện thực tế, các thiết bị hoặc môđun chức năng này có thể có các tên gọi khác. Các thiết bị hoặc môđun chức năng nằm trong phạm vi của các yêu cầu bảo hộ và các kỹ thuật tương đương của chúng trong các phương án của sáng chế, miễn là các chức năng của các thiết bị hoặc môđun chức năng là tương tự với các thiết bị hoặc môđun chức năng được mô tả trong các phương án của sáng chế.

Mô tả vắn tắt các hình vẽ

FIG.1 là sơ đồ giản lược của đường truyền AS có hiệu lực theo phương án của sáng chế;

FIG.2(a) và FIG.2(b) là các sơ đồ giản lược của các đường truyền AS

không có hiệu lực theo phương án của sáng chế;

FIG.3 là sơ đồ giản lược của cấu trúc phần cứng của thiết bị mạng theo phương án của sáng chế;

FIG.4 là sơ đồ giản lược của kiến trúc của hệ thống kiểm tra theo phương án của sáng chế;

FIG.5 là lưu đồ giản lược của phương pháp kiểm tra cặp AS theo phương án của sáng chế;

FIG.6 là lưu đồ giản lược của phương pháp để tạo cơ sở dữ liệu đầu vào cấp quyền thứ nhất theo phương án của sáng chế;

FIG.7(a) và FIG.7(b) là các sơ đồ giản lược của việc đăng ký thông tin ASPA bởi người dùng AS trên trang web RIR theo phương án của sáng chế;

FIG.8 là sơ đồ giản lược của bản tin PDU theo phương án của sáng chế;

FIG.9 là lưu đồ giản lược của phương pháp để tạo cơ sở dữ liệu đầu vào cấp quyền thứ hai theo phương án của sáng chế;

FIG.10 là sơ đồ giản lược của cấu trúc thiết bị kiểm tra cặp AS 100 theo phương án của sáng chế;

FIG.11 là sơ đồ giản lược của cấu trúc hệ thống chip theo phương án của sáng chế; và

FIG.12 là sơ đồ giản lược của cấu trúc sản phẩm chương trình máy tính theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Để hiểu hơn về các phương án của sáng chế, phần sau đây mô tả một số thuật ngữ hoặc kỹ thuật được sử dụng trong các phương án của sáng chế.

(1) quan hệ kinh doanh lân cận AS

Quan hệ kinh doanh lân cận AS là quan hệ hợp đồng công việc được ký giữa hai AS lân cận về cách thức thanh toán chuyển tiếp lưu lượng. Các quan hệ kinh doanh cơ sở bao gồm quan hệ khách hàng với nhà cung cấp (customer to

provider, C2P), quan hệ nhà cung cấp với khách hàng (provider to customer, P2C), và quan hệ ngang hàng (peer to peer, P2P), và quan hệ anh em với anh em (sibling to sibling, S2S).

Quan hệ C2P có nghĩa rằng AS khách hàng phục vụ như là bộ gửi tuyến BGP, thanh toán cho AS nhà cung cấp, và gửi tuyến của AS khách hàng và tuyến của khách hàng đến internet (internet) thông qua AS nhà cung cấp, để thực hiện truyền thông giữa AS khách hàng và internet thông qua AS nhà cung cấp. Có thể hiểu được rằng AS nhà cung cấp là bộ thu tuyến BGP.

Quan hệ P2C có thể được hiểu là sự mô tả đảo ngược của quan hệ C2P, và nội dung được xác định bởi quan hệ P2C là giống như nội dung được xác định bởi quan hệ C2P. Sự khác nhau là ở chỗ quan hệ C2P được mô tả từ quan điểm của AS khách hàng, trái lại quan hệ P2C được mô tả từ quan điểm của AS nhà cung cấp. Các chi tiết không được mô tả.

Ngoài ra, hai AS có quan hệ P2P là ngang hàng, và các AS ngang hàng là tự do song phương. Tuy nhiên, từ quan điểm về kinh tế, một trong số hai AS ngang hàng không mong muốn AS còn lại truy nhập internet thông qua AS này. Do đó, một trong số hai AS ngang hàng thông báo chỉ tuyến của AS này và tuyến của khách hàng đến AS còn lại.

Hai AS có quan hệ S2S thuộc về cùng tổ chức, và có thể trao đổi lưu lượng tự do mà không mất phí.

(2) Các thuật ngữ khác

Trong các phương án của sáng chế, thuật ngữ "ví dụ" hoặc "ví dụ" được sử dụng để thể hiện việc đưa ra ví dụ, sự minh họa, hoặc sự mô tả. Phương án hoặc cách thức thực hiện bất kỳ mô tả là "ví dụ" hoặc với "ví dụ" trong các phương án của sáng chế cần được giải thích là ưu tiên hơn hoặc có ưu điểm hơn so với phương án khác hoặc cách thức thực hiện khác. Chính xác là, việc sử dụng thuật ngữ như "ví dụ" hoặc "ví dụ" nhằm thể hiện khái niệm liên quan theo cách cụ thể.

Các thuật ngữ "thứ nhất" và "thứ hai" trong các phương án của sáng chế chỉ nhằm mục đích mô tả, và không nên được hiểu là chỉ báo hoặc ngụ ý tầm quan trọng tương ứng hoặc ngầm chỉ báo số lượng dấu hiệu kỹ thuật được chỉ báo. Do đó, dấu hiệu bị giới hạn bởi "thứ nhất" hoặc "thứ hai" có thể là ngầm hoặc rõ ràng bao gồm một hoặc nhiều dấu hiệu. Trong phần mô tả của sáng chế, trừ khi được định rõ khác, "các" nghĩa là hai hoặc nhiều hơn hai.

Thuật ngữ "ít nhất một" trong sáng chế nghĩa là một hoặc nhiều, và thuật ngữ "các" trong sáng chế nghĩa là hai hoặc nhiều hơn hai. Ví dụ, "các bản tin thứ hai" nghĩa là hai hoặc nhiều hơn hai bản tin thứ hai. Các thuật ngữ "hệ thống" và "mạng" có thể được sử dụng hoán đổi cho nhau trong bản mô tả này.

Sẽ được hiểu rằng các thuật ngữ được sử dụng trong các phần mô tả của các ví dụ khác nhau trong bản mô tả này chỉ nhằm mô tả các ví dụ cụ thể, mà không nhằm giới hạn bản mô tả này. Các thuật ngữ "một" ("a", "an") và "the" của các dạng số ít được sử dụng trong các phần mô tả của các ví dụ khác nhau và các yêu cầu bảo hộ kèm theo cũng nhằm bao gồm các dạng số nhiều, trừ khi được định rõ khác theo ngữ cảnh rõ ràng.

Cần hiểu rằng thuật ngữ "và/hoặc" được sử dụng trong bản mô tả này chỉ báo và bao gồm bất kỳ hoặc tất cả các kết hợp khả thi của một hoặc nhiều mục trong các mục được liệt kê liên quan. Thuật ngữ "và/hoặc" mô tả quan hệ kết hợp để mô tả các đối tượng được kết hợp và biểu diễn rằng ba quan hệ có thể tồn tại. Ví dụ, A và/hoặc B có thể biểu diễn ba trường hợp sau đây: chỉ A tồn tại, cả A và B cùng tồn tại, và chỉ B tồn tại. Ngoài ra, ký hiệu "/" trong sáng chế luôn chỉ báo quan hệ "hoặc" giữa các đối tượng được kết hợp.

Cần hiểu rằng số thứ tự của các xử lý nêu trên không có nghĩa là các trình tự thực hiện trong các phương án của sáng chế. Các trình tự thực hiện của các xử lý này cần được xác định dựa trên các chức năng và logic bên trong của các xử lý, và không nên hiểu là tạo ra giới hạn bất kỳ lên việc thực hiện các xử lý của các phương án của sáng chế.

Sẽ được hiểu rằng xác định B dựa trên A không có nghĩa là B được xác

định dựa trên chỉ A, mà B có thể còn được xác định dựa trên A và/hoặc thông tin khác.

Cần hiểu rằng thuật ngữ "bao gồm" (còn được đề cập tới như là "bao gồm", "bao gồm", "bao gồm", và/hoặc "bao gồm"), khi được sử dụng trong bản mô tả này, định rõ sự xuất hiện của các dấu hiệu được thể hiện, các số nguyên, các bước, các thao tác, các phần tử, và/hoặc các thành phần, nhưng không loại trừ sự xuất hiện hoặc bổ sung của một hoặc nhiều dấu hiệu, số nguyên, các bước, các thao tác, các phần tử, các thành phần khác, và/hoặc các nhóm của chúng.

Cần hiểu rằng thuật ngữ "nếu" có thể được hiểu theo nghĩa là "khi" ("khi" hoặc "vào lúc"), "đáp lại việc xác định", hoặc "đáp lại việc phát hiện". Tương tự, theo ngữ cảnh này, cụm từ "nếu được xác định rằng" hoặc "nếu (điều kiện hoặc sự kiện được trình bày) được phát hiện" có thể được hiểu theo nghĩa là "khi được xác định rằng", "đáp lại việc xác định", "khi (điều kiện hoặc sự kiện được trình bày) được phát hiện", hoặc "đáp lại việc phát hiện (điều kiện hoặc sự kiện được trình bày)".

Sẽ được hiểu rằng "một phương án", "phương án", hoặc "cách thức thực hiện khả thi" được đề cập xuyên suốt bản mô tả có nghĩa rằng các dấu hiệu, các cấu trúc, hoặc các đặc tính riêng biệt liên quan đến các phương án hoặc các cách thức thực hiện được chứa trong ít nhất một phương án của sáng chế. Do đó, "theo một phương án", "theo phương án", hoặc "theo cách thức thực hiện khả thi" xuất hiện xuyên suốt bản mô tả này không nhất thiết là đề cập đến cùng phương án. Ngoài ra, các dấu hiệu, các cấu trúc, hoặc các đặc tính riêng biệt này có thể được kết hợp trong một hoặc nhiều phương án theo cách thích hợp bất kỳ.

Sẽ được hiểu rằng thông tin định tuyến BGP bao gồm thông tin đường truyền của đường truyền AS (mà được đề cập ngắn gọn là thông tin đường truyền AS dưới đây), và một đoạn thông tin đường truyền AS có thể bao gồm các số AS (AS number, ASN) được sắp xếp theo thứ tự thiết lập trước thứ nhất (tương ứng với thứ tự thiết lập trước trong các phương án của sáng chế). Mỗi số AS trong thông tin đường truyền AS nhận diện duy nhất một AS. Theo cách này,

thứ tự thiết lập trước thứ nhất được sử dụng để chỉ báo thứ tự của các AS mà được nhận diện bởi các số AS và được đi qua trong đường truyền AS được chỉ báo bởi thông tin đường truyền AS.

Trong số các số AS được sắp xếp theo thứ tự thiết lập trước thứ nhất, hai số AS liền kề là một cặp AS (AS pair). Cụ thể, thông tin đường truyền AS bao gồm các cặp AS, và các cặp AS cũng được sắp xếp theo thứ tự thiết lập trước thứ nhất.

Theo một ví dụ, thông tin đường truyền của đường truyền AS 1 bao gồm (ASN 3, ASN 2, và ASN 1). Trong trường hợp này, trong đường truyền AS 1, AS bắt đầu có thể là AS được nhận diện bởi ASN 1, và AS kết thúc có thể là AS được nhận diện bởi ASN 3. Cụ thể, thứ tự sắp xếp của ASN 1, ASN 2, và ASN 3 chỉ báo rằng trong đường truyền AS 1, AS được nhận diện bởi ASN 1, AS được nhận diện bởi ASN 2, và AS được nhận diện bởi ASN 3 được đi qua theo trình tự. Thông tin đường truyền của đường truyền AS 1 bao gồm hai cặp AS: ASN 1:ASN 2 và ASN 2:ASN 3.

Cặp AS bất kỳ trong thông tin đường truyền AS có thể là các số trình tự của cặp AS lân cận có quan hệ kinh doanh lân cận AS thiết lập trước. Quan hệ kinh doanh lân cận AS thiết lập trước có thể là bất kỳ một trong số quan hệ quan hệ C2P, P2C, quan hệ P2P, hoặc quan hệ S2S được mô tả ở trên.

Để làm ngắn gọn phần mô tả, trong các ngữ cảnh của các phương án của sáng chế sau đây, cặp AS có quan hệ C2P được gọi là cặp C2P AS, cặp AS có quan hệ P2C được gọi là cặp P2C AS, cặp AS có quan hệ P2P được gọi là cặp P2P AS, và cặp AS có quan hệ S2S được gọi là cặp S2S AS.

Đối với cặp AS bất kỳ có quan hệ C2P hoặc quan hệ P2C, thứ tự của AS lân cận của cặp AS tương ứng với quan hệ kinh doanh giữa cặp AS.

Theo một ví dụ, đối với cặp AS 1, nghĩa là, ASN 1:ASN 2, nếu cặp AS 1 là cặp C2P AS, AS được nhận diện bởi ASN 1 là AS khách hàng, và AS được nhận diện bởi ASN 2 là AS nhà cung cấp. Nếu cặp AS 1 là cặp P2C AS, AS được nhận diện bởi ASN 1 là AS nhà cung cấp, và AS được nhận diện bởi ASN

2 là AS khách hàng.

Hiện tại, nguyên tắc thung lũng tự do thường được sử dụng để phát hiện liệu sự rò rỉ tuyến có xảy ra trên thông tin đường truyền AS trong đoạn thông tin định tuyến BGP, để tránh tác động gây ra bởi sự rò rỉ tuyến BGP.

Nguyên tắc thung lũng tự do là việc, đối với thông tin đường truyền AS trong thông tin định tuyến BGP bất kỳ, thông tin đường truyền AS có thể bao gồm chỉ ít nhất một trong số m cặp C2P AS, 0 hoặc 1 cặp P2P AS, hoặc n cặp P2C AS mà được sắp xếp nghiêm ngặt theo thứ tự thiết lập trước thứ hai, trong đó m và n là các số nguyên lớn hơn hoặc bằng 0.

Thứ tự thiết lập trước thứ hai bao gồm thứ tự sau đây: cặp C2P AS có thể được theo sau bởi ít nhất một trong số 0 hoặc nhiều cặp C2P AS, cặp P2P AS, hoặc 0 hoặc nhiều cặp P2C AS; cặp P2P AS được theo sau bởi chỉ 0 hoặc nhiều cặp P2C AS; và cặp P2C AS được theo sau bởi chỉ 0 hoặc nhiều cặp P2C AS.

Cụ thể, nếu đường truyền được chỉ báo bởi thông tin đường truyền AS mà bao gồm chỉ cặp C2P AS được gọi là đường truyền đường lên (upstream path), và đường truyền được chỉ báo bởi thông tin đường truyền AS mà bao gồm chỉ cặp P2C AS được gọi là đường truyền đường xuống (downstream path), theo nguyên tắc thung lũng tự do, các đỉnh sóng hoặc các thung lũng sóng được tạo ra bởi các đường truyền đường lên và các đường truyền đường xuống có thể không xảy ra theo cách lặp lại trong đường truyền AS mà bao gồm cả các đường truyền đường lên và các đường truyền đường xuống. Điều này thỏa mãn nguyên tắc tối đa hóa lợi nhuận.

Trong trường hợp này, khi thứ tự sắp xếp của các cặp AS trong thông tin đường truyền AS thỏa mãn nguyên tắc thung lũng tự do, có thể được xem là không có sự rò rỉ tuyến xảy ra trên thông tin đường truyền AS, nói cách khác, đường truyền AS được chỉ báo bởi thông tin đường truyền AS là có hiệu lực. Khi thứ tự sắp xếp của các cặp AS trong thông tin đường truyền AS không thỏa mãn nguyên tắc thung lũng tự do, có thể được xem là sự rò rỉ tuyến xảy ra trên thông tin đường truyền AS, nói cách khác, đường truyền AS được chỉ báo bởi

thông tin đường truyền AS là không có hiệu lực.

Ví dụ, FIG.1 là sơ đồ giản lược của đường truyền AS có hiệu lực.

Như được thể hiện trong FIG.1, thông tin đường truyền của đường truyền AS 1 được thể hiện trong FIG.1 bao gồm (ASN 5, ASN 4, ASN 3, ASN 2, và ASN 1).

Trong đường truyền AS 1, AS bắt đầu là AS được nhận diện bởi ASN 1, và AS kết thúc là AS được nhận diện bởi ASN 5. Thông tin đường truyền của đường truyền AS 1 bao gồm bốn cặp AS: ASN 1:ASN 2, ASN 2:ASN 3, ASN 3:ASN 4, và ASN 4:ASN 5. Cả ASN 1:ASN 2 và ASN 2:ASN 3 là cặp C2P AS, và cả ASN 3:ASN 4 và ASN 4:ASN 5 là cặp P2C AS.

Có thể hiểu được rằng, trong ASN 1:ASN 2, AS được nhận diện bởi ASN 2 là AS đóng vai trò như nhà cung cấp, và trong ASN 2:ASN 3, AS được nhận diện bởi ASN 2 là AS đóng vai trò như khách hàng. Tương tự, trong ASN 3:ASN 4, AS được nhận diện bởi ASN 4 là AS đóng vai trò như khách hàng, và trong ASN 4:ASN 5, AS được nhận diện bởi ASN 4 là AS đóng vai trò như nhà cung cấp.

Có thể hiểu được rằng, trong thông tin đường truyền của đường truyền AS 1, ASN 1:ASN 2 có quan hệ C2P được theo sau bởi ASN 2:ASN 3 có quan hệ C2P, và mỗi ASN 3:ASN 4 và ASN 4:ASN 5 có quan hệ P2C. ASN 2:ASN 3 có quan hệ C2P được theo sau bởi chỉ ASN 3:ASN 4 và mỗi ASN 4:ASN 5 có quan hệ P2C. ASN 3:ASN 4 có quan hệ P2C được theo sau bởi chỉ ASN 4:ASN 5 có quan hệ P2C.

Do đó, thứ tự sắp xếp của các cặp AS trong thông tin đường truyền của đường truyền AS 1 thỏa mãn nguyên tắc thung lũng tự do, nói cách khác, đường truyền AS 1 là có hiệu lực.

Thông tin đường truyền của đường truyền AS 2 được thể hiện trong FIG.1 bao gồm (ASN 8, ASN 7, ASN 6, ASN 3, ASN 2, và ASN 1).

Trong đường truyền AS 2, AS bắt đầu là AS được nhận diện bởi ASN 1,

và AS kết thúc là AS được nhận diện bởi ASN 8. Thông tin đường truyền của đường truyền AS 2 bao gồm năm cặp AS: ASN 1:ASN 2, ASN 2:ASN 3, ASN 3:ASN 6, ASN 6:ASN 7, và ASN 7:ASN 8. Cả ASN 1:ASN 2 và ASN 2:ASN 3 là cặp C2P AS, ASN 3:ASN 6 là cặp P2P AS, và cả ASN 6:ASN 7 và ASN 7:ASN 8 là cặp P2C AS.

Có thể hiểu được rằng, trong thông tin đường truyền của đường truyền AS 2, ASN 1:ASN 2 có quan hệ C2P được theo sau bởi ASN 2:ASN 3 có quan hệ C2P, ASN 3:ASN 6 có quan hệ P2P, và mỗi ASN 6:ASN 7 và ASN 7:ASN 8 có quan hệ P2C. ASN 2:ASN 3 có quan hệ C2P được theo sau bởi ASN 3:ASN 6 có quan hệ P2P, và mỗi ASN 6:ASN 7 và ASN 7:ASN 8 có quan hệ P2C. ASN 3:ASN 6 có quan hệ P2P được theo sau bởi chỉ ASN 6:ASN 7 và mỗi ASN 7:ASN 8 có quan hệ P2C. ASN 6:ASN 7 có quan hệ P2C được theo sau bởi chỉ ASN 7:ASN 8 có quan hệ P2C.

Do đó, thứ tự sắp xếp của các cặp AS trong thông tin đường truyền của đường truyền AS 2 thỏa mãn nguyên tắc thung lũng tự do, nói cách khác, đường truyền AS 2 cũng là có hiệu lực.

FIG.2(a) và FIG.2(b) là các sơ đồ giản lược của các đường truyền AS không có hiệu lực.

Như được thể hiện trong FIG.2(a), thông tin đường truyền của đường truyền AS 1 bao gồm (ASN 9, ASN 5, ASN 4, ASN 3, ASN 2, và ASN 1).

Trong đường truyền AS 1, AS bắt đầu là AS được nhận diện bởi ASN 1, và AS kết thúc là AS được nhận diện bởi ASN 9. Thông tin đường truyền của đường truyền AS 1 bao gồm năm cặp AS: ASN 1:ASN 2, ASN 2:ASN 3, ASN 3:ASN 4, ASN 4:ASN 5, và ASN 5:ASN 9. Tất cả trong số ASN 1:ASN 2, ASN 2:ASN 3, và ASN 5:ASN 9 có thể là cặp C2P AS, và cả ASN 3:ASN 4 và ASN 4:ASN 5 có thể là cặp P2C AS.

