(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) **1-0052675**

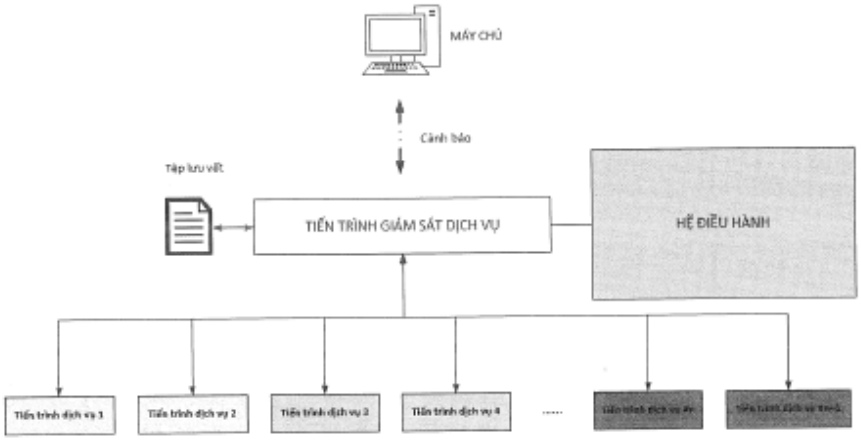
(51)[2021.01] **G06F 15/16**; H04L 29/06; G06F 11/30 (13) **B**

(21) 1-2022-04834 (22) 29/07/2022
(45) 27/10/2025 451 (43) 25/10/2022 415A
(73) Tập đoàn Công nghiệp - Viễn thông Quân đội (VN)
Lô D26 khu đô thị mới Cầu Giấy, phường Yên Hoà, quận Cầu Giấy, thành phố Hà Nội
(72) La Văn Thiện (VN); Trần Văn Hưởng (VN).
(74) Công ty TNHH NACILAW (NACILAW)

(54) PHƯƠNG PHÁP BẢO VỆ CÁC TIẾN TRÌNH DỊCH VỤ TRÊN THIẾT BỊ ĐỊNH TUYẾN TRONG MẠNG TRUYỀN DẪN

(21) 1-2022-04834

(57) Sáng chế đề cập đến phương pháp bảo vệ các tiến trình dịch vụ trên thiết bị định tuyến trong mạng truyền dẫn đang hoạt động trên mạng lưới của nhà cung cấp dịch vụ internet. Việc bảo vệ các tiến trình này vô cùng quan trọng đảm bảo các thông tin chuyển tiếp trên mạng được thông suốt, liên tục, không gián đoạn. Sáng chế được thực hiện trên thiết bị mạng truyền dẫn định tuyến vùng biên. Sáng chế nhằm giúp đảm bảo sự ổn định của các tiến trình dịch vụ cốt lõi trên thiết bị SRT (chuyển tiếp lớp 2, định tuyến lớp 3, định tuyến nhãn, truyền hình, …), từ đó, đảm bảo các dịch vụ như 2G, 3G, 4G, truyền hình số, internet băng rộng không bị gián đoạn.



Hình 1

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp bảo vệ các tiến trình dịch vụ trên thiết bị định tuyến trong mạng truyền dẫn. Cụ thể, phương pháp bảo vệ được đề cập trong sáng chế được ứng dụng để bảo vệ các tiến trình dịch vụ trên thiết bị định tuyến trong mạng truyền dẫn đang hoạt động trên mạng lưới của nhà cung cấp dịch vụ internet.