Có thể hiểu được rằng, trong thông tin đường truyền của đường truyền AS 1, ASN 4:ASN 5 có quan hệ P2C được theo sau bởi ASN 5:ASN 9 có quan hệ C2P. Có thể hiểu được rằng thứ tự sắp xếp của cặp AS ASN 4:ASN 5 và cặp

AS ASN 5:ASN 9 trong thông tin đường truyền của đường truyền AS 1 không thỏa mãn nguyên tắc thung lũng tự do, nói cách khác, đường truyền AS 1 là không có hiệu lực.

Thông tin đường truyền của đường truyền AS 2 được thể hiện trong FIG.2(b) bao gồm (ASN 10, ASN 8, ASN 7, ASN 6, ASN 3, ASN 2, và ASN 1).

Trong đường truyền AS 2, AS bắt đầu là AS được nhận diện bởi ASN 1, và AS kết thúc là AS được nhận diện bởi ASN 10. Thông tin đường truyền của đường truyền AS 2 bao gồm sáu cặp AS: ASN 1:ASN 2, ASN 2:ASN 3, ASN 3:ASN 6, ASN 6:ASN 7, ASN 7:ASN 8, và ASN 8:ASN 10. Tất cả trong số ASN 1:ASN 2, ASN 2:ASN 3, và ASN 8:ASN 10 là cặp C2P AS, ASN 3:ASN 6 là cặp P2P AS, và cả ASN 6:ASN 7 và ASN 7:ASN 8 là cặp P2C AS.

Có thể hiểu được rằng, trong thông tin đường truyền của đường truyền AS 2, ASN 7:ASN 8 có quan hệ P2C được theo sau bởi ASN 8:ASN 10 có quan hệ C2P. Có thể hiểu được rằng thứ tự sắp xếp của cặp AS ASN 7:ASN 8 và cặp AS ASN 8:ASN 10 trong thông tin đường truyền của đường truyền AS 2 không thỏa mãn nguyên tắc thung lũng tự do, nói cách khác, đường truyền AS 2 cũng là không có hiệu lực.

Tuy nhiên, khi hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền AS trong thông tin định tuyến BGP được kiểm tra theo nguyên tắc thung lũng tự do, quan hệ kinh doanh giữa cặp AS trong thông tin đường truyền AS thường được xác định không chính xác. Do đó, lỗi xảy ra trong quá trình kiểm tra hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền AS.

Thông thường, quan hệ kinh doanh giữa cặp AS trong thông tin đường truyền AS được xác định không chính xác do cùng cặp AS có thể có các quan hệ kinh doanh khác nhau trong các vùng khác nhau.

Theo một ví dụ, trong vùng A, cặp AS 1 là cặp AS có quan hệ C2P. Tuy nhiên, trong vùng B, cặp AS 1 là cặp AS có quan hệ P2C.

Trong vùng B, khi hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền AS bao gồm cặp AS 1 được kiểm tra theo nguyên tắc thung lũng tự do nêu trên, quan hệ kinh doanh giữa cặp AS 1 trong vùng A có thể được xem là quan hệ kinh doanh giữa cặp AS 1 trong vùng B, để xác định liệu đường truyền AS được chỉ báo bởi thông tin đường truyền AS là có hiệu lực. Trong trường hợp này, trong vùng B, mặc dù đường truyền AS thực tế là đường truyền AS có hiệu lực, đường truyền AS được xác định là không có hiệu lực; hoặc mặc dù đường truyền AS thực tế là đường truyền AS không có hiệu lực, đường truyền AS được xác định là có hiệu lực.

Xét về vấn đề này, phương án của sáng chế đề xuất phương pháp kiểm tra cặp AS. Theo phương pháp này, ký hiệu nhận dạng vùng của vùng mà mỗi cặp AS thuộc về được bổ sung vào cơ sở dữ liệu đầu vào cấp quyền được sử dụng để kiểm tra cặp AS. Điều này có thể tránh được trường hợp trong đó hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền trong thông tin định tuyến BGP được xác định không chính xác do quan hệ kinh doanh giữa cặp AS trong thông tin đường truyền được xác định không chính xác khi hiệu lực của đường truyền AS được kiểm tra theo nguyên tắc thung lũng tự do.

Do đó, phương pháp kiểm tra cặp AS được đề xuất trong phương án này của sáng chế cải thiện độ chính xác kiểm tra hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền bao gồm cặp AS.

Phương án của sáng chế còn đề xuất thiết bị kiểm tra cặp AS (mà được đề cập ngắn gọn là thiết bị kiểm tra dưới đây). Thiết bị kiểm tra có thể là thiết bị mạng bất kỳ mà cần kiểm tra cặp AS.

Ví dụ, thiết bị mạng có thể là thiết bị phân tích mạng, thiết bị điều khiển mạng, thiết bị cổng, hoặc thiết bị định tuyến. Điều này không bị giới hạn ở đây.

FIG.3 là sơ đồ giản lược của cấu trúc phần cứng của thiết bị mạng 30 theo phương án của sáng chế.

Như được thể hiện trong FIG.3, thiết bị mạng 30 bao gồm bộ xử lý 31,

bộ nhớ 32, giao diện truyền thông 33, và kênh truyền 34. Bộ xử lý 31, bộ nhớ 32, và giao diện truyền thông 33 có thể được kết nối với nhau thông qua kênh truyền 34.

Bộ xử lý 31 là trung tâm điều khiển của thiết bị mạng 30, và có thể là bộ xử lý trung tâm mục đích chung (central processing unit, CPU), hoặc có thể là bộ xử lý mục đích chung khác hoặc tương tự. Bộ xử lý mục đích chung có thể là bộ vi xử lý, bộ xử lý thông thường bất kỳ, hoặc tương tự.

Theo một ví dụ, bộ xử lý 31 có thể bao gồm một hoặc nhiều CPU, ví dụ, CPU 0 và CPU 1 mà được thể hiện trong FIG.3.

Bộ nhớ 32 có thể là bộ nhớ chỉ đọc (read-only memory, ROM) hoặc loại thiết bị lưu trữ tĩnh khác có khả năng lưu trữ thông tin tĩnh và các lệnh, hoặc bộ nhớ truy nhập ngẫu nhiên (random access memory, RAM) hoặc loại thiết bị lưu trữ động khác có khả năng lưu trữ thông tin và các lệnh; có thể là bộ nhớ chỉ đọc có thể lập trình có thể xóa bằng điện (electrically erasable programmable read-only memory, EEPROM), phương tiện lưu trữ đĩa từ hoặc thiết bị lưu trữ từ khác, hoặc phương tiện khác bất kỳ có khả năng mang hoặc lưu trữ mã chương trình mong muốn ở dạng lệnh hoặc cấu trúc dữ liệu và có thể được truy nhập bởi máy tính. Tuy nhiên, điều này không bị giới hạn ở đây.

Theo cách thức thực hiện khả thi, bộ nhớ 32 có thể là độc lập với bộ xử lý 31. Bộ nhớ 32 có thể được kết nối với bộ xử lý 31 thông qua kênh truyền 34, và được cấu hình để lưu trữ dữ liệu, các lệnh, hoặc mã chương trình. Khi gọi ra và thực thi các lệnh hoặc mã chương trình được lưu trữ trong bộ nhớ 32, bộ xử lý 31 có thể thực hiện phương pháp kiểm tra cặp AS được đề xuất trong các phương án của sáng chế.

Theo cách thức thực hiện khả thi khác, bộ nhớ 32 có thể còn được tích hợp với bộ xử lý 31.

Giao diện truyền thông 33 được cấu hình để kết nối thiết bị mạng 30 với thiết bị khác (như máy chủ) bằng cách sử dụng mạng truyền thông. Mạng truyền thông có thể là Ethernet, mạng truy nhập vô tuyến (radio access network,

RAN), mạng vùng cục bộ không dây (wireless local area network, WLAN), hoặc tương tự. Giao diện truyền thông 33 có thể bao gồm bộ thu được cấu hình để thu dữ liệu và bộ gửi được cấu hình để gửi dữ liệu.

Kênh truyền 34 có thể là kênh truyền kiến trúc tiêu chuẩn công nghiệp (Industry Standard Architecture, ISA), kênh truyền liên kết thành phần ngoại vi (Peripheral Component Interconnect, PCI), kênh truyền kiến trúc tiêu chuẩn công nghiệp mở rộng (Extended Industry Standard Architecture, EISA), hoặc tương tự. Kênh truyền có thể được phân loại thành kênh truyền địa chỉ, kênh truyền dữ liệu, kênh truyền điều khiển, và loại tương tự. Để dễ dàng biểu diễn, chỉ một đường nét đậm được sử dụng để thể hiện kênh truyền trên FIG.3, nhưng điều này không có nghĩa là chỉ có một kênh truyền hoặc chỉ có một loại kênh truyền.

Lưu ý rằng cấu trúc được thể hiện trong FIG.3 không tạo thành giới hạn lên thiết bị mạng. Ngoài các thành phần được thể hiện trong FIG.3, thiết bị mạng 30 có thể bao gồm nhiều hơn hoặc ít thành phần hơn so với các thành phần được thể hiện trong hình vẽ, kết hợp một số thành phần, hoặc có các cách sắp xếp thành phần khác nhau.

Phương án của sáng chế còn đề xuất hệ thống kiểm tra cặp AS (mà được đề cập ngắn gọn là hệ thống kiểm tra dưới đây). Hệ thống kiểm tra là hệ thống kiểm tra dựa trên cơ chế RPKI.

Cụ thể, FIG.4 là sơ đồ giản lược của kiến trúc của hệ thống kiểm tra 40 theo phương án của sáng chế.

Như được thể hiện trong FIG.4, hệ thống kiểm tra 40 bao gồm AS 41 và AS 42. BGP bên ngoài (external/exterior BGP, EBGP) có thể chạy giữa AS 41 và AS 42 bằng cách sử dụng thiết bị mạng 411 và thiết bị mạng 421, để trao đổi thông tin định tuyến BGP. Thiết bị mạng 411 có thể là thiết bị cổng trong AS 41, và thiết bị mạng 421 có thể là thiết bị cổng trong AS 42. Sẽ được hiểu rằng thiết bị kiểm tra có thể được áp dụng với thiết bị mạng.

Thiết bị mạng 411 được kết nối với máy chủ RPKI 43 để truyền thông.

Máy chủ RPKI 43 truyền thông với neo tin cậy 44, và có thể thu nhận thông tin cấp quyền nhà cung cấp hệ thống tự trị (autonomous system provider authorization, ASPA) từ neo tin cậy 44.

Sau đó, máy chủ RPKI 43 xử lý thông tin ASPA để thu nhận thông tin cấp quyền ASPA dạng văn bản. Máy chủ RPKI 43 có thể là máy chủ RPKI được sử dụng riêng bởi AS 41, hoặc có thể là máy chủ RPKI được chia sẻ bởi các AS bao gồm AS 41 (ví dụ, còn bao gồm AS 42). Điều này không bị giới hạn ở đây.

Theo cách này, thiết bị mạng 411 có thể thu nhận thông tin cấp quyền ASPA từ máy chủ RPKI 43, để tạo ra cơ sở dữ liệu đầu vào cấp quyền. Trong trường hợp này, sau khi thu thông tin định tuyến BGP được gửi bởi thiết bị mạng 421, thiết bị mạng 411 có thể kiểm tra cặp AS trong thông tin đường truyền AS trong thông tin định tuyến BGP dựa trên cơ sở dữ liệu đầu vào cấp quyền, để kiểm tra hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền AS.

Phần sau đây mô tả phương pháp kiểm tra cặp AS được đề xuất trong các phương án của sáng chế viện dẫn tới các hình vẽ kèm theo.

FIG.5 là lưu đồ giản lược của phương pháp kiểm tra cặp AS theo phương án của sáng chế. Phương pháp có thể được áp dụng với thiết bị mạng trong hệ thống kiểm tra 40 được thể hiện trong FIG.4. Phương pháp này có thể bao gồm các bước sau đây.

S101: thiết bị mạng thu nhận thông tin đường truyền.

Thông tin đường truyền là thông tin đường truyền AS nêu trên. Cụ thể, thông tin đường truyền chỉ báo một đường truyền AS, và đường truyền AS là đường truyền tương ứng với thông tin đường truyền.

Nghĩa là, thông tin đường truyền bao gồm ít nhất một cặp AS, và cặp AS bất kỳ trong ít nhất một cặp AS là hai số AS liền kề trong thông tin đường truyền. Đối với phần mô tả liên quan của cặp AS, tham khảo phần mô tả nêu trên. Chi tiết không được mô tả lại ở đây.

Một cách tùy chọn, thiết bị mạng có thể thu nhận thông tin đường truyền bằng cách thu nhận bản tin cập nhật BGP. Bản tin cập nhật BGP bao gồm thông tin đường truyền.

Theo cách thức thực hiện khả thi, sau khi tạo bản tin cập nhật BGP và trước khi gửi bản tin cập nhật BGP đến thiết bị lân cận, thiết bị mạng có thể kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền.

Theo một ví dụ, viện dẫn tới FIG.4, nếu thiết bị mạng là thiết bị mạng 411 đóng vai trò làm thiết bị cổng trong AS 41, sau khi tạo bản tin cập nhật BGP và trước khi gửi bản tin cập nhật BGP đến thiết bị mạng 421 đóng vai trò làm thiết bị cổng trong AS lân cận 42 của AS 41, thiết bị mạng 411 có thể kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền.

Theo cách thức thực hiện khả thi khác, sau khi thu bản tin cập nhật BGP được gửi bởi thiết bị lân cận, thiết bị mạng có thể kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền.

Theo một ví dụ, viện dẫn tới FIG.4, nếu thiết bị mạng là thiết bị mạng 411 đóng vai trò làm thiết bị cổng trong AS 41, sau khi thu bản tin cập nhật BGP được gửi bởi thiết bị mạng 421 đóng vai trò làm thiết bị cổng trong AS lân cận 42 của AS 41, thiết bị mạng 411 có thể kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền.

Đối với phần mô tả của việc kiểm tra cặp AS để kiểm tra hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền bao gồm cặp AS, tham khảo phần mô tả trong bước S104 dưới đây. Các chi tiết không được mô tả ở đây.

S102: thiết bị mạng xác định thông tin vùng của vùng mà cặp AS trong thông tin đường truyền thuộc về.

Để làm ngắn gọn phần mô tả, việc thiết bị mạng xác định thông tin vùng của vùng mà cặp AS thứ nhất thuộc về được sử dụng như là ví dụ để mô tả dưới đây. Cặp AS thứ nhất là cặp AS bất kỳ trong ít nhất một cặp AS trong thông tin đường truyền thu được ở bước S101.

Theo cách thức thực hiện khả thi, thông tin định tuyến bao gồm thông tin đường truyền bao gồm thông tin vùng của vùng mà cặp AS thứ nhất thuộc về. Trong trường hợp này, thiết bị mạng có thể xác định, từ thông tin định tuyến bao gồm thông tin đường truyền, thông tin vùng của vùng mà cặp AS thứ nhất thuộc về.

Một cách tùy chọn, đối với thiết bị mạng 1 mà thu thông tin định tuyến (ví dụ, thông tin định tuyến BGP), thiết bị mạng 1 có thể bổ sung thông tin vị trí địa lý của thiết bị mạng 1 vào thông tin thuộc tính đường truyền trong thông tin định tuyến BGP. Sau đó thiết bị mạng 1 có thể gửi, đến thiết bị lân cận, thông tin định tuyến BGP mà thông tin vị trí địa lý của thiết bị mạng 1 được bổ sung.

Nếu thiết bị lân cận là thiết bị mạng trong AS lân cận với AS mà trong đó thiết bị mạng 1 được đặt, thiết bị mạng 1 còn bổ sung số AS (ví dụ, ASN 1) của AS mà trong đó thiết bị mạng 1 được đặt vào thông tin đường truyền trong thông tin định tuyến BGP.

Trong trường hợp này, nếu thiết bị lân cận là thiết bị mạng được mô tả trong phương án này của sáng chế, sau khi thiết bị mạng được mô tả trong phương án này của sáng chế thu thông tin định tuyến BGP mà thiết bị mạng 1 bổ sung vào thông tin vị trí địa lý của thiết bị mạng 1, thiết bị mạng có thể xác định, dựa trên thông tin vị trí địa lý được bổ sung bởi thiết bị mạng 1, thông tin vùng mà là của vùng mà cặp AS thứ nhất thuộc về và được chứa trong thông tin định tuyến BGP bao gồm ASN 1.

Ví dụ, thiết bị mạng 1 có thể bổ sung thông tin vị trí địa lý vào thông tin định tuyến BGP 1 thu được, trong đó thông tin vị trí địa lý cụ thể là như sau:

- đường truyền AS:3356 4809 9392

- 286:4990 (Châu Âu)

"286" là số AS của AS (ví dụ, AS 1) mà trong đó thiết bị mạng 1 được đặt. Thông tin vị trí địa lý của thiết bị mạng 1 mà được bổ sung bởi thiết bị mạng 1 vào thông tin thuộc tính đường truyền trong thông tin định tuyến BGP 1 có thể là "4990 (Châu Âu)", để đánh dấu vị trí địa lý của thiết bị mạng 1 là "Châu Âu", trong đó "4990" là số nhận dạng cho "Châu Âu".

Nếu AS lân cận của AS mà trong đó thiết bị mạng được đặt là AS 2, khi thiết bị mạng 1 cần gửi thông tin định tuyến BGP 1 thu được đến thiết bị mạng 2 trong AS 2, thiết bị mạng 1 còn cần bổ sung số AS "286" của AS 1 vào thông tin đường truyền trong thông tin định tuyến BGP 1. Nghĩa là, đường truyền AS được thay đổi thành "đường truyền AS: 286 3356 4809 9392".

Trong trường hợp này, khi thiết bị mạng được mô tả trong phương án này của sáng chế là thiết bị mạng 2, sau khi thiết bị mạng được mô tả trong phương án này của sáng chế thu thông tin định tuyến BGP 1 được gửi bởi thiết bị mạng 1, thông tin vùng của vùng mà cặp AS thứ nhất (nghĩa là, cặp AS 3356:286) bao gồm số AS 286 thuộc về trong thông tin định tuyến BGP 1 là thông tin vị trí địa lý "4990 (Châu Âu)" được bổ sung bởi thiết bị mạng 1 vào thông tin định tuyến BGP 1, nói cách khác, thông tin vùng của vùng mà cặp AS 3356:286 thuộc về là "Châu Âu", trong đó 3356 là số AS của AS lân cận khác (ví dụ, AS 3) của AS mà trong đó thiết bị mạng 1 được đặt.

Theo cách thức thực hiện khả thi khác, thông tin định tuyến bao gồm thông tin đường truyền bao gồm tiền tố. Tiền tố thường bao gồm đoạn địa chỉ IP và mặt nạ. Điều này không bị giới hạn ở đây. Theo cách này, thiết bị mạng có thể phát hiện, dựa trên địa chỉ IP bất kỳ được chứa trong tiền tố, vị trí địa lý đi qua trước khi địa chỉ IP đạt đến, để xác định thông tin vùng của vùng mà cặp AS trong thông tin đường truyền thuộc về.

Theo một ví dụ, thông tin đường truyền 1 cụ thể là như sau:

"as_path": "4809 58879 132813"

"prefix": "45.195.52.0/22"

Thông tin đường truyền 1 là (4809, 58879, 132813), và tiền tố trong thông tin đường truyền 1 là 45.195.52.0/22. Trong trường hợp này, thiết bị mạng có thể thực hiện phát hiện truy vết dựa trên địa chỉ IP (ví dụ, 45.195.52.1) được chứa trong tiền tố, và thu nhận kết quả truy vết được trả lại.

Ví dụ, kết quả truy vết chỉ báo rằng các nút mạng sau đây được đi qua trước khi 45.195.52.1 tới: một hoặc nhiều nút mạng trong AS có số AS 4809 trong vùng 1, một hoặc nhiều nút mạng trong AS có số AS 58879 trong vùng 1 và vùng 2, và một hoặc nhiều nút mạng trong AS có số AS 132813 trong vùng 2.

Trong trường hợp này, thiết bị mạng có thể xác định rằng thông tin vùng của vùng mà cặp AS 132813:58879 trong thông tin đường truyền thuộc về là vùng 2, và thông tin vùng của vùng mà cặp AS 58879:4809 trong thông tin đường truyền thuộc về là vùng 1.