Tình trạng kỹ thuật của sáng chế

Mạng truyền dẫn của các nhà cung cấp dịch vụ mạng (Internet Service Provider - ISP) là một hệ thống liên mạng vô cùng phức tạp cả về kết nối vật lý với hàng trăm nghìn thiết bị và hàng nghìn các dịch vụ lớn nhỏ. Chính vì vậy, mỗi thiết bị mạng truyền dẫn trên mạng lưới của ISP phải chạy nhiều dịch vụ đồng thời để đáp ứng được yêu cầu đó. Trong hệ thống phần mềm của thiết bị mạng truyền dẫn, mỗi dịch vụ tương ứng với một hoặc nhiều tiến trình (có thể gọi là tiến trình dịch vụ). Các tiến trình được chia làm hai loại chính:

- Các tiến trình hệ thống, là các tiến trình như hệ điều hành, phân chia bộ nhớ, tài nguyên, hoặc từ bên phát triển thứ ba, … Các tiến trình này đảm bảo hệ thống phần mềm trên thiết bị mạng hoạt động ổn định.
- Các tiến trình dịch vụ, là các tiến trình dịch vụ trực tiếp trên mạng lưới như:
    - Các tiến trình chuyển tiếp gói tin lớp 2: giao thức điều khiển gộp liên kết (Link Aggregation Control Protocol – LACP), giao thức cây kéo dài (Spanning Tree Protocol – STP), mạng cục bộ ảo (Virtual Local Area Network – VLAN), …
    - Các tiến trình định tuyến lớp 3: tiến trình thông tin định tuyến (Routing Information Base - RIB) trên mặt phẳng điều khiển (Control Plane), giao thức định tuyến tuyến đường ngắn nhất mở (Open Shortest Path First – OSPF), giao thức định tuyến vùng biên (Border Gateway Protocol – BGP), giao thức định tuyến hệ trung cấp (Intermediate System to Intermediate System – ISIS), …
    - Các tiến trình định tuyến bằng nhãn: giao thức quảng bá nhãn (Label Distribution Protocol – LDP), chuyển mạch nhãn đa giao thức (MultiProtocol Label Switching – MPLS), giao thức dành riêng tài nguyên (Resource Reservation Protocol – RSVP), …

- Các tiến trình định tuyến gói tin đa đích (Multicast): giao thức quản lý nhóm trên mạng (Internet Group Management Protocol – IGMP), giao thức nhóm độc lập (Protocol Independent Multicast – PIM).
- Các tiến trình dịch vụ lõi của nền tảng mạng (Network Platform) khác.

Các tiến trình dịch vụ trong thiết bị mạng truyền dẫn này cần hoạt động liên tục trong thời gian dài để đảm bảo các dịch vụ trên mạng được thông suốt không gián đoạn. Thời gian hoạt động có thể lên đến nhiều tháng hoặc nhiều năm.

Thực tế, trong nhiều tình huống, các tiến trình dịch vụ này xảy ra lỗi dẫn đến việc sụp đổ (crash). Điều này vô cùng nguy hiểm cho mạng lưới vì các lý do sau đây :

- Toàn bộ dịch vụ mà tiến trình đó thực hiện bị gián đoạn, có thể xảy ra mất kết nối diện rộng trên mạng lưới.
- Các tiến trình trong một hệ thống có sự liên kết với nhau, tiến trình này sụp đổ có thể kéo theo các tiến trình dịch vụ khác hoạt động không đúng theo yêu cầu.
- Nếu tiến trình dịch vụ bị lỗi là các tiến trình cốt lõi có nhiệm vụ điều khiển các tiến trình khác, hoặc là trung tâm tính toán, điều này sẽ gây sụp đổ toàn hệ thống trên thiết bị mạng truyền dẫn.

Chính vì vậy, phương pháp trong sáng chế sẽ đảm bảo các tiến trình dịch vụ này hoạt động liên tục hoặc gián đoạn trong khoảng thời gian cho phép.