Chắc chắn là, các cách thức thực hiện khả thi nêu trên để xác định thông tin vùng của vùng mà cặp AS thứ nhất thuộc về chỉ được sử dụng làm các ví dụ cho phần mô tả. Cách thức thực hiện cụ thể để xác định thông tin vùng của vùng mà cặp AS thứ nhất thuộc về không bị giới hạn trong phương án này của sáng chế.

S103: Thiết bị mạng kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về.

Để làm ngắn gọn phần mô tả, việc thiết bị mạng kiểm tra cặp AS thứ nhất dựa trên thông tin vùng được xác định của vùng mà cặp AS thứ nhất thuộc về được sử dụng như là ví dụ để mô tả.

Cụ thể, thiết bị mạng kiểm tra cặp AS thứ nhất dựa trên thông tin vùng được xác định của vùng mà cặp AS thứ nhất thuộc về (trong phương án này của sáng chế, "thông tin vùng của vùng mà cặp AS thứ nhất thuộc về" được đề cập ngắn gọn là "thông tin vùng thứ nhất" dưới đây) và cơ sở dữ liệu đầu vào cấp quyền.

Cơ sở dữ liệu đầu vào cấp quyền có thể được thiết lập trước bởi thiết bị mạng, hoặc có thể thu được bởi thiết bị mạng từ máy chủ trước khi thiết bị mạng kiểm tra cặp AS trong thông tin đường truyền. Điều này không bị giới hạn ở đây.

Cơ sở dữ liệu đầu vào cấp quyền bao gồm ít nhất một đầu vào cấp quyền.

Đối với đầu vào cấp quyền thứ nhất trong ít nhất một đầu vào cấp quyền, đầu vào cấp quyền thứ nhất bao gồm ít nhất một cặp AS có quan hệ kinh doanh được thiết lập trước. Quan hệ kinh doanh được thiết lập trước có thể là bất kỳ một trong số quan hệ C2P, quan hệ P2C, quan hệ P2P, hoặc quan hệ S2S nêu trên.

Để dễ dàng mô tả, quan hệ kinh doanh được thiết lập trước là quan hệ C2P được sử dụng như là ví dụ để mô tả dưới đây trong phương án này của sáng chế. Trong trường hợp này, đầu vào cấp quyền thứ nhất bao gồm ít nhất một cặp C2P AS. Nói cách khác, tất cả các cặp AS trong cơ sở dữ liệu đầu vào cấp quyền là cặp C2P AS.

Sẽ được hiểu rằng đối với ít nhất một cặp C2P AS trong đầu vào cấp quyền thứ nhất, ít nhất một cặp C2P AS bao gồm cùng số AS khách hàng (ví dụ, ASN 1 của AS 1). Cụ thể, các AS được chỉ báo bởi số AS khách hàng bao gồm ít nhất một AS nhà cung cấp.

Ví dụ, như được thể hiện trong bảng 1, một dòng được thể hiện trong Bảng 1 thể hiện một đầu vào cấp quyền.

Đầu vào cấp quyền 1 có thể bao gồm cặp AS (nghĩa là, ASN 1:ASN 2) bao gồm số AS (nghĩa là, ASN 1) của AS khách hàng 1 và số AS (nghĩa là, ASN 2) của AS nhà cung cấp 2.

Đầu vào cấp quyền 2 có thể bao gồm cặp AS (nghĩa là, ASN 3:ASN 4) bao gồm số AS (nghĩa là, ASN 3) của AS khách hàng 3 và số AS (ASN 4) của AS nhà cung cấp 4, và cặp AS (nghĩa là, ASN 3:ASN 5) bao gồm số AS (nghĩa là, ASN 3) của AS khách hàng 3 và số AS (ASN 5) của AS nhà cung cấp 5.

Có thể hiểu được rằng AS khách hàng 3 có hai AS nhà cung cấp (nghĩa là, AS nhà cung cấp 4 và AS nhà cung cấp 5).

Chi tiết được thể hiện trong bảng 1:

Bảng 1

ASN khách hàng	ASN nhà cung cấp
ASN 1	ASN 2
ASN 3	ASN 4, ASN 5

Lưu ý rằng đầu vào cấp quyền thứ nhất còn bao gồm ký hiệu nhận dạng vùng của vùng mà ít nhất một cặp C2P AS thuộc về.

Vùng mà ít nhất một cặp C2P AS thuộc về là vùng địa lý mà trong đó ít nhất một cặp C2P AS được đặt. Ký hiệu nhận dạng vùng nhận diện duy nhất vùng địa lý mà trong đó ít nhất một cặp C2P AS được đặt.

Trong ví dụ thứ hai, viện dẫn tới bảng 1, như được thể hiện trong bảng 2, bảng 2 thể hiện giản lược đầu vào cấp quyền 1 và đầu vào cấp quyền 2 mỗi đầu vào bao gồm ký hiệu nhận dạng vùng của vùng mà cặp AS thuộc về.

Vùng mà một cặp C2P AS được chứa trong đầu vào cấp quyền 1 thuộc về có ký hiệu nhận dạng vùng 1, và vùng mà hai cặp C2P AS được chứa trong đầu vào cấp quyền 2 thuộc về có ký hiệu nhận dạng vùng 2.

Chi tiết được thể hiện trong bảng 2:

Bảng 2

ASN khách hàng	ASN nhà cung cấp	Ký hiệu nhận dạng vùng (Region Identifier)
ASN 1	ASN 2	Ký hiệu nhận dạng vùng 1
ASN 3	ASN 4, ASN 5	Ký hiệu nhận dạng vùng 2

Có thể hiểu rằng các quan hệ kinh doanh giữa cùng cặp AS trong các vùng khác nhau có thể tất cả là quan hệ C2P. Do đó, cơ sở dữ liệu đầu vào cấp quyền có thể bao gồm các đầu vào cấp quyền mà bao gồm cùng cặp AS và các ký hiệu nhận dạng vùng khác nhau.

Trong ví dụ thứ ba, nếu cặp AS (ASN 1:ASN 2) được thể hiện trong Bảng 2 nằm trong vùng có ký hiệu nhận dạng vùng 3, và cũng có quan hệ C2P, cơ sở dữ liệu đầu vào cấp quyền còn bao gồm một đầu vào cấp quyền mà bao gồm cặp AS (ASN 1:ASN 2) và ký hiệu nhận dạng vùng 3.

Chi tiết được thể hiện trong bảng 3:

Bảng 3

ASN khách hàng	ASN nhà cung cấp	Ký hiệu nhận dạng vùng (Region Identifier)
ASN 1	ASN 2	Ký hiệu nhận dạng vùng 1
ASN 3	ASN 4, ASN 5	Ký hiệu nhận dạng vùng 2
ASN 1	ASN 2	Ký hiệu nhận dạng vùng 3

Trong ví dụ thứ tư, nếu cặp AS (ASN 3:ASN 4) được thể hiện trong Bảng 2 nằm trong vùng có ký hiệu nhận dạng vùng 4, và cũng có quan hệ C2P, cơ sở dữ liệu đầu vào cấp quyền còn bao gồm một đầu vào cấp quyền mà bao gồm cặp AS (ASN 3:ASN 4) và ký hiệu nhận dạng vùng 4.

Chi tiết được thể hiện trong bảng 4:

Bảng 4

ASN khách hàng	ASN nhà cung cấp	Ký hiệu nhận dạng vùng (Region Identifier)
ASN 1	ASN 2	Ký hiệu nhận dạng vùng 1

ASN khách hàng	ASN nhà cung cấp	Ký hiệu nhận dạng vùng (Region Identifier)
ASN 3	ASN 4, ASN 5	Ký hiệu nhận dạng vùng 2
ASN 3	ASN 4	Ký hiệu nhận dạng vùng 4

Cần hiểu rằng đối với ít nhất một cặp AS bao gồm cùng ASN khách hàng, nếu các quan hệ kinh doanh giữa ít nhất một cặp AS trong tất cả các vùng là các quan hệ C2P, ký hiệu nhận dạng vùng trong đầu vào cấp quyền mà bao gồm ít nhất một cặp C2P AS có thể là trống.

Trong ví dụ thứ năm, nếu các cặp AS (ASN 3:ASN 4) và (ASN 3:ASN 5) được thể hiện trong Bảng 2 có quan hệ C2P trong tất cả các vùng, cơ sở dữ liệu đầu vào cấp quyền bao gồm đầu vào cấp quyền mà bao gồm (ASN 3:ASN 4) và (ASN 3:ASN 5) và trong đó ký hiệu nhận dạng vùng có thể là trống.

Chi tiết được thể hiện trong bảng 5:

Bảng 5

ASN khách hàng	ASN nhà cung cấp	Ký hiệu nhận dạng vùng (Region Identifier)
ASN 1	ASN 2	Ký hiệu nhận dạng vùng 1
ASN 3	ASN 4, ASN 5	

Một cách tùy chọn, cơ sở dữ liệu đầu vào cấp quyền có thể bao gồm ít nhất một trong số cơ sở dữ liệu đầu vào cấp quyền thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Để làm rõ ràng phần mô tả, cơ sở dữ liệu đầu vào cấp quyền bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ hai được sử dụng làm ví dụ cho việc mô tả cụ thể dưới đây trong phương án này

của sáng chế.

Cơ sở dữ liệu đầu vào cấp quyền thứ nhất có thể là cơ sở dữ liệu đầu vào cấp quyền được tạo ra dựa trên thông tin cấp quyền ASPA thu được bởi máy chủ. Thông tin cấp quyền ASPA có thể thu được bởi máy chủ từ neo tin cậy của cơ quan đăng ký internet khu vực (Regional Internet Registry, RIR) (ví dụ, có năm RIR: RIR châu Á-Thái Bình Dương, RIR châu Mỹ, RIPE RIR, RIR Mỹ Latin và Caribbean, và RIR châu Phi).

Đối với phần mô tả cụ thể của việc tạo cơ sở dữ liệu đầu vào cấp quyền thứ nhất, tham khảo phần mô tả trong S201 đến S203 dưới đây. Các chi tiết không được mô tả ở đây.

Cơ sở dữ liệu đầu vào cấp quyền thứ hai có thể là cơ sở dữ liệu đầu vào cấp quyền được tạo ra dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên mạng. Đối với phần mô tả cụ thể của việc tạo cơ sở dữ liệu đầu vào cấp quyền thứ hai, tham khảo phần mô tả trong S301 và S302 dưới đây. Các chi tiết không được mô tả ở đây.

Sẽ được hiểu rằng cơ sở dữ liệu đầu vào cấp quyền thứ nhất có thể bao gồm cơ sở dữ liệu con đầu vào cấp quyền thứ nhất và cơ sở dữ liệu con đầu vào cấp quyền thứ hai. Đối với cặp AS bất kỳ trong đầu vào cấp quyền bất kỳ trong cơ sở dữ liệu con đầu vào cấp quyền thứ nhất, các địa chỉ IP được sử dụng bởi cặp AS được nhận diện bởi cặp AS bất kỳ là các địa chỉ IP phiên bản giao thức internet 4 (Internet protocol version 4, IPv4).

Đối với cặp AS bất kỳ trong đầu vào cấp quyền bất kỳ trong cơ sở dữ liệu con đầu vào cấp quyền thứ hai, các địa chỉ IP được sử dụng bởi cặp AS được nhận diện bởi cặp AS bất kỳ là các địa chỉ IP phiên bản giao thức internet 6 (Internet protocol version 6, IPv6).

Tương tự, cơ sở dữ liệu đầu vào cấp quyền thứ hai có thể bao gồm cơ sở dữ liệu con đầu vào cấp quyền thứ ba và cơ sở dữ liệu con đầu vào cấp quyền thứ tư. Đối với cặp AS bất kỳ trong đầu vào cấp quyền bất kỳ trong cơ sở dữ liệu con đầu vào cấp quyền thứ ba, các địa chỉ IP được sử dụng bởi cặp AS được

nhận diện bởi cặp AS bất kỳ là các địa chỉ IP IPv4.

Đối với cặp AS bất kỳ trong đầu vào cấp quyền bất kỳ trong cơ sở dữ liệu con đầu vào cấp quyền thứ tư, các địa chỉ IP được sử dụng bởi cặp AS được nhận diện bởi cặp AS bất kỳ là các địa chỉ IP IPv6.

Do đó, thiết bị mạng có thể kiểm tra cặp AS trong thông tin đường truyền dựa trên thông tin vùng thứ nhất, cơ sở dữ liệu đầu vào cấp quyền thứ nhất, và cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Theo cách thức thực hiện khả thi, thiết bị mạng đầu tiên có thể kiểm tra cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ nhất. Khi cặp AS thứ nhất không được kiểm tra, thiết bị mạng có thể kiểm tra lại cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Cụ thể, khi thiết bị mạng đầu tiên kiểm tra cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ nhất, thiết bị mạng có thể xác định, dựa trên tiền tố trong thông tin đường truyền thu được, cơ sở dữ liệu con đầu vào cấp quyền được sử dụng để kiểm tra cặp AS trong thông tin đường truyền.

Dễ hiểu là, nếu đoạn địa chỉ IP trong tiền tố trong thông tin đường truyền thu được là đoạn địa chỉ IPv4, cơ sở dữ liệu con đầu vào cấp quyền được sử dụng để kiểm tra cặp AS thứ nhất là cơ sở dữ liệu con đầu vào cấp quyền thứ nhất; hoặc nếu đoạn địa chỉ IP trong tiền tố trong thông tin đường truyền là đoạn địa chỉ IPv6, cơ sở dữ liệu đầu vào cấp quyền được sử dụng để kiểm tra cặp AS thứ nhất là cơ sở dữ liệu con đầu vào cấp quyền thứ hai.

Ví dụ, đoạn địa chỉ IP trong tiền tố trong thông tin đường truyền là đoạn địa chỉ IPv4. Trong trường hợp này, cơ sở dữ liệu đầu vào cấp quyền được sử dụng để kiểm tra cặp AS thứ nhất là cơ sở dữ liệu con đầu vào cấp quyền thứ nhất (trong trường hợp này, đầu vào cấp quyền trong cơ sở dữ liệu con đầu vào cấp quyền thứ nhất tương ứng với đầu vào cấp quyền đích trong các phương án của sáng chế).

Sau đó dựa trên thông tin vùng thứ nhất, thiết bị mạng có thể xác định liệu cơ sở dữ liệu con đầu vào cấp quyền thứ nhất có bao gồm đầu vào cấp quyền mà bao gồm cặp AS thứ nhất và ký hiệu nhận dạng vùng tương ứng với thông tin vùng thứ nhất, hoặc xác định liệu cơ sở dữ liệu con đầu vào cấp quyền thứ nhất có bao gồm đầu vào cấp quyền mà bao gồm cặp AS thứ nhất và trong đó mục ký hiệu nhận dạng vùng là trống, để xác định liệu cặp AS thứ nhất có được kiểm tra thành công.

Cụ thể, nếu thiết bị mạng xác định rằng cơ sở dữ liệu con đầu vào cấp quyền thứ nhất bao gồm đầu vào cấp quyền mà bao gồm cặp AS thứ nhất và ký hiệu nhận dạng vùng tương ứng với thông tin vùng thứ nhất, thiết bị mạng xác định rằng cặp AS thứ nhất được kiểm tra thành công.

Nếu thiết bị mạng xác định rằng cơ sở dữ liệu con đầu vào cấp quyền thứ nhất không bao gồm đầu vào cấp quyền mà bao gồm cặp AS thứ nhất và ký hiệu nhận dạng vùng tương ứng với thông tin vùng thứ nhất, thiết bị mạng xác định rằng cặp AS thứ nhất không được kiểm tra.

Một cách tùy chọn, thiết bị mạng đầu tiên có thể xem xét cơ sở dữ liệu con đầu vào cấp quyền thứ nhất, để xác định liệu cơ sở dữ liệu con đầu vào cấp quyền thứ nhất có bao gồm cặp AS thứ nhất.

Do đó, khi cơ sở dữ liệu con đầu vào cấp quyền thứ nhất bao gồm cặp AS thứ nhất, thiết bị mạng có thể còn xác định liệu mục ký hiệu nhận dạng vùng trong đầu vào cấp quyền mà bao gồm cặp AS thứ nhất trong cơ sở dữ liệu con đầu vào cấp quyền thứ nhất là trống. Có thể học được từ nội dung nêu trên là, nếu mục ký hiệu nhận dạng vùng là trống, thì cặp AS trong đầu vào cấp quyền mà bao gồm ký hiệu nhận dạng vùng có cùng quan hệ kinh doanh trong tất cả các vùng.

Do đó, nếu mục ký hiệu nhận dạng vùng là trống, thiết bị mạng xác định rằng cơ sở dữ liệu con đầu vào cấp quyền thứ nhất bao gồm đầu vào cấp quyền mà bao gồm cặp AS thứ nhất và ký hiệu nhận dạng vùng tương ứng với thông tin vùng thứ nhất, nghĩa là, xác định rằng cặp AS thứ nhất được kiểm tra

thành công.

Theo cách thức thực hiện khả thi, nếu mục ký hiệu nhận dạng vùng không trống, thiết bị mạng có thể xác định, theo quy tắc thiết lập trước, vùng địa lý tương ứng với ký hiệu nhận dạng vùng trong mục ký hiệu nhận dạng vùng, và còn xác định liệu vùng địa lý là giống như vùng địa lý được chỉ báo bởi thông tin vùng thứ nhất.

Nếu vùng địa lý là giống như vùng địa lý được chỉ báo bởi thông tin vùng thứ nhất, thiết bị mạng xác định rằng cơ sở dữ liệu con đầu vào cấp quyền thứ nhất bao gồm đầu vào cấp quyền mà bao gồm cặp AS thứ nhất và ký hiệu nhận dạng vùng tương ứng với thông tin vùng thứ nhất. Nếu vùng địa lý khác với vùng địa lý được chỉ báo bởi thông tin vùng thứ nhất, thiết bị mạng xác định rằng cơ sở dữ liệu con đầu vào cấp quyền thứ nhất không bao gồm đầu vào cấp quyền mà bao gồm cặp AS thứ nhất và ký hiệu nhận dạng vùng tương ứng với thông tin vùng thứ nhất, nghĩa là, xác định rằng cặp AS thứ nhất không được kiểm tra.

Theo cách thức thực hiện khả thi khác, nếu mục ký hiệu nhận dạng vùng không trống, thiết bị mạng có thể còn xác định, dựa trên ký hiệu nhận dạng vùng thứ nhất mà được xác định trước theo quy tắc thiết lập trước và tương ứng với thông tin vùng thứ nhất, liệu ký hiệu nhận dạng vùng trong mục ký hiệu nhận dạng vùng trong đầu vào cấp quyền mà bao gồm cặp AS thứ nhất trong cơ sở dữ liệu con đầu vào cấp quyền thứ nhất là ký hiệu nhận dạng vùng thứ nhất.

Nếu ký hiệu nhận dạng vùng trong mục ký hiệu nhận dạng vùng là ký hiệu nhận dạng vùng thứ nhất, thiết bị mạng xác định rằng cơ sở dữ liệu con đầu vào cấp quyền thứ nhất bao gồm đầu vào cấp quyền mà bao gồm cặp AS thứ nhất và ký hiệu nhận dạng vùng tương ứng với thông tin vùng thứ nhất. Nếu ký hiệu nhận dạng vùng trong mục ký hiệu nhận dạng vùng không là ký hiệu nhận dạng vùng thứ nhất, thiết bị mạng xác định rằng cơ sở dữ liệu con đầu vào cấp quyền thứ nhất không bao gồm đầu vào cấp quyền mà bao gồm cặp AS thứ nhất và ký hiệu nhận dạng vùng tương ứng với thông tin vùng thứ nhất, nghĩa là, xác

định rằng cặp AS thứ nhất không được kiểm tra.

Khi cặp AS thứ nhất không được kiểm tra, thiết bị mạng có thể kiểm tra lại cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Cụ thể, khi đoạn địa chỉ IP trong tiền tố trong thông tin đường truyền thu được là đoạn địa chỉ IPv4, thiết bị mạng có thể kiểm tra cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu con đầu vào cấp quyền thứ ba trong cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Đối với quy trình trong đó thiết bị mạng kiểm tra cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu con đầu vào cấp quyền thứ ba, tham khảo phần mô tả nêu trên của quy trình trong đó thiết bị mạng kiểm tra cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu con đầu vào cấp quyền thứ nhất. Chi tiết không được mô tả lại ở đây.

Theo cách thức thực hiện khả thi khác, thiết bị mạng có thể kiểm tra cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ ba. Cơ sở dữ liệu đầu vào cấp quyền thứ ba là cơ sở dữ liệu đầu vào cấp quyền thu được bằng cách kết hợp cơ sở dữ liệu đầu vào cấp quyền thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Có thể hiểu rằng cơ sở dữ liệu đầu vào cấp quyền thứ ba bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ năm và cơ sở dữ liệu đầu vào cấp quyền thứ sáu. Đối với cặp AS bất kỳ trong đầu vào cấp quyền bất kỳ trong cơ sở dữ liệu đầu vào cấp quyền thứ năm, địa chỉ IP được sử dụng bởi cặp AS được nhận diện bởi cặp AS bất kỳ là địa chỉ IP IPv4.