Bản chất kỹ thuật của sáng chế

Do đó, mục đích của sáng chế là nghiên cứu và cải tiến thiết bị định tuyến trong mạng truyền dẫn có khả năng:

- Phát hiện được các tiến trình dịch vụ xảy ra lỗi hoặc sụp đổ, xác định và phân loại các mức độ lỗi hay sụp đổ;
- Áp dụng hành động tương tứng với từng tiến trình theo từng mức độ quan trọng của tiến trình và lỗi xảy ra;
- Lưu lại các sự kiện của tiến trình dịch vụ vào các bản ghi cho người quản trị mạng, gửi cảnh bảo lên máy chủ được cài đặt để thông báo về việc tiến trình dịch vụ xảy ra lỗi;
- Các tiến trình phục vụ giám sát, phát hiện lỗi và quyết định hành động có khả năng tự bảo vệ trong trường hợp xảy ra lỗi.

Theo sáng chế, một tiến trình mới được tạo ra để giám sát toàn bộ các tiến trình dịch vụ trong thiết bị.

Tiến trình giám sát dịch vụ kết nối và giao tiếp hai chiều với toàn bộ các tiến trình dịch vụ trong thiết bị dựa vào cơ chế giao tiếp liên tiến trình (Inter-Process Communication - IPC) do hệ điều hành hỗ trợ. Dựa vào cơ chế này, khi tiến trình dịch vụ bị lỗi hay sụp đổ, tiến trình giám sát ngay lập tức phát hiện và phân loại mức độ quan trọng của lỗi:

- Tiến trình dịch vụ 1,2: màu vàng, mức độ nguy cơ thấp;
- Tiến trình dịch vụ 3,4: màu cam, mức độ nguy cơ trung bình;
- Tiến trình dịch vụ n, n+1: màu đỏ, mức độ nguy cơ cao.

Đối với từng nhóm tiến trình dịch vụ bị lỗi, tiến trình giám sát sẽ can thiệp để bảo vệ và phục hồi dịch vụ ngay sau khi phát hiện bằng cách gửi các tín hiệu cho hệ điều hành. Cụ thể:

- Nhóm tiến trình nguy cơ thấp: gửi tín hiệu cho hệ điều hành yêu cầu khởi động lại tiến trình bị lỗi. Cấu hình lại dịch vụ nếu cần thiết;
- Nhóm tiến trình nguy cơ trung bình: gửi tín hiệu cho hệ điều hành yêu cầu khởi động lại tiến trình bị lỗi và các tiến trình liên quan do các tiến trình này có sự liên kết chặt chẽ, không thể khởi động đơn lẻ một tiến trình dịch vụ;
- Nhóm tiến trình nguy cơ cao: đây là nhóm các tiến trình dịch vụ cốt lõi của thiết bị, việc khởi động lại tiến trình dịch vụ đó không đảm bảo thiết bị hoạt động như mong muốn. Ngay lập tức, cần gửi tín hiệu cho hệ điều hành yêu cầu khởi động lại toàn bộ thiết bị.

Ngay khi phát hiện các tiến trình dịch vụ bị lỗi, tiến trình giám sát cần phải :

- Lưu lại các sự kiện vào tệp trong thiết bị như: tiến trình lỗi, thời điểm xảy ra lỗi, loại lỗi, các tệp cần thiết, hành động đối với tiến trình, … để phục vụ quá trình thống kê, giám sát và gỡ lỗi sau này cho thiết bị;
- Gửi các thông tin cảnh báo về các tiến trình dịch vụ lỗi lên trên máy chủ qua giao thức quản lý mạng đơn giản (Simple Network Management Protocol - SNMP).

Sáng chế sẽ chỉnh sửa và triển khai mã nguồn trên kiến trúc phần mềm hiện tại.

Để đạt được mục đích trên, sáng chế phương pháp bảo vệ các tiến trình dịch vụ trên thiết bị mạng truyền dẫn bao gồm năm bước:

Bước 1: phân tích và thiết kế phương pháp theo sáng chế trên mã nguồn hiện tại;

Tại bước này, sử dụng mã nguồn của thiết bị mạng truyền dẫn định tuyến vùng biên (Site Router - SRT) Viettel đã phát triển và triển khai thực tế trên mạng lưới đánh giá tính khả thi khi triển khai phương pháp theo sáng chế dựa vào mã nguồn hiện tại và các tài liệu mô tả phần cứng. Tiến hành thiết kế sơ đồi khối phần mềm các thành phần của sáng chế và sự tương tác của các khối đó trên mã nguồn hiện tại.