Một cách tùy chọn, cơ sở dữ liệu đầu vào cấp quyền thứ năm có thể thu được bằng cách kết hợp cơ sở dữ liệu con đầu vào cấp quyền thứ nhất và cơ sở dữ liệu con đầu vào cấp quyền thứ ba. Điều này không bị giới hạn ở đây.

Đối với cặp AS bất kỳ trong đầu vào cấp quyền bất kỳ trong cơ sở dữ liệu đầu vào cấp quyền thứ sáu, địa chỉ IP được sử dụng bởi cặp AS được nhận

diện bởi cặp AS bất kỳ là địa chỉ IP IPv6.

Một cách tùy chọn, cơ sở dữ liệu đầu vào cấp quyền thứ sáu có thể thu được bằng cách kết hợp cơ sở dữ liệu con đầu vào cấp quyền thứ hai và cơ sở dữ liệu con đầu vào cấp quyền thứ tư. Điều này không bị giới hạn ở đây.

Do đó, khi đoạn địa chỉ IP trong tiền tố trong thông tin đường truyền thu được là đoạn địa chỉ IPv4, thiết bị mạng có thể kiểm tra cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ năm trong cơ sở dữ liệu đầu vào cấp quyền thứ ba.

Đối với quy trình mà trong đó thiết bị mạng kiểm tra cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu đầu vào cấp quyền thứ năm, tham khảo phần mô tả nêu trên của quy trình mà trong đó thiết bị mạng kiểm tra cặp AS thứ nhất dựa trên thông tin vùng thứ nhất và cơ sở dữ liệu con đầu vào cấp quyền thứ nhất. Chi tiết không được mô tả lại ở đây.

S104: thiết bị mạng kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền thu được, để kiểm tra đường truyền AS được chỉ báo bởi thông tin đường truyền.

Cụ thể, thiết bị mạng có thể kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền thu được, và kiểm tra, theo nguyên tắc thung lũng tự do nêu trên, hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền.

Đối với phần mô tả của nguyên tắc thung lũng tự do, tham khảo phần mô tả nêu trên. Chi tiết không được mô tả lại ở đây.

Có thể học được từ các phần mô tả nêu trên là ít nhất một cặp AS được chứa trong thông tin đường truyền được sắp xếp theo thứ tự thiết lập trước thứ nhất, và thứ tự thiết lập trước thứ nhất tương ứng với thứ tự của các AS mà được đi qua trong đường truyền AS được chỉ báo bởi thông tin đường truyền.

Do đó, thiết bị mạng có thể kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền thu được theo thứ tự thiết lập trước thứ nhất, và

kiểm tra, theo nguyên tắc thung lũng tự do nêu trên, hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền.

Theo một ví dụ, viện dẫn tới FIG.1, thông tin đường truyền là thông tin đường truyền của đường truyền AS 1 được thể hiện trong FIG.1 được sử dụng như là ví dụ để mô tả.

Đối với đường truyền AS 1 (ASN 5, ASN 4, ASN 3, ASN 2, ASN 1), thiết bị mạng có thể kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền của đường truyền AS 1 bắt đầu từ cặp AS bao gồm AS bắt đầu trong đường truyền AS 1. Cụ thể, thiết bị mạng có thể kiểm tra tất cả các cặp AS trong thông tin đường truyền của đường truyền AS 1 theo thứ tự là ASN 1:ASN 2 → ASN 2:ASN 3 → ASN 3:ASN 4 → ASN 4:ASN 5.

Chắc chắn là, thiết bị mạng có thể còn kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền của đường truyền AS 1 bắt đầu từ cặp AS bao gồm AS kết thúc trong đường truyền AS 1. Cụ thể, thiết bị mạng có thể kiểm tra tất cả các cặp AS trong thông tin đường truyền của đường truyền AS 1 theo thứ tự là ASN 4:ASN 5 → ASN 3:ASN 4 → ASN 2:ASN 3 → ASN 1:ASN 2. Điều này không bị giới hạn ở đây.

Sẽ được hiểu rằng, khi mỗi cặp AS trong thông tin đường truyền được kiểm tra theo nguyên tắc thung lũng tự do nêu trên và cơ sở dữ liệu đầu vào cấp quyền mà bao gồm chỉ cặp C2P AS, nếu thông tin đường truyền bao gồm nhiều nhất một cặp AS mà không được kiểm tra, có thể được xác định rằng đường truyền AS được chỉ báo bởi thông tin đường truyền được kiểm tra thành công, nói cách khác, đường truyền AS là có hiệu lực. Nếu thông tin đường truyền bao gồm ít nhất hai cặp AS mà không được kiểm tra, có thể được xác định rằng đường truyền AS được chỉ báo bởi thông tin đường truyền không được kiểm tra, nói cách khác, đường truyền AS là không có hiệu lực.

Sẽ được hiểu rằng, khi cặp AS trong thông tin đường truyền không được kiểm tra trong lần đầu tiên, thiết bị mạng có thể đảo ngược cặp AS mà chưa được kiểm tra trong thông tin đường truyền. Đối với cặp AS bất kỳ mà

chưa được kiểm tra, thiết bị mạng có thể trao đổi hai số AS trong cặp AS, để đảo ngược cặp AS. Theo cách này, quan hệ kinh doanh giữa cặp AS có thể được đảo ngược.

Ví dụ, đối với cặp AS ASN 1:ASN 2 có quan hệ C2P, sau khi các số AS trong cặp AS được trao đổi, cặp AS được đảo ngược ASN 2:ASN 1 thu được, và quan hệ kinh doanh của cặp AS được đảo ngược là quan hệ P2C.

Theo cách này, thiết bị mạng có thể kiểm tra cặp P2C AS trong thông tin đường truyền dựa trên cơ sở dữ liệu đầu vào cấp quyền mà bao gồm chỉ cặp C2P AS. Có thể hiểu rằng sau khi cặp P2C AS được đảo ngược, cặp C2P AS được thu nhận.

Theo một ví dụ, viện dẫn tới FIG.1, thông tin đường truyền là thông tin đường truyền của đường truyền AS 1 được thể hiện trong FIG.1, và thiết bị mạng kiểm tra tất cả các cặp AS trong thông tin đường truyền của đường truyền AS 1 theo thứ tự là ASN 1:ASN 2 → ASN 2:ASN 3 → ASN 3:ASN 4 → ASN 4:ASN 5 được sử dụng như là ví dụ để mô tả.

Thiết bị mạng có thể kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền của đường truyền AS 1 dựa trên phương pháp được mô tả trong S102 và S103. Thiết bị mạng thành công trong việc kiểm tra các cặp AS ASN 1:ASN 2 và ASN 2:ASN 3, nhưng không kiểm tra cặp AS ASN 3:ASN 4. Nói cách khác, thiết bị mạng không kiểm tra các cặp AS trong lần đầu tiên trong quá trình kiểm tra của đường truyền AS 1.

Trong trường hợp này, thiết bị mạng có thể đảo ngược cặp AS ASN 4:ASN 5 mà chưa được kiểm tra trong thông tin đường truyền của đường truyền AS 1, nghĩa là, đảo ngược cặp AS ASN 4:ASN 5 thành ASN 5:ASN 4. Sau đó thiết bị mạng tiếp tục kiểm tra cặp AS ASN 5:ASN 4 bằng cách sử dụng phương pháp được mô tả trong S102 và S103.

Nếu cặp AS ASN 5:ASN 4 được kiểm tra thành công, nó chỉ báo là thông tin đường truyền của đường truyền AS 1 bao gồm một cặp AS mà không được kiểm tra (nghĩa là, cặp AS ASN 3:ASN 4 mà không được kiểm tra). Trong

trường hợp này, được xem là đường truyền AS 1 được kiểm tra thành công, nói cách khác, đường truyền AS 1 là có hiệu lực. Nếu cặp AS ASN 5:ASN 4 không được kiểm tra, nó chỉ báo là thông tin đường truyền của đường truyền AS 1 bao gồm hai cặp AS mà không được kiểm tra (cụ thể, các cặp AS ASN 3:ASN 4 và ASN 4:ASN 5 (hoặc ASN 5:ASN 4) không được kiểm tra). Trong trường hợp này, được xem là đường truyền AS 1 không được kiểm tra, nói cách khác, đường truyền AS 1 là không có hiệu lực.

S105 (tùy chọn): thiết bị mạng gửi kết quả kiểm tra của đường truyền AS được chỉ báo bởi thông tin đường truyền đến thiết bị đích.

Thiết bị đích có thể là thiết bị mà ở trong AS (tương ứng với AS thứ nhất trong các phương án của sáng chế) mà thiết bị mạng thuộc về và được kết nối với thiết bị mạng để truyền thông. Thiết bị đích có thể trao đổi thông tin định tuyến BGP với thiết bị mạng bằng cách chạy BGP nội bộ (internal/interior BGP, IBGP). Các chi tiết không được mô tả ở đây.

Sau khi hoàn thành việc kiểm tra đường truyền AS được chỉ báo bởi thông tin đường truyền, thiết bị mạng có thể gửi thông tin đường truyền và kết quả kiểm tra đến thiết bị đích.

Đáp lại điều này, thiết bị đích có thể thu thông tin đường truyền và kết quả kiểm tra. Do đó, sau khi thu bản tin cập nhật BGP bao gồm thông tin đường truyền, thiết bị đích có thể xử lý thông tin đường truyền dựa trên kết quả kiểm tra, mà không kiểm tra thông tin đường truyền. Điều này làm giảm các tài nguyên được sử dụng của thiết bị đích, và cải thiện hiệu quả của thiết bị đích.

S106 (tùy chọn): thiết bị mạng tạo ra đầu vào chuyển tiếp dựa trên thông tin đường truyền.

Khi thiết bị mạng thành công trong việc kiểm tra đường truyền AS được chỉ báo bởi thông tin đường truyền, nó chỉ báo là không có sự rò rỉ tuyến xảy ra trên thông tin đường truyền, nói cách khác, đường truyền AS được chỉ báo bởi thông tin đường truyền là có hiệu lực.

Trong trường hợp này, thiết bị mạng có thể tạo ra đầu vào chuyển tiếp thứ nhất dựa trên thông tin đường truyền, và sử dụng đầu vào chuyển tiếp thứ nhất làm đầu vào chuyển tiếp với quyền ưu tiên cao nhất, để chuyển tiếp bản tin.

Khi thiết bị mạng không kiểm tra đường truyền AS được chỉ báo bởi thông tin đường truyền, nó chỉ báo là sự rò rỉ tuyến có thể xảy ra trên thông tin đường truyền, nói cách khác, đường truyền AS được chỉ báo bởi thông tin đường truyền là không có hiệu lực.

Trong trường hợp này, thiết bị mạng có thể tạo ra đầu vào chuyển tiếp thứ hai dựa trên thông tin đường truyền, và đánh dấu thông tin cụ thể cho đầu vào chuyển tiếp thứ hai. Thông tin cụ thể được sử dụng để chỉ báo liệu đầu vào chuyển tiếp thứ hai là đầu vào chuyển tiếp rủi ro cao hay đầu vào chuyển tiếp ưu tiên thấp.

Mức độ rủi ro hoặc mức độ ưu tiên của đầu vào chuyển tiếp có thể được sử dụng để chỉ báo xác suất rò rỉ thông tin định tuyến trong đầu vào chuyển tiếp. Ví dụ, đối với đầu vào chuyển tiếp có mức độ rủi ro cao (nghĩa là, đầu vào chuyển tiếp rủi ro cao) hoặc đầu vào chuyển tiếp có mức độ ưu tiên thấp (nghĩa là, đầu vào chuyển tiếp ưu tiên thấp), có khả năng cao là rò rỉ thông tin định tuyến ở đầu vào chuyển tiếp. Nói cách khác, thông tin định tuyến trong đầu vào chuyển tiếp dễ rò rỉ.

Do đó, thiết bị mạng có thể xác định, dựa trên mức độ rủi ro hoặc mức độ ưu tiên của đầu vào chuyển tiếp, đầu vào chuyển tiếp được sử dụng để chuyển tiếp bản tin. Thiết bị mạng thường lựa chọn đầu vào an toàn để chuyển tiếp bản tin. Khi không có đầu vào chuyển tiếp an toàn trong đầu vào chuyển tiếp ứng viên, thiết bị mạng có thể lựa chọn đầu vào chuyển tiếp rủi ro thấp hoặc đầu vào chuyển tiếp ưu tiên cao để chuyển tiếp bản tin.

Phần nêu trên mô tả phương pháp kiểm tra cặp AS được đề xuất trong phương án này của sáng chế. Phương pháp này có thể tránh được một cách hiệu quả trường hợp trong đó đường truyền AS được chỉ báo bởi thông tin đường truyền được xác định không chính xác do cặp AS trong thông tin đường truyền

được xác định không chính xác trong quá trình kiểm tra của đường truyền AS, và cải thiện một cách hiệu quả độ chính xác kiểm tra đường truyền AS.

Phần sau đây mô tả phương pháp để tạo cơ sở dữ liệu đầu vào cấp quyền thứ nhất và phương pháp để tạo cơ sở dữ liệu đầu vào cấp quyền thứ hai mà được đề xuất trong các phương án của sáng chế.

FIG.6 là lưu đồ giản lược của phương pháp để tạo cơ sở dữ liệu đầu vào cấp quyền thứ nhất theo phương án của sáng chế. Phương pháp có thể được áp dụng với hệ thống kiểm tra 40 được thể hiện trong FIG.4. Phương pháp này có thể bao gồm các bước sau đây.

S201: máy chủ thu nhận thông tin cấp quyền ASPA.

Máy chủ có thể là máy chủ bộ nhớ sẵn RPKI. Điều này không bị giới hạn ở đây.

Thông tin cấp quyền ASPA bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước, và ký hiệu nhận dạng vùng của vùng mà cặp AS thuộc về.

Ở đây, đối với phần mô tả của cặp AS có quan hệ kinh doanh được thiết lập trước, tham khảo phần mô tả nêu trên của cặp AS có quan hệ kinh doanh được thiết lập trước. Chi tiết không được mô tả lại ở đây.

Ký hiệu nhận dạng vùng có thể được sử dụng để nhận diện duy nhất vùng địa lý. Do đó, ký hiệu nhận dạng vùng của vùng mà cặp AS thuộc về được sử dụng để nhận diện duy nhất vùng địa lý mà trong đó cặp AS được đặt. Diện tích của vùng địa lý không bị giới hạn cụ thể trong phương án này của sáng chế.

Ví dụ, vùng địa lý có thể là vùng địa lý thu được thông qua việc phân chia theo lục địa, có thể là vùng địa lý thu được thông qua việc phân chia theo nước, hoặc có thể là vùng địa lý thu được thông qua việc phân chia theo tỉnh. Điều này không bị giới hạn ở đây.

Đối với các vùng địa lý khác nhau, các tài liệu nhận dạng đơn nhất (identity document, ID) có thể được sử dụng làm ký hiệu nhận dạng vùng tương ứng với vùng địa lý. Các ID được sử dụng để nhận dạng các vùng địa lý khác

nhau có thể được xác định theo quy tắc thiết lập trước. Quy tắc thiết lập trước không bị giới hạn cụ thể trong phương án này của sáng chế.

Một cách tùy chọn, quy tắc thiết lập trước có thể là để nhận dạng các vùng địa lý khác nhau bằng cách sử dụng các ID được xác định trước.

Ví dụ, vùng địa lý 1 có thể được nhận dạng bằng cách sử dụng ID được xác định trước 1, và vùng địa lý 2 có thể được nhận dạng bằng cách sử dụng ID được xác định trước 2. Các chi tiết không được mô tả ở đây.

Một cách tùy chọn, quy tắc thiết lập trước có thể còn là để nhận dạng các vùng địa lý khác nhau bằng cách sử dụng các ID được xác định theo quy tắc mã hóa thiết lập trước. Quy tắc mã hóa thiết lập trước không bị giới hạn cụ thể trong phương án này của sáng chế.

Ví dụ, ID được sử dụng để nhận dạng vùng địa lý thu được thông qua việc phân chia theo lục địa có thể thu được bằng cách mã hóa số nhị phân 5-bit theo thứ tự tăng dần theo quy tắc mã hóa.

Như được thể hiện trong Bảng 6, ký hiệu nhận dạng vùng tương ứng với châu Phi có thể là 00001 (nghĩa là, 1), ký hiệu nhận dạng vùng tương ứng với châu Đại Dương có thể là 00010 (nghĩa là, 2), ký hiệu nhận dạng vùng tương ứng với châu Á có thể là 00011 (nghĩa là, 3), ký hiệu nhận dạng vùng tương ứng với Nam Cực có thể là 00100 (nghĩa là, 4), ký hiệu nhận dạng vùng tương ứng với châu Âu có thể là 00101 (nghĩa là, 5), ký hiệu nhận dạng vùng tương ứng với Mỹ Latin/các đảo Caribbean có thể là 00110 (nghĩa là, 6), ký hiệu nhận dạng vùng tương ứng với Bắc Mỹ có thể là 00111 (nghĩa là, 7), và ký hiệu nhận dạng vùng tương ứng với vùng đặt trước có thể nằm trong khoảng từ 01000 đến 11111 (nghĩa là, 8 đến 31).

Chi tiết được thể hiện trong bảng 6:

Bảng 6

Vùng địa lý	Ký hiệu nhận dạng vùng

Vùng địa lý	Ký hiệu nhận dạng vùng
Châu Phi (Africa (AF))	00001
Châu Đại Dương (Oceania (OC))	00010
Châu Á (Asia (AS))	00011
Nam Cực (Antarctica (AQ))	00100
Châu Âu (Europe (EU))	00101
Mỹ Latin /đảo Caribbean (Latin America / Caribbean Islands (LAC))	00110
Bắc Mỹ (North America (NA))	00111
Vùng đặt trước (Reserved)	01000 đến 11111

Theo cách thức thực hiện khả thi, máy chủ có thể thu nhận thông tin cấp quyền ASPA từ neo tin cậy.

Cụ thể, chức năng của neo tin cậy có thể được thực hiện bởi thiết bị máy tính bất kỳ có khả năng xử lý điện toán. Dạng cụ thể của thiết bị thực hiện chức năng của neo tin cậy không bị giới hạn trong phương án này của sáng chế.

Neo tin cậy có thể là neo tin cậy của RIR. Ví dụ, đối với RIR châu Á-Thái Bình Dương, neo tin cậy có thể là neo tin cậy 1. Theo ví dụ khác, đối với RIR châu Mỹ, neo tin cậy có thể là neo tin cậy 2. Các chi tiết không được mô tả ở đây.

Cụ thể, người dùng có số AS (mà được đề cập ngắn gọn là người dùng AS) có thể báo cáo thông tin ASPA của người dùng AS cho neo tin cậy của RIR tương ứng với vùng mà trong đó người dùng AS được đặt. Theo cách này, neo tin cậy của RIR có thể thu nhận thông tin cấp quyền ASPA của người dùng AS.

Một cách tùy chọn, người dùng AS có thể đăng ký thông tin ASPA trên

trang web RIR tương ứng với vùng mà trong đó người dùng AS được đặt, sao cho neo tin cậy của RIR xác định thông tin cấp quyền ASPA dựa trên thông tin ASPA.

Có thể học được từ phần mô tả nêu trên là cơ sở dữ liệu đầu vào cấp quyền có thể bao gồm chỉ cặp C2P AS. Do đó, khi người dùng AS đăng ký thông tin ASPA trên trang web RIR tương ứng với vùng mà trong đó người dùng AS được đặt, chỉ người dùng AS đóng vai trò làm khách hàng cần đăng ký thông tin ASPA trên trang web RIR tương ứng với vùng mà trong đó người dùng AS được đặt.

Phần sau đây đề xuất phần mô tả bằng cách sử dụng ví dụ là người dùng AS đóng vai trò làm khách hàng đăng ký thông tin ASPA trên trang web RIR tương ứng với vùng mà trong đó người dùng AS được đặt.

Ví dụ, FIG.7(a) và FIG.7(b) là các sơ đồ giản lược của việc đăng ký thông tin ASPA bởi người dùng AS trên trang web RIR.

Như được thể hiện trong FIG.7(a), người dùng AS đầu tiên có thể đăng nhập vào trang web RIR bằng cách sử dụng tài khoản và mật khẩu đã đăng ký trước thông qua giao diện đăng nhập trang web RIR trên màn hình 70.

Sau đó trong giao diện "Đăng ký quan hệ kinh doanh" 701 của trang web RIR được hiển thị trên màn hình 70, người dùng AS có thể nhập số AS của AS đóng vai trò làm khách hàng trong hộp "AS khách hàng", nhập số AS của AS đóng vai trò làm nhà cung cấp của AS khách hàng trong hộp "AS nhà cung cấp", và nhập, trong hộp "Vùng địa lý", vùng địa lý mà trong đó cặp AS bao gồm số AS của AS khách hàng và số AS của AS nhà cung cấp được đặt.

Sẽ được hiểu rằng chỉ có một số AS trong hộp "AS khách hàng", nhưng có thể có nhiều số AS trong hộp "AS nhà cung cấp". Nói cách khác, một AS khách hàng có thể tương ứng với nhiều AS nhà cung cấp. Điều này không bị giới hạn ở đây.

Sau đó người dùng AS gõ vào nút "Đăng ký" trong giao diện 701, để

gửi thông tin ASPA được nhập trong giao diện "701" đến RIR.

Theo cách này, neo tin cậy của RIR có thể thu thông tin ASPA được gửi bởi người dùng AS, và xác định ít nhất một cặp C2P AS dựa trên thông tin ASPA. Neo tin cậy của RIR có thể còn xác định, dựa trên vùng địa lý mà trong đó ít nhất một cặp C2P AS được đặt và theo quy tắc thiết lập trước nêu trên, ký hiệu nhận dạng vùng của vùng mà ít nhất một cặp C2P AS thuộc về. Theo cách này, neo tin cậy của RIR thu nhận thông tin cấp quyền ASPA của người dùng AS dựa trên thông tin ASPA được gửi bởi người dùng AS.

Có thể hiểu được rằng, dựa trên ví dụ được mô tả trên FIG.7(a), người dùng AS có thể đăng ký thông tin ASPA của người dùng AS trên trang web RIR, nghĩa là, nhập số AS của người dùng AS trong hộp "AS khách hàng" trên FIG.7(a). Theo cách khác, thông tin ASPA đã biết của người dùng AS khác có thể được đăng ký trên trang web RIR. Cụ thể, số AS của AS khác được nhập trong hộp "AS khách hàng" trên FIG.7(a). Điều này không bị giới hạn ở đây.

Như được thể hiện trong FIG.7(b), giao diện "Đăng ký quan hệ kinh doanh" 701 của trang web RIR được hiển thị trên màn hình 70 bao gồm chỉ hộp "AS nhà cung cấp". Trong trường hợp này, AS đóng vai trò làm khách hàng của AS nhà cung cấp là người dùng AS mà nhập vào thông tin ASPA theo cách mặc định.

Người dùng AS có thể đăng nhập vào trang web RIR bằng cách sử dụng tài khoản và mật khẩu đã đăng ký trước thông qua giao diện đăng nhập trang web RIR trên màn hình 70. Sau khi giao diện "Đăng ký quan hệ kinh doanh" 701 được hiển thị trên màn hình 70, người dùng AS có thể nhập số AS của AS đóng vai trò làm nhà cung cấp của người dùng AS trong hộp "AS nhà cung cấp", và nhập, trong hộp "Vùng địa lý", vùng địa lý mà trong đó cặp AS bao gồm số AS của AS nhà cung cấp và số AS của người dùng AS được đặt.

Sẽ được hiểu rằng có thể có nhiều số AS trong hộp "AS nhà cung cấp". Các chi tiết không được mô tả ở đây.

Sau đó người dùng AS gõ vào nút "Đăng ký" trong giao diện 701, để

gửi thông tin ASPA được nhập trong giao diện "701" đến RIR.

Theo cách này, neo tin cậy của RIR có thể thu thông tin ASPA được gửi bởi người dùng AS, và xác định ít nhất một cặp C2P AS dựa trên thông tin ASPA. Neo tin cậy của RIR có thể còn xác định, dựa trên vùng địa lý mà trong đó ít nhất một cặp C2P AS được đặt và theo quy tắc thiết lập trước nêu trên, ký hiệu nhận dạng vùng của vùng mà ít nhất một cặp C2P AS thuộc về. Theo cách này, neo tin cậy của RIR thu nhận thông tin cấp quyền ASPA của người dùng AS dựa trên thông tin ASPA được gửi bởi người dùng AS.

Có thể hiểu được rằng, dựa trên ví dụ được mô tả trên FIG.7(b), người dùng AS có thể đăng ký thông tin ASPA của người dùng AS trên trang web RIR.

Theo cách này, neo tin cậy của RIR có thể xác định các đoạn thông tin cấp quyền ASPA dựa trên các đoạn thông tin ASPA được đăng ký bởi một hoặc nhiều người dùng AS.

Sau đó neo tin cậy của RIR có thể gửi thông tin cấp quyền ASPA được xác định đến máy chủ theo cách mã hóa hoặc không mã hóa.

Một cách tùy chọn, neo tin cậy của RIR có thể gửi thông tin cấp quyền ASPA được xác định đến máy chủ theo cách mã hóa hoặc không mã hóa vào lúc thu yêu cầu của máy chủ để thu nhận thông tin cấp quyền ASPA.

Một cách tùy chọn, neo tin cậy của RIR có thể chủ động gửi thông tin cấp quyền ASPA được xác định đến máy chủ theo cách mã hóa hoặc không mã hóa.

Một cách tùy chọn, neo tin cậy của RIR có thể chủ động gửi thông tin cấp quyền ASPA được xác định đến máy chủ theo cách mã hóa hoặc không mã hóa dựa trên chu kỳ thiết lập trước. Điều này không bị giới hạn ở đây.

Đáp lại điều này, máy chủ thu thông tin cấp quyền ASPA được gửi bởi neo tin cậy của RIR, nghĩa là, thu nhận thông tin cấp quyền ASPA.

Theo cách thức thực hiện khả thi khác, máy chủ thu nhận ít nhất một đoạn thông tin cấp quyền ASPA được xác định dựa trên bảng định tuyến mạng

và/hoặc dữ liệu mạng được bộc lộ trên mạng.

Một cách tùy chọn, máy chủ có thể thu ít nhất một đoạn thông tin cấp quyền ASPA được gửi bởi thiết bị mạng. Ít nhất một đoạn thông tin cấp quyền ASPA có thể là ít nhất một đoạn thông tin cấp quyền ASPA được xác định bởi thiết bị mạng dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên và thu được từ mạng.

Bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên mạng bao gồm/bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước và thông tin vùng của vùng mà cặp AS thuộc về. Theo cách này, thiết bị mạng có thể xác định ít nhất một đoạn thông tin cấp quyền ASPA dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng.

Ví dụ, thiết bị mạng có thể trích xuất ít nhất một cặp AS trong bảng định tuyến mạng và/hoặc dữ liệu mạng bằng cách sử dụng công cụ xử lý tuyến, và phân tích quan hệ kinh doanh giữa ít nhất một cặp AS. Sau đó thiết bị mạng có thể xác định, từ ít nhất một cặp AS, ít nhất một cặp AS có quan hệ kinh doanh được thiết lập trước.

Sau đó thiết bị mạng có thể xác định, dựa trên ngữ cảnh hoặc tiền tố của bảng định tuyến mạng và/hoặc dữ liệu mạng, thông tin vùng của vị trí địa lý của ít nhất một cặp AS có quan hệ kinh doanh được thiết lập trước. Chắc chắn là, bảng định tuyến mạng và/hoặc dữ liệu mạng có thể còn bao gồm thông tin vùng tương ứng với ít nhất một cặp AS có quan hệ kinh doanh được thiết lập trước. Điều này không bị giới hạn ở đây.

Sau đó thiết bị mạng có thể xác định, dựa trên thông tin vùng tương ứng với ít nhất một cặp AS có quan hệ kinh doanh được thiết lập trước và theo quy tắc thiết lập trước nêu trên, ký hiệu nhận dạng vùng tương ứng với ít nhất một cặp AS có quan hệ kinh doanh được thiết lập trước. Theo cách này, thiết bị mạng xác định ít nhất một đoạn thông tin cấp quyền ASPA dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên mạng.

Một cách tùy chọn, máy chủ có thể còn trực tiếp thu nhận, từ mạng,

bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên mạng, và xác định ít nhất một đoạn thông tin cấp quyền ASPA.

Đối với quy trình mà trong đó máy chủ xác định ít nhất một đoạn thông tin cấp quyền ASPA dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên mạng, tham khảo phần mô tả nêu trên để xác định, bởi thiết bị mạng, ít nhất một đoạn thông tin cấp quyền ASPA dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên mạng. Chi tiết không được mô tả lại ở đây.

S202: máy chủ gửi thông tin cấp quyền ASPA tới thiết bị mạng.

Thiết bị mạng có thể là thiết bị mạng mà thực hiện phương pháp kiểm tra cặp AS nêu trên, hoặc có thể là thiết bị mạng khác bất kỳ mà có khả năng xử lý điện toán. Điều này không bị giới hạn ở đây.

Một cách tùy chọn, máy chủ đầu tiên có thể tạo ra ít nhất một bản tin đơn vị dữ liệu giao thức (protocol data unit, PDU) dựa trên ít nhất một đoạn thông tin cấp quyền ASPA thu được. Sau đó máy chủ gửi ít nhất một bản tin PDU đến thiết bị mạng.

Sẽ được hiểu rằng một đoạn thông tin cấp quyền ASPA tương ứng với một bản tin PDU. Cụ thể, một bản tin PDU bao gồm ít nhất một cặp AS có quan hệ kinh doanh được thiết lập trước, và bao gồm ký hiệu nhận dạng vùng của vùng mà ít nhất một cặp AS có quan hệ kinh doanh được thiết lập trước thuộc về. Ở đây, đối với phần mô tả của cặp AS có quan hệ kinh doanh được thiết lập trước, tham khảo phần mô tả nêu trên của cặp AS có quan hệ kinh doanh được thiết lập trước. Chi tiết không được mô tả lại ở đây.

Ví dụ, quan hệ kinh doanh được thiết lập trước là quan hệ C2P. Trong trường hợp này, một bản tin PDU bao gồm một số AS của một AS đóng vai trò làm khách hàng, ít nhất một số AS của ít nhất một AS đóng vai trò làm nhà cung cấp, và ký hiệu nhận dạng vùng của vùng mà ít nhất một cặp C2P AS bao gồm số AS khách hàng và ít nhất một số AS nhà cung cấp thuộc về.

Phần sau đây thể hiện ví dụ về định dạng của bản tin PDU được đề xuất trong phương án này của sáng chế.

FIG.8 là sơ đồ giản lược của bản tin PDU theo phương án của sáng chế.

Như được thể hiện trong FIG.8, trường phiên bản giao thức (Protocol Version) được sử dụng để chỉ báo số phiên bản của giao thức truyền thông được sử dụng giữa máy chủ và thiết bị mạng, và thường chiếm giữ 1 byte, nghĩa là, 8 bit.

Ví dụ, nếu số phiên bản của giao thức truyền thông chạy giữa máy chủ và thiết bị mạng là 2.0, giá trị của trường này là 2, nghĩa là, 00000010.

Trường loại PDU (PDU type) được sử dụng để chỉ báo loại PDU, và thường chiếm giữ 1 byte, nghĩa là, 8 bit. Ví dụ, nếu giá trị của loại PDU là 11, giá trị của trường này là 11, nghĩa là, 00001011.

Trường đệm (zero) được sử dụng để thực hiện việc căn chỉnh 4-byte trên bản tin PDU, trong đó việc căn chỉnh 4-byte có nghĩa là số lượng bit có thể chia cho 32. Các chi tiết không được mô tả ở đây.

Như được thể hiện trong FIG.8, bản tin PDU bao gồm hai trường zero, và trường zero thứ nhất chiếm giữ 2 byte, nghĩa là, 16 bit. Trường zero thứ hai chiếm giữ 1 byte, nghĩa là, 8 bit.

Trường độ dài (length) được sử dụng để chỉ báo độ dài của bản tin PDU, và thường chiếm giữ 4 byte, nghĩa là, 32 bit.

Trường cờ (flags) thường chiếm giữ 1 byte, nghĩa là, 8 bit. Các bit trong trường này có thể nhận diện nội dung khác nhau.

Ví dụ, bit thứ nhất trong trường này có thể được sử dụng để chỉ báo liệu cặp AS được mang trong bản tin PDU có cần được thông báo. Ví dụ, khi bit thứ nhất là 0, nó chỉ báo là cặp AS được mang trong bản tin PDU là cần được thông báo; hoặc khi bit thứ nhất là 1, nó chỉ báo là cặp AS được mang trong bản tin PDU là cần được rút.

Bit thứ hai trong trường này có thể được sử dụng để chỉ báo phiên bản IP được sử dụng bởi cặp AS được chỉ báo bởi cặp AS bất kỳ được mang trong bản tin PDU. Ví dụ, khi bit thứ hai là 0, nó chỉ báo là cặp AS được chỉ báo bởi cặp AS bất kỳ được mang trong bản tin PDU sử dụng địa chỉ IP IPv4; hoặc khi bit thứ hai là 1, nó chỉ báo là cặp AS được chỉ báo bởi cặp AS bất kỳ được mang trong bản tin PDU sử dụng địa chỉ IP IPv6.

Sẽ được hiểu rằng, trong trường hợp này, việc duy trì 6 bit trong trường này là được đặt trước.

Trường đếm AS nhà cung cấp (đếm AS nhà cung cấp) được sử dụng để chỉ báo số lượng AS đóng vai trò làm nhà cung cấp trong các cặp AS được mang trong bản tin PDU, và thường chiếm giữ 2 byte, nghĩa là, 16 bit.

Trường số AS khách hàng (customer autonomous system number) được sử dụng để chỉ báo số AS của AS đóng vai trò làm khách hàng trong cặp AS được mang trong bản tin PDU, và thường chiếm giữ 4 byte, nghĩa là, 32 bit.

Trường số AS nhà cung cấp (provider autonomous system number(s)) được sử dụng để chỉ báo số AS của AS đóng vai trò làm nhà cung cấp trong cặp AS được mang trong bản tin PDU, và thường chiếm giữ 4 byte, nghĩa là, 32 bit.

Sẽ được hiểu rằng trường này có thể bao gồm các số AS của nhiều AS đóng vai trò làm các nhà cung cấp, và số lượng cụ thể là số lượng được chỉ báo trong trường đếm AS nhà cung cấp.

Trường ký hiệu nhận dạng vùng (ký hiệu nhận dạng vùng) được sử dụng để chỉ báo ký hiệu nhận dạng vùng của vùng mà cặp C2P AS được mang trong bản tin PDU thuộc về. Như được thể hiện trong FIG.8, trường này có thể có độ dài là 4 byte, nghĩa là, 32 bit.

Sẽ được hiểu rằng độ dài thực tế của trường ký hiệu nhận dạng vùng liên quan đến quy tắc thiết lập trước nêu trên để xác định ký hiệu nhận dạng vùng tương ứng với vùng địa lý. Ví dụ, khi số nhị phân 5-bit được sử dụng để mã hóa ký hiệu nhận dạng vùng, độ dài thực tế của ký hiệu nhận dạng vùng là 5

bit.

Có thể hiểu rằng đối với các cặp C2P AS bao gồm cùng số AS khách hàng, các cặp C2P AS có thể thuộc về cùng vùng hoặc có thể thuộc về các vùng khác nhau. Khi các cặp C2P AS bao gồm cùng số AS khách hàng thuộc về các vùng khác nhau, số lượng bản tin PDU mang các cặp C2P AS là giống như số lượng các vùng mà các cặp C2P AS thuộc về.

Ví dụ, đối với năm cặp C2P AS sau đây: ASN 1:ASN 2, ASN 1:ASN 3, ASN 1:ASN 4, ASN 1:ASN 5, và ASN 1:ASN 6; cặp C2P AS ASN 1:ASN 2, ASN 1:ASN 3, và ASN 1:ASN 4 thuộc về vùng 1 với ký hiệu nhận dạng vùng 1 tương ứng; và cặp C2P AS ASN 1:ASN 5 và ASN 1:ASN 6 thuộc về vùng 2 với ký hiệu nhận dạng vùng 2 tương ứng. Nói cách khác, số lượng vùng mà năm cặp C2P AS thuộc về là 2.

Trong trường hợp này, máy chủ có thể gửi năm C2P AS và các ký hiệu nhận dạng vùng tương ứng bằng cách sử dụng hai bản tin PDU. Ví dụ, PDU 1 mang cặp C2P AS ASN 1:ASN 2, ASN 1:ASN 3, và ASN 1:ASN 4, và ký hiệu nhận dạng vùng 1; và PDU 2 mang cặp C2P AS ASN 1:ASN 5 và ASN 1:ASN 6, và ký hiệu nhận dạng vùng 2.

S203: thiết bị mạng thu nhận thông tin cấp quyền ASPA, và tạo ra cơ sở dữ liệu đầu vào cấp quyền thứ nhất dựa trên thông tin cấp quyền ASPA.

Một cách tùy chọn, sau khi thu ít nhất một bản tin PDU được gửi bởi máy chủ, thiết bị mạng có thể thu nhận thông tin cấp quyền ASPA từ ít nhất một bản tin PDU.

Sau đó thiết bị mạng có thể tạo ra cơ sở dữ liệu đầu vào cấp quyền thứ nhất dựa trên thông tin cấp quyền ASPA thu được.

Có thể hiểu rằng, khi trường cờ trong bản tin PDU chỉ báo rằng địa chỉ IP được sử dụng bởi cặp AS được chỉ báo bởi cặp AS bất kỳ được mang trong bản tin PDU là địa chỉ IP IPv4, thông tin cấp quyền ASPA thu được bởi thiết bị mạng từ bản tin PDU được sử dụng để tạo ra cơ sở dữ liệu con đầu vào cấp

quyền thứ nhất trong cơ sở dữ liệu đầu vào cấp quyền thứ nhất.

Tương tự, khi trường cờ trong bản tin PDU chỉ báo rằng địa chỉ IP được sử dụng bởi cặp AS được chỉ báo bởi cặp AS bất kỳ được mang trong bản tin PDU là địa chỉ IP IPv6, thông tin cấp quyền ASPA thu được bởi thiết bị mạng từ bản tin PDU được sử dụng để tạo ra cơ sở dữ liệu con đầu vào cấp quyền thứ hai trong cơ sở dữ liệu đầu vào cấp quyền thứ nhất.

Đối với phần mô tả chi tiết của cơ sở dữ liệu đầu vào cấp quyền thứ nhất, tham khảo phần mô tả nêu trên của cơ sở dữ liệu đầu vào cấp quyền. Chi tiết không được mô tả lại ở đây.

Có thể hiểu rằng khi thông tin cấp quyền ASPA thu được bởi thiết bị mạng bao gồm thông tin cấp quyền ASPA được xác định dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên mạng, cơ sở dữ liệu đầu vào cấp quyền trong phương án này của sáng chế không còn bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ hai nữa. Nói cách khác, cơ sở dữ liệu đầu vào cấp quyền thứ nhất là cơ sở dữ liệu đầu vào cấp quyền được mô tả trong phương án này của sáng chế.

FIG.9 là lưu đồ giản lược của phương pháp để tạo cơ sở dữ liệu đầu vào cấp quyền thứ hai theo phương án của sáng chế. Phương pháp có thể được áp dụng với hệ thống kiểm tra 40 được thể hiện trong FIG.4. Phương pháp này có thể bao gồm các bước sau đây.

S301: thiết bị mạng thu nhận thông tin cấp quyền ASPA.

Một cách tùy chọn, thiết bị mạng đầu tiên có thể thu nhận, từ mạng, bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên mạng, và sau đó xác định ít nhất một đoạn thông tin cấp quyền ASPA dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng thu được.

Đối với phần mô tả của việc xác định, bởi thiết bị mạng, ít nhất một đoạn thông tin cấp quyền ASPA dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng được bộc lộ trên mạng, tham khảo phần mô tả liên quan nêu trên trong

S201. Chi tiết không được mô tả lại ở đây.

S302: thiết bị mạng tạo ra cơ sở dữ liệu đầu vào cấp quyền thứ hai dựa trên thông tin cấp quyền ASPA thu được.

Cụ thể, thiết bị mạng tạo ra cơ sở dữ liệu đầu vào cấp quyền thứ hai dựa trên ít nhất một đoạn thông tin cấp quyền ASPA thu được.

Đối với thông tin cấp quyền ASPA thứ nhất trong ít nhất một đoạn thông tin cấp quyền ASPA, khi địa chỉ IP được sử dụng bởi cặp AS được chỉ báo bởi cặp AS bất kỳ trong thông tin cấp quyền ASPA thứ nhất là địa chỉ IP IPv4, thông tin cấp quyền ASPA thứ nhất được sử dụng để tạo ra cơ sở dữ liệu con đầu vào cấp quyền thứ ba trong cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Tương tự, khi địa chỉ IP được sử dụng bởi cặp AS được chỉ báo bởi cặp AS bất kỳ trong thông tin cấp quyền ASPA thứ nhất trong địa chỉ IP IPv6, thông tin cấp quyền ASPA thứ nhất được sử dụng để tạo ra cơ sở dữ liệu con đầu vào cấp quyền thứ tư trong cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Đối với phần mô tả của cơ sở dữ liệu đầu vào cấp quyền thứ hai, tham khảo phần mô tả nêu trên của cơ sở dữ liệu đầu vào cấp quyền. Chi tiết không được mô tả lại ở đây.

Tóm lại, phương án của sáng chế đề xuất phương pháp kiểm tra cặp AS. Theo phương pháp này, ký hiệu nhận dạng vùng của vùng mà mỗi cặp AS thuộc về được bổ sung vào cơ sở dữ liệu đầu vào cấp quyền được sử dụng để kiểm tra cặp AS. Điều này có thể tránh trường hợp trong đó hiệu lực của đường truyền AS được chỉ báo bởi thông tin đường truyền trong thông tin định tuyến BGP được xác định không chính xác do quan hệ kinh doanh giữa cặp AS trong thông tin đường truyền được xác định không chính xác khi hiệu lực của đường truyền AS được kiểm tra theo nguyên tắc thung lũng tự do. Do đó, phương pháp kiểm tra cặp AS được đề xuất trong phương án này của sáng chế cải thiện độ chính xác kiểm tra đường truyền AS được chỉ báo bởi thông tin đường truyền bao gồm cặp AS.

Phần nêu trên chủ yếu mô tả, từ quan điểm phương pháp, các giải pháp được đề xuất trong các phương án của sáng chế. Để thực hiện các chức năng nêu trên, các cấu trúc phần cứng và/hoặc các môđun phần mềm tương ứng để thực hiện các chức năng này được bao gồm. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật cần hiểu rằng, kết hợp với các bộ phận và các bước thuật toán trong các ví dụ được mô tả trong các phương án được bộc lộ trong bản mô tả này, sáng chế có thể được thực hiện bởi phần cứng hoặc kết hợp của phần cứng và phần mềm máy tính. Việc chức năng được thực hiện bởi phần cứng hoặc phần cứng được điều khiển bởi phần mềm máy tính phụ thuộc vào các ứng dụng và các điều kiện thiết kế cụ thể của các giải pháp kỹ thuật. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể sử dụng các phương pháp khác nhau để thực hiện các chức năng được mô tả đối với mỗi ứng dụng cụ thể, nhưng sẽ không được xem rằng cách thức thực hiện này vượt quá phạm vi của sáng chế.

Theo các phương án của sáng chế, thiết bị kiểm tra cặp AS có thể được chia thành môđun chức năng dựa trên các ví dụ phương pháp nêu trên. Ví dụ, mỗi môđun chức năng có thể thu được thông qua việc phân chia dựa trên mỗi chức năng tương ứng, hoặc hai chức năng hoặc nhiều hơn có thể được tích hợp vào một môđun xử lý. Môđun được tích hợp có thể được thực hiện dưới dạng phần cứng, hoặc có thể được thực hiện dưới dạng môđun chức năng phần mềm. Lưu ý rằng, theo các phương án của sáng chế, việc phân chia thành các môđun chỉ là ví dụ và chỉ là sự phân chia chức năng logic, và có thể là sự phân chia khác trong cách thức thực hiện thực tế.

Như được thể hiện trong FIG.10, FIG.10 là sơ đồ giản lược của cấu trúc thiết bị kiểm tra cặp AS 100 theo phương án của sáng chế. Thiết bị 100 có thể được áp dụng với thiết bị mạng, và được cấu hình để thực hiện phương pháp kiểm tra cặp AS nêu trên, ví dụ, được cấu hình để thực hiện phương pháp được thể hiện trong FIG.5. Thiết bị 100 có thể bao gồm bộ thu nhận 101 và bộ xử lý 102.

Bộ thu nhận 101 được cấu hình để thu nhận thông tin đường truyền,

trong đó thông tin đường truyền bao gồm cặp AS, và cặp AS trong thông tin đường truyền bao gồm hai số AS liền kề trong thông tin đường truyền. Bộ xử lý 102 được cấu hình để: xác định thông tin vùng của vùng mà cặp AS thuộc về, và kiểm tra cặp AS dựa trên thông tin vùng của vùng mà cặp AS thuộc về.

Theo một ví dụ, viện dẫn tới FIG.5, bộ thu nhận 101 có thể được cấu hình để thực hiện S101, và bộ xử lý 102 có thể được cấu hình để thực hiện S102 và S103.

Một cách tùy chọn, bộ xử lý 102 được cấu hình cụ thể để kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S103.

Một cách tùy chọn, bộ xử lý 102 được cấu hình cụ thể để: khi cơ sở dữ liệu đầu vào cấp quyền bao gồm đầu vào cấp quyền mà bao gồm cặp AS và ký hiệu nhận dạng vùng tương ứng với thông tin vùng của vùng mà cặp AS thuộc về, xác định rằng cặp AS được kiểm tra thành công.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S103.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình riêng để: khi cơ sở dữ liệu đầu vào cấp quyền không bao gồm đầu vào cấp quyền mà bao gồm cặp AS và ký hiệu nhận dạng vùng tương ứng với thông tin vùng của vùng mà cặp AS thuộc về, xác định rằng cặp AS không được kiểm tra.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S103.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình để: xác định, từ thông tin định tuyến bao gồm thông tin đường truyền, thông tin vùng của vùng mà cặp AS thuộc về; hoặc xác định, dựa trên tiền tố trong thông tin định tuyến, thông tin vùng của vùng mà cặp AS thuộc về.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S103.

Một cách tùy chọn, bộ thu nhận 101 còn được cấu hình để thu nhận cơ sở dữ liệu đầu vào cấp quyền.

Theo một ví dụ, viện dẫn tới FIG.6, bộ thu nhận 101 có thể được cấu hình để thực hiện S203.

Một cách tùy chọn, cơ sở dữ liệu đầu vào cấp quyền bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ nhất. Thiết bị 100 còn bao gồm: bộ thu 103, được cấu hình để thu bản tin đơn vị dữ liệu giao thức (PDU) từ máy chủ, trong đó bản tin PDU bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước và ký hiệu nhận dạng vùng của vùng mà cặp AS có quan hệ kinh doanh được thiết lập trước thuộc về. Bộ xử lý 102 còn được cấu hình để tạo ra cơ sở dữ liệu đầu vào cấp quyền thứ nhất dựa trên bản tin PDU thu được.

Theo một ví dụ, viện dẫn tới FIG.6, bộ thu 103 và bộ xử lý 102 có thể được cấu hình để thực hiện S203.

Một cách tùy chọn, cơ sở dữ liệu đầu vào cấp quyền còn bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ hai. Bộ xử lý 102 còn được cấu hình để tạo ra cơ sở dữ liệu đầu vào cấp quyền thứ hai dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng. Bảng định tuyến mạng và/hoặc dữ liệu mạng bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước và thông tin vùng của vùng mà cặp AS có quan hệ kinh doanh được thiết lập trước thuộc về.

Theo một ví dụ, viện dẫn tới FIG.9, bộ xử lý 102 có thể được cấu hình để thực hiện S302.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình riêng để: kiểm tra cặp AS dựa trên thông tin vùng của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền thứ nhất; và nếu cặp AS không được kiểm tra, kiểm tra cặp AS dựa trên thông tin vùng của vùng mà cặp AS thuộc về và cơ sở dữ liệu đầu vào cấp quyền thứ hai.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S103.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình riêng để kiểm tra cặp AS dựa trên thông tin vùng của vùng mà cặp AS thuộc về và đầu vào cấp quyền đích mà ở trong cơ sở dữ liệu đầu vào cấp quyền và tương ứng với tiền tố trong thông tin đường truyền, trong đó phiên bản IP của cặp AS trong đầu vào cấp quyền đích là giống như phiên bản IP trong tiền tố trong thông tin đường truyền.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S103.

Một cách tùy chọn, thông tin đường truyền bao gồm các số AS được sắp xếp theo thứ tự thiết lập trước, và các số AS được sử dụng để chỉ báo đường truyền tương ứng với thông tin đường truyền. Bộ xử lý 102 còn được cấu hình để kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền, để kiểm tra đường truyền tương ứng với thông tin đường truyền.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S104.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình để: khi cặp AS trong thông tin đường truyền không được kiểm tra trong lần đầu tiên, đảo ngược cặp AS mà chưa được kiểm tra trong thông tin đường truyền. Bộ xử lý 102 còn được cấu hình để kiểm tra cặp AS được đảo ngược, để hoàn thành việc kiểm tra đường truyền tương ứng với thông tin đường truyền.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S104.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình để: nếu thông tin đường truyền bao gồm nhiều nhất một cặp AS mà không được kiểm tra, xác định rằng đường truyền tương ứng với thông tin đường truyền được kiểm tra thành công.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S104.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình để tạo ra đầu vào chuyển tiếp thứ nhất dựa trên thông tin đường truyền.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S106.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình để: nếu thông tin đường truyền bao gồm ít nhất hai cặp AS mà không được kiểm tra, xác định rằng đường truyền tương ứng với thông tin đường truyền không được kiểm tra.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S104.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình để tạo ra đầu vào chuyển tiếp thứ hai dựa trên thông tin đường truyền. Bộ xử lý 102 còn được cấu hình để đánh dấu thông tin cụ thể cho đầu vào chuyển tiếp thứ hai, trong đó thông tin cụ thể được sử dụng để chỉ báo liệu đầu vào chuyển tiếp thứ hai là đầu vào chuyển tiếp rủi ro cao hoặc đầu vào chuyển tiếp ưu tiên thấp.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S106.

Một cách tùy chọn, thiết bị mạng là thiết bị mạng trong AS thứ nhất. Thiết bị 100 còn bao gồm: bộ gửi 104, được cấu hình để gửi kết quả kiểm tra của đường truyền tương ứng với thông tin đường truyền đến thiết bị đích. Thiết bị đích là thiết bị mà ở trong AS thứ nhất và được kết nối với thiết bị mạng để truyền thông.

Theo một ví dụ, viện dẫn tới FIG.5, bộ gửi 104 có thể được cấu hình để thực hiện S105.

Một cách tùy chọn, bộ thu nhận 101 được cấu hình cụ thể để thu nhận bản tin cập nhật giao thức cổng biên (BGP), trong đó bản tin cập nhật BGP bao gồm thông tin đường truyền.

Theo một ví dụ, viện dẫn tới FIG.5, bộ thu nhận 101 có thể được cấu hình để thực hiện S101.

Một cách tùy chọn, bộ xử lý 102 còn được cấu hình để: sau khi bản tin cập nhật BGP được thu, kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra đường truyền tương ứng với thông tin đường truyền. Theo cách khác, bộ xử lý 102 được cấu hình để: trước khi bản tin cập nhật BGP được gửi, kiểm tra cặp AS trong thông tin đường truyền trong bản tin cập nhật BGP, để kiểm tra đường truyền tương ứng với thông tin đường truyền.

Theo một ví dụ, viện dẫn tới FIG.5, bộ xử lý 102 có thể được cấu hình để thực hiện S103 và S104.

Đối với các phần mô tả cụ thể của các cách thức tùy chọn, tham khảo các phương án phương pháp. Chi tiết không được mô tả lại ở đây. Ngoài ra, đối với sự giải thích bất kỳ về thiết bị 100 được đề xuất ở trên và các phần mô tả hiệu quả có lợi, tham khảo các phương án phương pháp tương ứng nêu trên. Chi tiết không được mô tả lại ở đây.

Theo một ví dụ, viện dẫn tới FIG.3, các chức năng của bộ thu nhận 101 và bộ xử lý 102 của thiết bị 100 có thể được thực hiện bằng cách sử dụng bộ xử lý 31 trên FIG.3 bằng cách thực thi mã chương trình trong bộ nhớ 32 trên FIG.3. Các chức năng của bộ thu 103 và bộ gửi 104 có thể được thực hiện bằng cách sử dụng giao diện truyền thông 3 trên FIG.3.

Phương án của sáng chế còn đề xuất hệ thống chip 110. Như được thể hiện trong FIG.11, hệ thống chip 110 bao gồm ít nhất một bộ xử lý và ít nhất một mạch giao diện.

Theo một ví dụ, khi hệ thống chip 110 bao gồm một bộ xử lý và một mạch giao diện, bộ xử lý có thể là bộ xử lý 111 được thể hiện trong hộp đường nét liền (hoặc bộ xử lý 111 được thể hiện trong hộp đường nét đứt) trên FIG.11, và mạch giao diện có thể là mạch giao diện 112 được thể hiện trong hộp đường nét liền (hoặc mạch giao diện 112 được thể hiện trong hộp nét đứt) trên FIG.11.

Khi hệ thống chip 110 bao gồm hai bộ xử lý và hai mạch giao diện, hai bộ xử lý bao gồm bộ xử lý 111 được thể hiện trong hộp đường nét liền và bộ xử lý 111 được thể hiện trong hộp đường nét đứt trên FIG.11, và hai mạch giao diện bao gồm mạch giao diện 112 được thể hiện trong hộp đường nét liền và mạch giao diện 112 được thể hiện trong hộp đường nét đứt trên FIG.11. Điều này không bị giới hạn ở đây.

Bộ xử lý 111 và mạch giao diện 112 có thể được kết nối với nhau thông qua đường dây. Ví dụ, mạch giao diện 112 có thể được cấu hình để thu tín hiệu (ví dụ, thu nhận thông tin vùng của vùng mà cặp AS thuộc về, hoặc thu bản tin PDU từ máy chủ). Theo ví dụ khác, mạch giao diện 112 có thể được cấu hình để gửi tín hiệu tới thiết bị khác (ví dụ, bộ xử lý 111).

Ví dụ, mạch giao diện 112 có thể đọc các lệnh được lưu trữ trong bộ nhớ, và gửi các lệnh tới bộ xử lý 111. Khi các lệnh được thực thi bởi bộ xử lý 111, thiết bị kiểm tra cặp AS được cho phép thực hiện các bước trong các phương án nêu trên. Chắc chắn là, hệ thống chip 110 có thể còn bao gồm thiết bị rời rạc khác. Điều này không bị giới hạn cụ thể trong phương án này của sáng chế.

Phương án khác của sáng chế còn đề xuất phương tiện lưu trữ đọc được bởi máy tính. Phương tiện lưu trữ đọc được bởi máy tính lưu trữ lệnh. Khi các lệnh được chạy trên thiết bị kiểm tra cặp AS, thiết bị kiểm tra cặp AS thực hiện các bước được thực hiện bởi thiết bị kiểm tra cặp AS trong các bước của phương pháp được thể hiện trong các phương án phương pháp nêu trên.

Trong một số phương án, phương pháp được bộc lộ có thể được thực hiện như là các lệnh chương trình máy tính được mã hóa theo định dạng có thể đọc được bằng máy trên phương tiện lưu trữ đọc được bởi máy tính hoặc được mã hóa trên sản phẩm hoặc phương tiện lưu trữ không tạm thời khác.

FIG.12 thể hiện giản lược hình vẽ khái niệm một phần của sản phẩm chương trình máy tính theo phương án của sáng chế. Sản phẩm chương trình máy tính bao gồm chương trình máy tính được sử dụng để thực thi xử lý máy

tính trên thiết bị máy tính.

Trong phương án, sản phẩm chương trình máy tính được đề xuất bằng cách sử dụng phương tiện kênh mang tín hiệu 120. Phương tiện kênh mang tín hiệu 120 có thể bao gồm một hoặc nhiều lệnh chương trình. Khi một hoặc nhiều lệnh chương trình được chạy bởi một hoặc nhiều bộ xử lý, các chức năng hoặc một số chức năng được mô tả trên FIG.5 có thể được đề xuất. Do đó, ví dụ, một hoặc nhiều dấu hiệu được mô tả viện dẫn tới S101 đến S106 trên FIG.5 có thể được sinh ra bởi một hoặc nhiều lệnh được kết hợp với phương tiện kênh mang tín hiệu 120. Ngoài ra, các lệnh chương trình trên FIG.12 cũng được mô tả như là các lệnh ví dụ.

Trong một số ví dụ, phương tiện kênh mang tín hiệu 120 có thể bao gồm phương tiện đọc được bởi máy tính 121, ví dụ, nhưng không giới hạn ở, ổ đĩa cứng, đĩa nén (CD), đĩa video số (DVD), băng số, bộ nhớ, bộ nhớ chỉ đọc (read-only memory, ROM), hoặc bộ nhớ truy nhập ngẫu nhiên (random access memory, RAM).

Trong một số cách thức thực hiện, phương tiện kênh mang tín hiệu 120 có thể bao gồm phương tiện ghi được bằng máy tính 122, ví dụ, nhưng không giới hạn ở, bộ nhớ, CD đọc/viết (R/W), hoặc R/W DVD.

Trong một số cách thức thực hiện, phương tiện kênh mang tín hiệu 120 có thể bao gồm phương tiện truyền thông 123, ví dụ, nhưng không giới hạn ở, phương tiện truyền thông tương tự và/hoặc số (ví dụ, sợi quang, ống dẫn sóng, liên kết truyền thông nối dây, hoặc liên kết truyền thông không dây).

Phương tiện kênh mang tín hiệu 120 có thể được vận chuyển bởi phương tiện truyền thông 123 ở dạng không dây (ví dụ, phương tiện truyền thông không dây mà đáp ứng tiêu chuẩn IEEE 1202.11 hoặc giao thức vận tải khác). Một hoặc nhiều lệnh chương trình có thể là, ví dụ, một hoặc nhiều lệnh có thể thực thi bằng máy tính hoặc một hoặc nhiều lệnh thực hiện logic.

Trong một số ví dụ, thiết bị kiểm tra cặp AS được mô tả viện dẫn tới FIG.5 có thể được cấu hình để cung cấp các thao tác khác nhau, các chức năng,

hoặc các hành động đáp lại một hoặc nhiều lệnh chương trình trong phương tiện đọc được bằng máy tính 121, phương tiện ghi được bằng máy tính 122, và/hoặc phương tiện truyền thông 123.

Sẽ được hiểu rằng cách bố trí được mô tả ở đây chỉ được sử dụng làm ví dụ. Do đó, người có hiểu biết trung bình trong lĩnh vực kỹ thuật hiểu rằng cách bố trí khác và phần tử khác (ví dụ, máy, giao diện, chức năng, trình tự, và nhóm chức năng) có thể được sử dụng làm các thay thế, và một số phần tử có thể được bỏ qua tùy thuộc vào kết quả mong đợi.

Ngoài ra, nhiều phần tử được mô tả là các thực thể chức năng mà có thể được thực hiện như là các thành phần được phân bố hoặc rời rạc, hoặc được thực hiện trong kết hợp thích hợp bất kỳ ở vị trí thích hợp bất kỳ kết hợp với thành phần khác.

Tất cả hoặc một số phương án có thể được thực hiện bằng cách sử dụng phần mềm, phần cứng, phần sụn, hoặc kết hợp bất kỳ của chúng. Khi chương trình phần mềm được sử dụng để thực hiện các phương án, tất cả hoặc một vài phương án có thể được thực hiện trong dạng của sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính bao gồm một hoặc nhiều lệnh máy tính. Khi các lệnh có thể thực thi bởi máy tính được thực thi trên máy tính, các thủ tục hoặc các chức năng theo các phương án của sáng chế đều tất cả hoặc một phần được tạo ra.

Máy tính có thể là máy tính mục đích chung, máy tính chuyên dụng, mạng máy tính, hoặc thiết bị khả trình khác. Các lệnh máy tính có thể được lưu trữ trong phương tiện lưu trữ đọc được bởi máy tính, hoặc có thể được truyền từ phương tiện lưu trữ đọc được bởi máy tính tới phương tiện lưu trữ đọc được bởi máy tính khác. Ví dụ, các lệnh máy tính có thể được truyền từ trang mạng, máy tính, máy chủ, hoặc trung tâm dữ liệu tới trang mạng khác, máy tính khác, máy chủ khác, hoặc trung tâm dữ liệu khác theo cách thức có dây (ví dụ, cáp đồng trục, cáp quang, hoặc đường dây thuê bao số (digital subscriber line, DSL)) hoặc cách thức không dây (ví dụ, hồng ngoại, vô tuyến, hoặc sóng viba).

Phương tiện lưu trữ đọc được bằng máy tính có thể là phương tiện có thể sử dụng được bất kỳ có thể truy nhập được bởi máy tính, hoặc thiết bị lưu trữ dữ liệu, ví dụ máy chủ hoặc trung tâm dữ liệu, mà tích hợp một hoặc nhiều phương tiện có thể sử dụng được. Phương tiện có thể được sử dụng có thể là phương tiện từ (ví dụ, đĩa mềm, đĩa cứng, hoặc băng từ), phương tiện quang (ví dụ, DVD), phương tiện bán dẫn (ví dụ, ổ bán dẫn (SSD-solid state drive)), hoặc loại tương tự.

Phần mô tả nêu trên chỉ là các phương án cụ thể của sáng chế, nhưng không nhằm mục đích giới hạn phạm vi bảo hộ của sáng chế. Bất kỳ thay đổi hoặc thay thế được thực hiện bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật nằm trong phạm vi kỹ thuật được bộc lộ trong sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế. Do đó, phạm vi bảo hộ của sáng chế sẽ được đưa vào phạm vi bảo hộ của yêu cầu bảo hộ.

YÊU CẦU BẢO HỘ

1. Phương pháp kiểm tra cặp hệ thống tự trị (AS - autonomous system), được áp dụng với thiết bị mạng, trong đó phương pháp này bao gồm:

thu nhận thông tin đường truyền, trong đó thông tin đường truyền bao gồm cặp AS, cặp AS bao gồm hai số AS liền kề trong thông tin đường truyền, thông tin đường truyền bao gồm nhiều số AS được sắp xếp theo thứ tự được thiết lập trước, và các số AS được sử dụng để chỉ báo đường truyền mà tương ứng với thông tin đường truyền;

xác định thông tin vùng của vùng mà cặp AS thuộc về;

kiểm tra cặp AS dựa trên thông tin vùng và cơ sở dữ liệu đầu vào cấp quyền, trong đó cơ sở dữ liệu đầu vào cấp quyền bao gồm ít nhất một đầu vào cấp quyền, mỗi ít nhất một đầu vào cấp quyền bao gồm ít nhất một cặp AS mà có quan hệ kinh doanh được thiết lập trước và ký hiệu nhận dạng vùng của vùng mà ít nhất một cặp AS mà có quan hệ kinh doanh được thiết lập trước thuộc về; và

khi cơ sở dữ liệu đầu vào cấp quyền bao gồm đầu vào cấp quyền mà bao gồm cặp AS và ký hiệu nhận dạng vùng tương ứng với thông tin vùng, xác định rằng cặp AS được kiểm tra thành công; hoặc

khi cơ sở dữ liệu đầu vào cấp quyền không bao gồm đầu vào cấp quyền mà bao gồm cặp AS và ký hiệu nhận dạng vùng tương ứng với thông tin vùng, xác định rằng cặp AS không được kiểm tra.

2. Phương pháp theo điểm 1, trong đó việc xác định thông tin vùng của vùng mà cặp AS thuộc về bao gồm:

xác định, từ thông tin định tuyến bao gồm thông tin đường truyền, thông tin vùng của vùng mà cặp AS thuộc về; hoặc

xác định, dựa trên tiền tố trong thông tin định tuyến, thông tin vùng của vùng mà cặp AS thuộc về.

3. Phương pháp theo điểm 1 hoặc 2, trong đó trước khi việc kiểm tra cặp AS dựa trên thông tin vùng và cơ sở dữ liệu đầu vào cấp quyền, phương pháp này còn bao gồm:

thu nhận cơ sở dữ liệu đầu vào cấp quyền.

4. Phương pháp theo điểm 3, trong đó cơ sở dữ liệu đầu vào cấp quyền bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ nhất; và bước thu nhận cơ sở dữ liệu đầu vào cấp quyền bao gồm:

thu bản tin đơn vị dữ liệu giao thức (PDU) từ máy chủ, trong đó bản tin PDU bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước và ký hiệu nhận dạng vùng của vùng mà cặp AS có quan hệ kinh doanh được thiết lập trước thuộc về; và

tạo cơ sở dữ liệu đầu vào cấp quyền thứ nhất dựa trên bản tin PDU.

5. Phương pháp theo điểm 4, trong đó cơ sở dữ liệu đầu vào cấp quyền còn bao gồm cơ sở dữ liệu đầu vào cấp quyền thứ hai; và bước thu nhận cơ sở dữ liệu đầu vào cấp quyền bao gồm:

tạo cơ sở dữ liệu đầu vào cấp quyền thứ hai dựa trên bảng định tuyến mạng và/hoặc dữ liệu mạng, trong đó

bảng định tuyến mạng và/hoặc dữ liệu mạng bao gồm cặp AS có quan hệ kinh doanh được thiết lập trước và thông tin vùng của vùng mà cặp AS có quan hệ kinh doanh được thiết lập trước thuộc về.

6. Phương pháp theo điểm 5, trong đó việc kiểm tra cặp AS dựa trên thông tin vùng và cơ sở dữ liệu đầu vào cấp quyền bao gồm:

kiểm tra cặp AS dựa trên thông tin vùng và cơ sở dữ liệu đầu vào cấp quyền thứ nhất; và

nếu cặp AS không được kiểm tra, kiểm tra cặp AS dựa trên thông tin vùng và cơ sở dữ liệu đầu vào cấp quyền thứ hai.

7. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 2 và 4 đến 6, trong

đó việc kiểm tra cặp AS dựa trên thông tin vùng và cơ sở dữ liệu đầu vào cấp quyền bao gồm:

kiểm tra cặp AS dựa trên thông tin vùng và đầu vào cấp quyền đích mà ở trong cơ sở dữ liệu đầu vào cấp quyền và tương ứng với tiền tố trong thông tin đường truyền, trong đó phiên bản giao thức internet (internet protocol, IP) của cặp AS trong đầu vào cấp quyền đích là giống như phiên bản IP trong tiền tố trong thông tin đường truyền.

8. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 2 và 4 đến 6, trong đó phương pháp này còn bao gồm:

kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền, để kiểm tra đường truyền tương ứng với thông tin đường truyền.

9. Phương pháp theo điểm 8, trong đó phương pháp này còn bao gồm:

khi cặp AS trong thông tin đường truyền không được kiểm tra trong lần đầu tiên, đảo ngược cặp AS mà chưa được kiểm tra trong thông tin đường truyền; và

kiểm tra cặp AS được đảo ngược, để hoàn thành việc kiểm tra đường truyền tương ứng với thông tin đường truyền.

10. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 2, 4 đến 6 và 9, trong đó phương pháp này còn bao gồm:

nếu thông tin đường truyền bao gồm nhiều nhất một cặp AS mà không được kiểm tra, xác định rằng đường truyền tương ứng với thông tin đường truyền được kiểm tra thành công.

11. Phương pháp theo điểm 10, trong đó phương pháp này còn bao gồm:

tạo đầu vào chuyển tiếp thứ nhất dựa trên thông tin đường truyền.

12. Phương pháp theo điểm 9 hoặc 11, trong đó phương pháp này còn bao gồm:

nếu thông tin đường truyền bao gồm ít nhất hai cặp AS mà không được kiểm tra, xác định rằng đường truyền tương ứng với thông tin đường truyền không được kiểm tra.

13. Phương pháp theo điểm 12, trong đó phương pháp này còn bao gồm:

tạo đầu vào chuyển tiếp thứ hai dựa trên thông tin đường truyền; và

đánh dấu thông tin cụ thể cho đầu vào chuyển tiếp thứ hai, trong đó thông tin cụ thể được sử dụng để chỉ báo liệu đầu vào chuyển tiếp thứ hai là đầu vào chuyển tiếp rủi ro cao hoặc đầu vào chuyển tiếp ưu tiên thấp.

14. Phương pháp theo điểm bất kỳ trong số các điểm 9, 11 và 13, trong đó thiết bị mạng là thiết bị mạng trong AS thứ nhất; và phương pháp này còn bao gồm:

gửi kết quả kiểm tra của đường truyền tương ứng với thông tin đường truyền đến thiết bị đích, trong đó thiết bị đích là thiết bị mà ở trong AS thứ nhất và được kết nối với thiết bị mạng để truyền thông.

15. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 2, 4 đến 6, 9, 11 và 13, trong đó bước thu nhận thông tin đường truyền bao gồm:

thu nhận bản tin cập nhật giao thức cổng biên (border gateway protocol, BGP), trong đó bản tin cập nhật BGP bao gồm thông tin đường truyền.

16. Phương pháp theo điểm 15, trong đó phương pháp này còn bao gồm:

sau khi thu bản tin cập nhật BGP, kiểm tra cặp AS trong thông tin đường truyền, để kiểm tra đường truyền tương ứng với thông tin đường truyền; hoặc

trước khi gửi bản tin cập nhật BGP, kiểm tra cặp AS trong thông tin đường truyền, để kiểm tra đường truyền tương ứng với thông tin đường truyền.

17. Thiết bị kiểm tra cặp hệ thống tự trị (AS), được áp dụng với thiết bị mạng, trong đó thiết bị mạng được cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 16.

18. Phương tiện lưu trữ đọc được bởi máy tính bao gồm các lệnh, các lệnh này, khi chạy trên thiết bị kiểm tra cặp hệ thống tự trị (AS), làm cho thiết bị kiểm tra cặp AS thực hiện phương pháp kiểm tra cặp AS theo điểm bất kỳ trong số các điểm 1 đến 16.

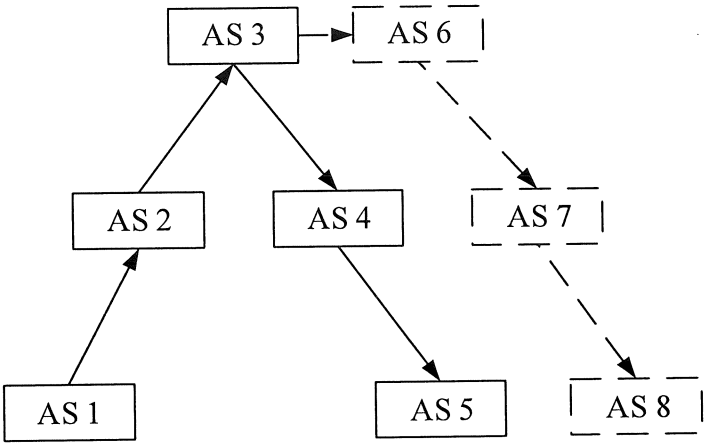

FIG. 1

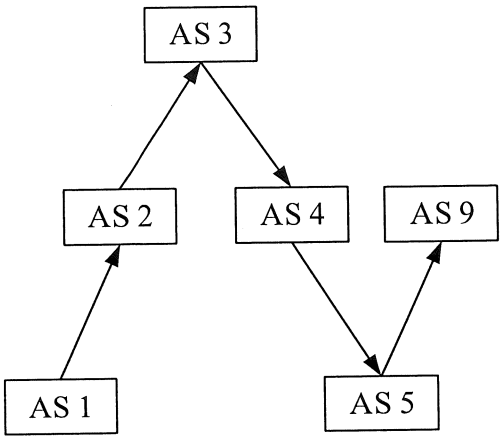

FIG. 2(a)

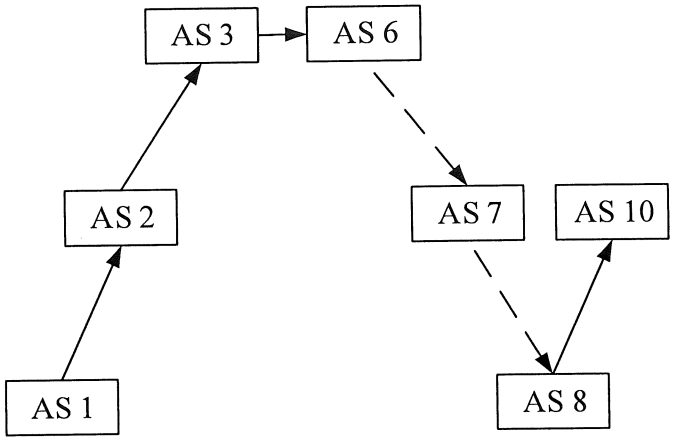

FIG. 2(b)

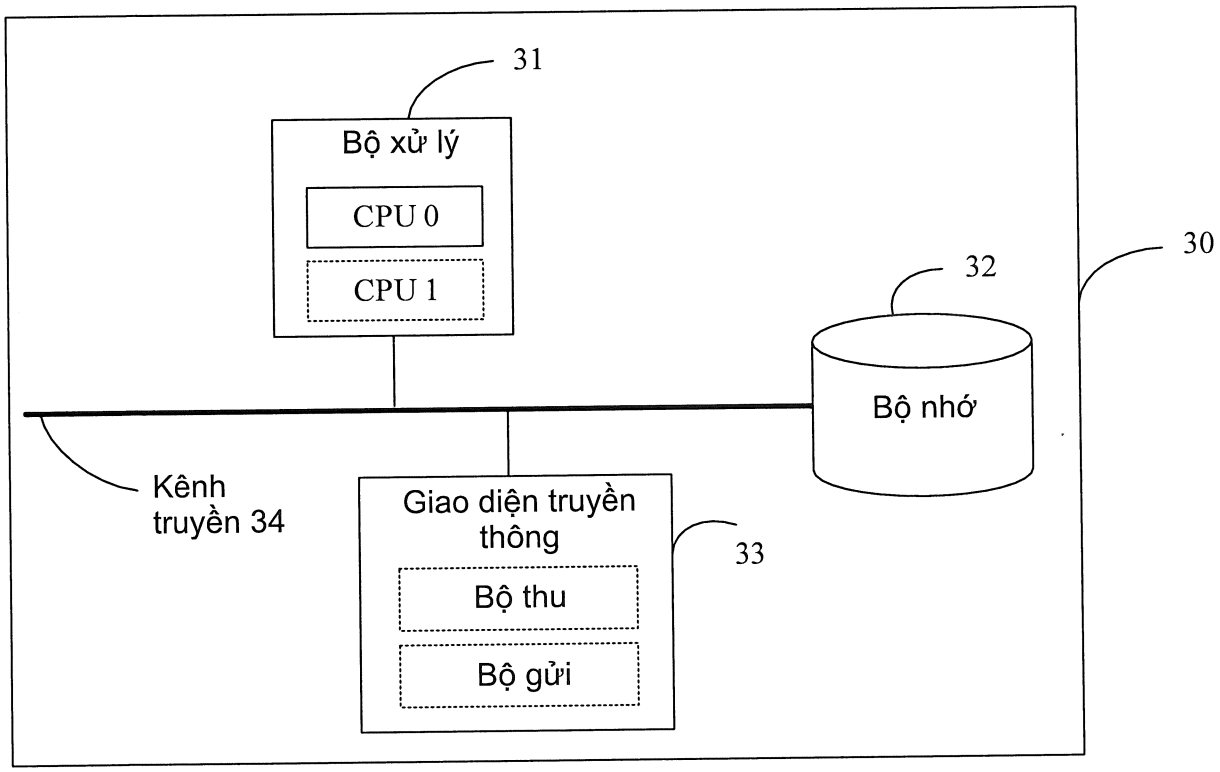
31
Bộ xử lý
CPU 0
CPU 1
30
32
Bộ nhớ
Kênh truyền 34
Giao diện truyền thông
33
Bộ thu
Bộ gửi

FIG. 3

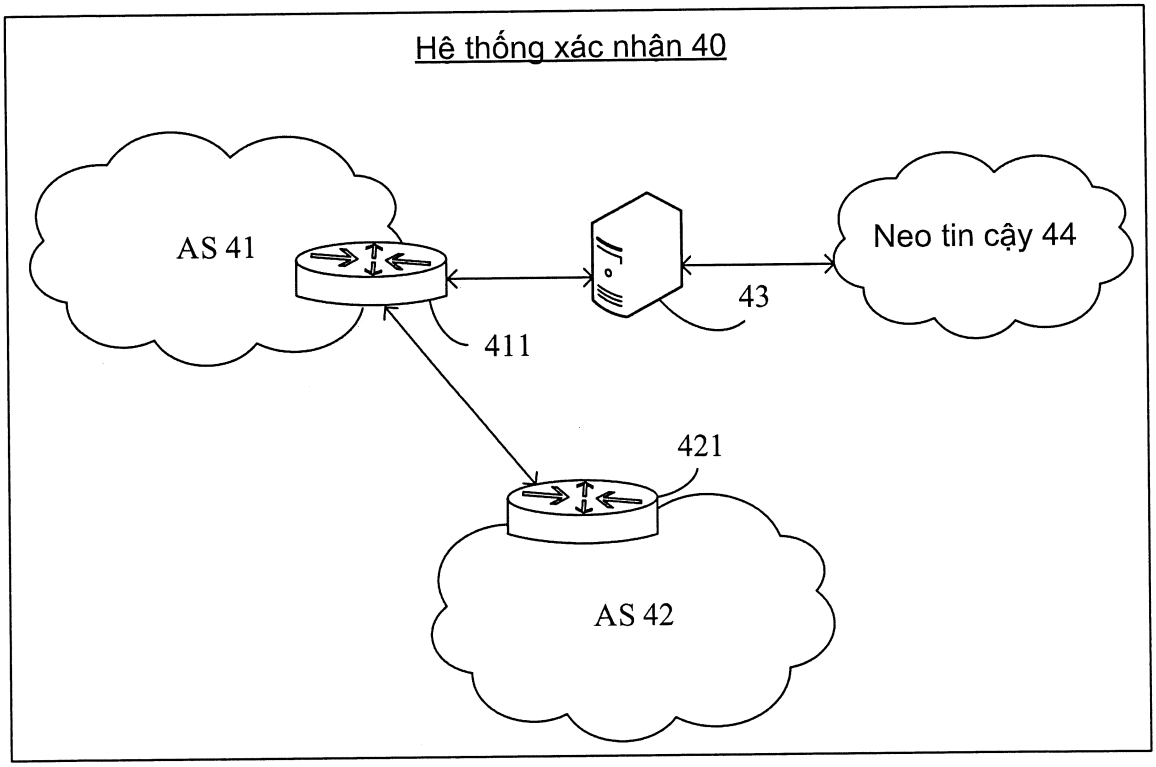
Hệ thống xác nhận 40
AS 41
Neo tin cậy 44
43
411
421
AS 42

FIG. 4

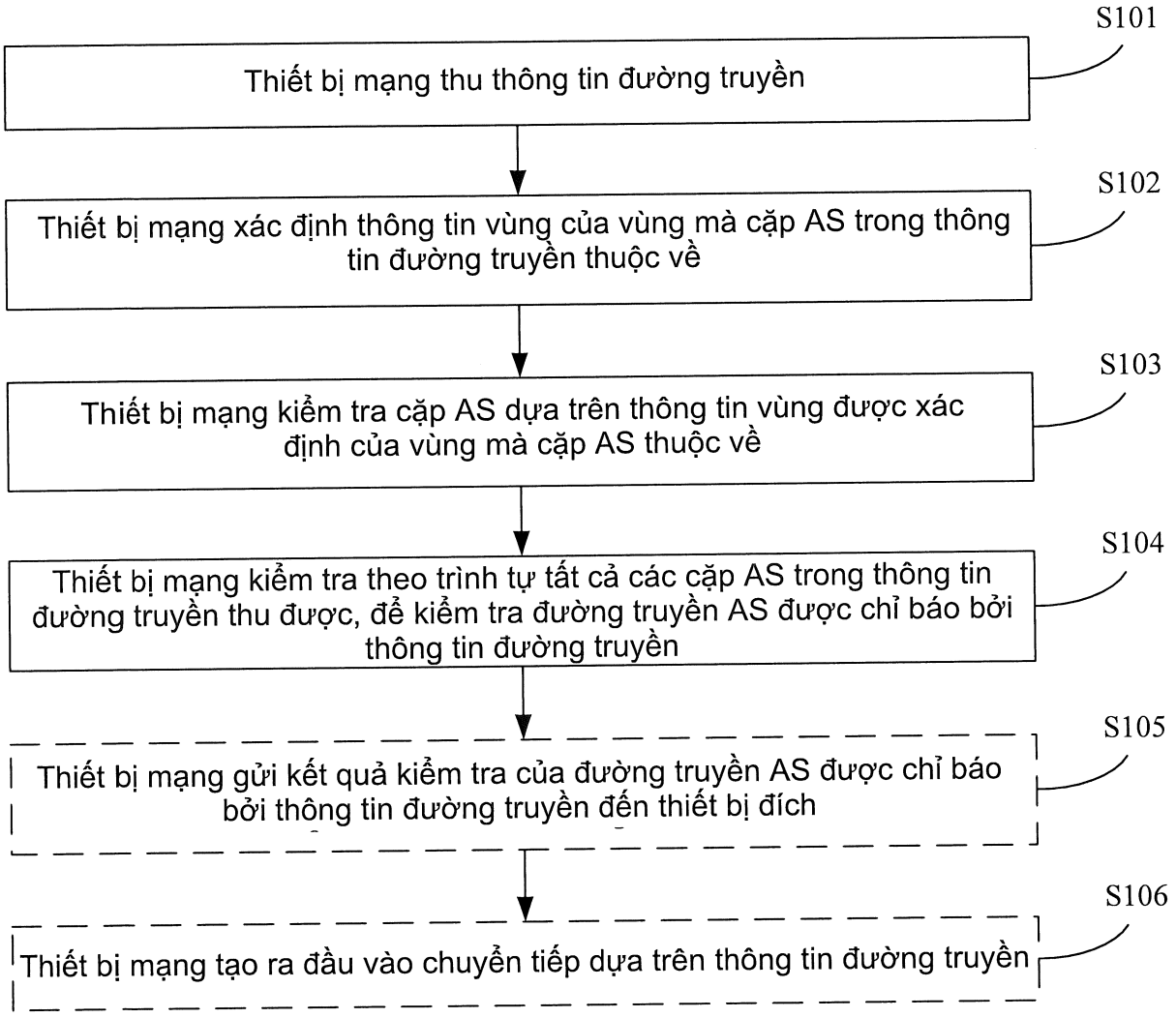
S101
Thiết bị mạng thu thông tin đường truyền
S102
Thiết bị mạng xác định thông tin vùng của vùng mà cặp AS trong thông tin đường truyền thuộc về
S103
Thiết bị mạng kiểm tra cặp AS dựa trên thông tin vùng được xác định của vùng mà cặp AS thuộc về
S104
Thiết bị mạng kiểm tra theo trình tự tất cả các cặp AS trong thông tin đường truyền thu được, để kiểm tra đường truyền AS được chỉ báo bởi thông tin đường truyền
S105
Thiết bị mạng gửi kết quả kiểm tra của đường truyền AS được chỉ báo bởi thông tin đường truyền đến thiết bị đích
S106
Thiết bị mạng tạo ra đầu vào chuyển tiếp dựa trên thông tin đường truyền

FIG. 5

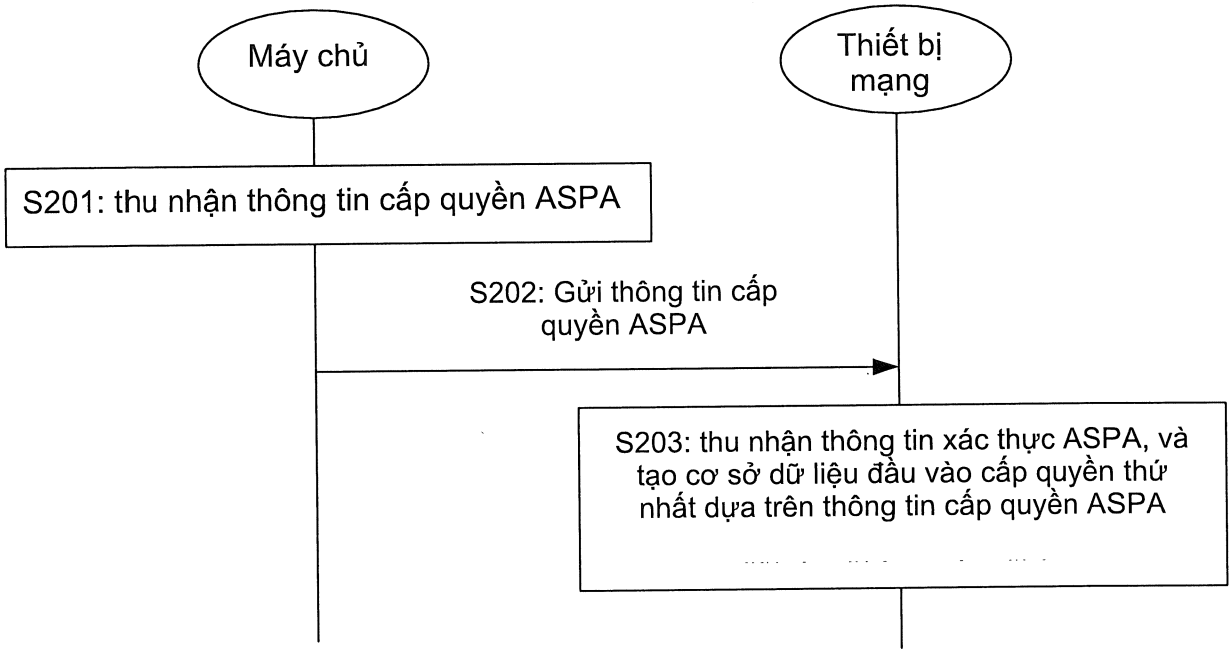
Máy chủ
Thiết bị mạng
S201: thu nhận thông tin cấp quyền ASPA
S202: Gửi thông tin cấp quyền ASPA
S203: thu nhận thông tin xác thực ASPA, và tạo cơ sở dữ liệu đầu vào cấp quyền thứ nhất dựa trên thông tin cấp quyền ASPA

FIG. 6

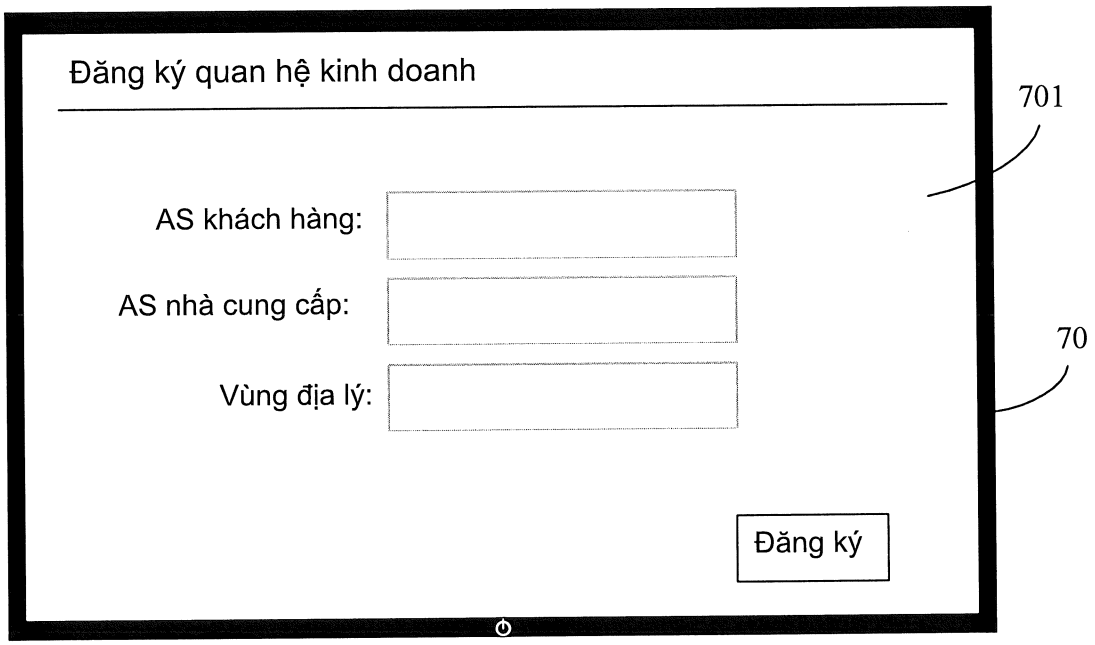
Đăng ký quan hệ kinh doanh
AS khách hàng:
AS nhà cung cấp:
Vùng địa lý:
Đăng ký
701
70

FIG. 7(a)

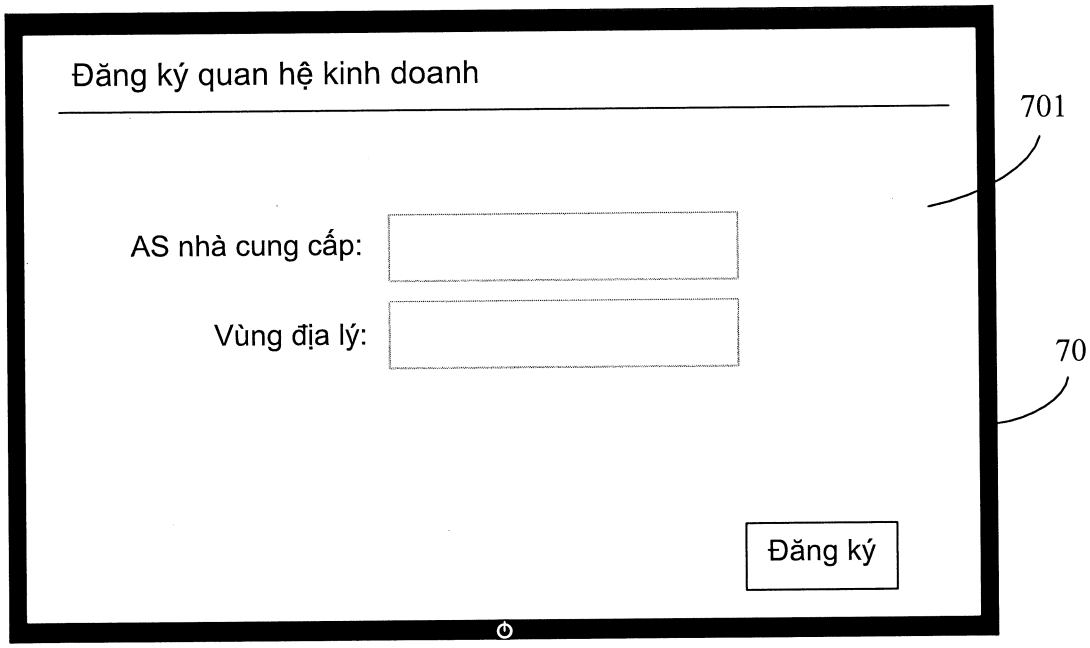
Đăng ký quan hệ kinh doanh
AS nhà cung cấp:
Vùng địa lý:
Đăng ký
701
70

FIG. 7(b)

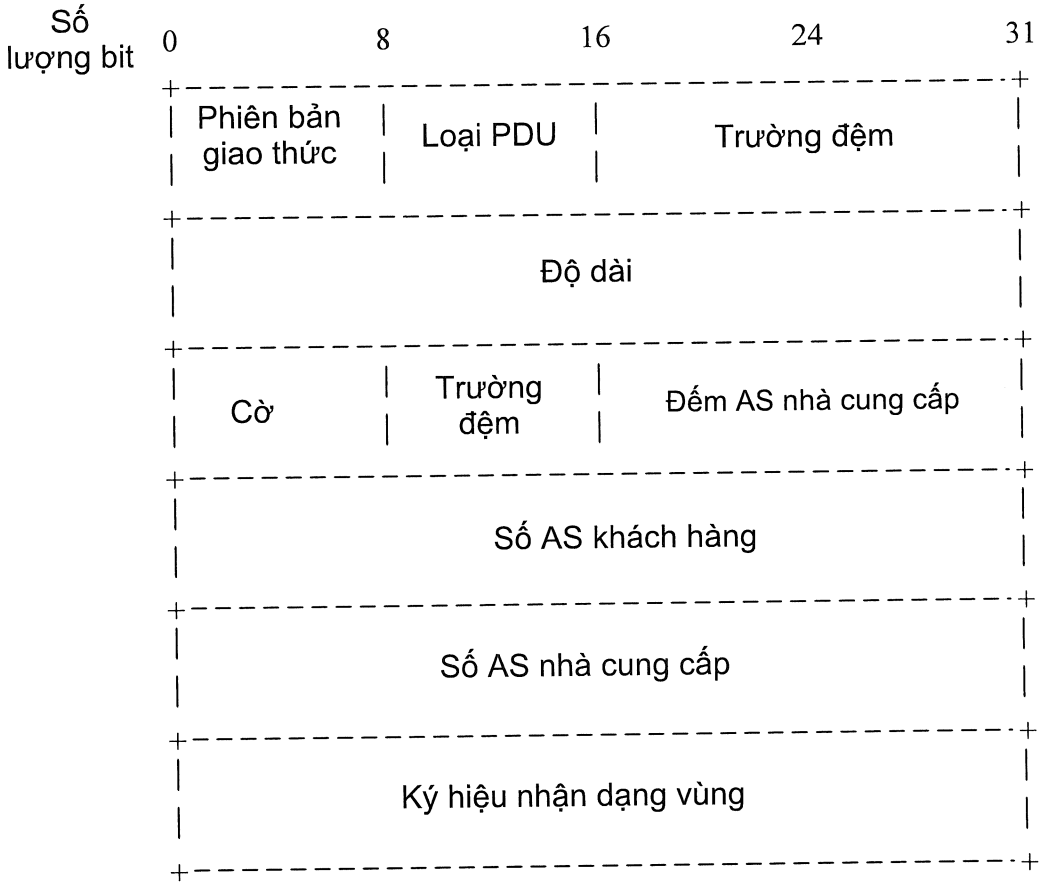
Số lượng bit
0
8
16
24
31
Phiên bản giao thức
Loại PDU
Trường đệm
Độ dài
Cờ
Trường đệm
Đếm AS nhà cung cấp
Số AS khách hàng
Số AS nhà cung cấp
Ký hiệu nhận dạng vùng

FIG. 8

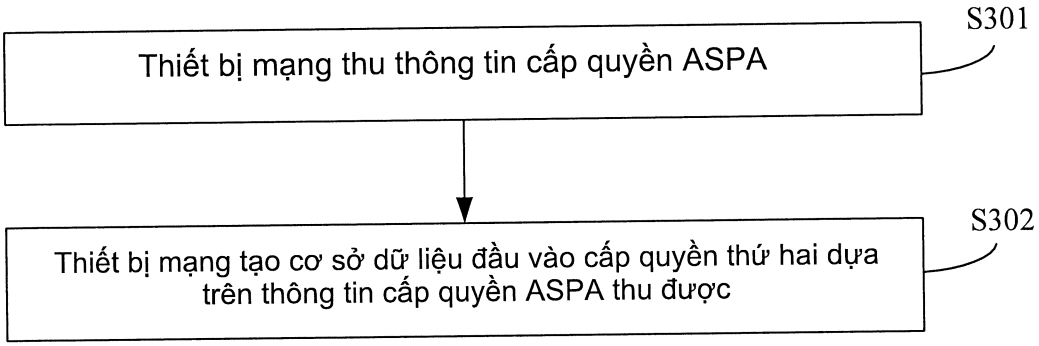
S301
Thiết bị mạng thu thông tin cấp quyền ASPA
S302
Thiết bị mạng tạo cơ sở dữ liệu đầu vào cấp quyền thứ hai dựa trên thông tin cấp quyền ASPA thu được

FIG. 9

7/8

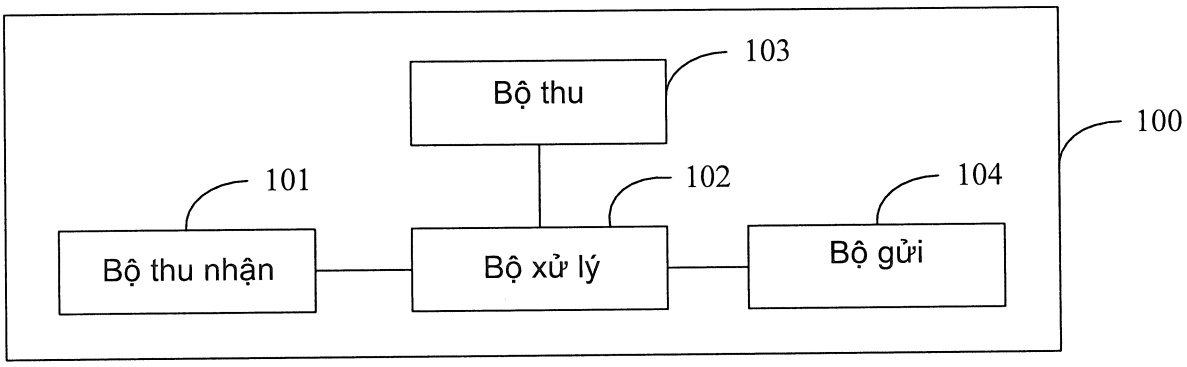

FIG. 10

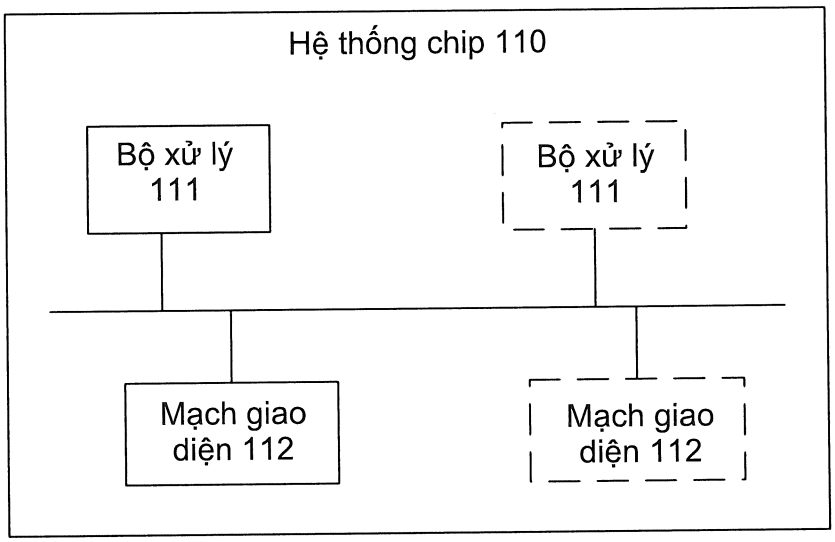

FIG. 11

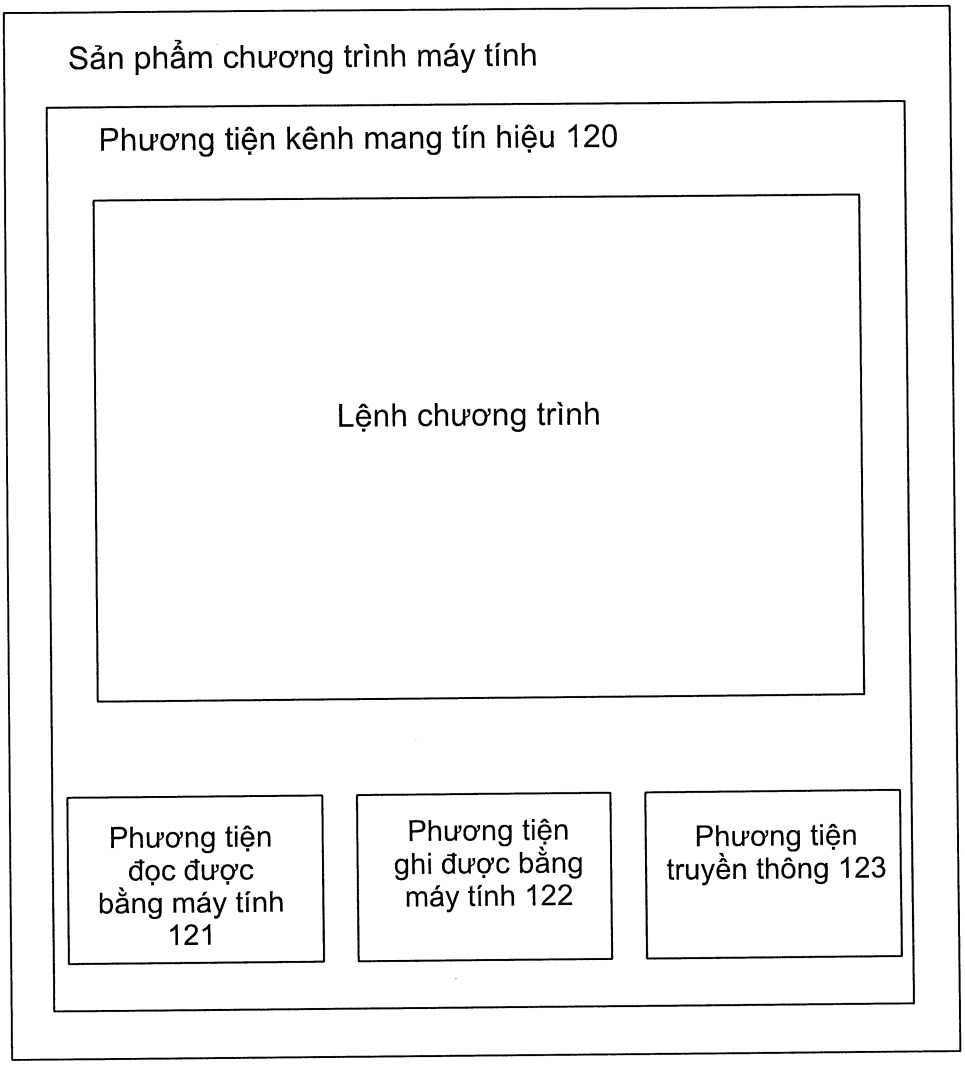
Sản phẩm chương trình máy tính
Phương tiện kênh mang tín hiệu 120
Lệnh chương trình
Phương tiện đọc được bằng máy tính 121
Phương tiện ghi được bằng máy tính 122
Phương tiện truyền thông 123

FIG. 12