Bước 2: triển khai mã nguồn phát triển tiến trình giám sát dịch vụ;

Thực hiện thiết kế chi tiết các thành phần của tiến trình giám sát dịch vụ cả về phần mềm lẫn giải pháp tương tác với phần cứng, sau đó thực hiện triển khai bằng cách phát triển phần mềm lên mã nguồn hiện tại

Bước 3: triển khai mã nguồn phát triển tiến trình giám sát dịch vụ dự phòng;

Thực hiện thiết kế chi tiết các thành phần của tiến trình giám sát dịch vụ dự phòng cả về phần mềm lẫn giải pháp tương tác với phần cứng, sau đó thực hiện triển khai bằng cách phát triển phần mềm lên mã nguồn hiện tại

Bước 4: chỉnh sửa mã nguồn các tiến trình dịch vụ để giao tiếp với các tiến trình giám sát qua cơ chế IPC khi có lỗi xảy ra;

Sau khi triển khai xong mã nguồn của các tiến trình giám sát dịch vụ, cần triển khai cơ chế kết nối với các tiến trình dịch vụ mà chúng sẽ giám sát để thu thập trạng thái lỗi của các tiến trình theo thời gian thực. Một số các cơ chế IPC khác nhau sẽ được sử dụng tùy thuộc vào mức độ quan trọng của tiến trình dịch vụ.

Bước 5: chỉnh sửa mã nguồn cho phép tiến trình giám sát giao tiếp với hệ điều hành để điều khiển và thực hiện hành động đối với các tiến trình dịch vụ bị lỗi.

Các tiến trình giám sát cần phải ra lệnh và thực hiện hành động đối với các tiến trình xảy ra lỗi, việc này cần hệ điều hành làm trung gian và tiến trình giám sát phải giao tiếp với hệ điều hành để thao tác điều khiển.

Mô tả vắn tắt các hình vẽ

Hình 1 là hình vẽ mô tả tính năng tổng quát phương pháp giám sát tiến trình dịch vụ của sáng chế;

Hình 2 là hình vẽ mô tả tiến trình giám sát và hệ điều hành kết hợp để giám sát các tiến trình dịch vụ;

Hình 3 là hình vẽ mô tả quá trình PFM gửi các thông tin cảnh báo nên máy chủ hoặc hệ thống NMS;

Hình 4 là hình vẽ mô tả mối quan hệ giữa tiến trình giám sát PFM và tiến trình giám sát dự phòng;

Hình 5 là hình vẽ mô tả luồng hoạt động giao tiếp giữa tiến trình giám sát và tiến trình được giám sát;

Hình 6 là hình vẽ mô tả quá trình khởi động lại các tiến trình dịch vụ;

Hình 7 là hình vẽ mô tả ví dụ thực hiện sáng chế trên thiết bị SRT Viettel.

Mô tả chi tiết sáng chế

Để đạt được mục đích sáng chế, cần triển khai phát triển thêm hai tiến trình giám sát dịch vụ. Hai tiến trình này vừa giám sát các tiến trình dịch vụ, vừa giám sát lẫn nhau đảm bảo việc bảo vệ chính tiến trình giám sát khi có lỗi xảy ra.

Tham chiếu Hình 1, sáng chế phương pháp bảo vệ các tiến trình dịch vụ trên thiết bị mạng truyền dẫn bao gồm năm bước, cụ thể nội dung từng bước lần lượt như sau:

Bước 1: phân tích và thiết kế phương pháp theo sáng chế trên mã nguồn hiện tại;

Sử dụng mã nguồn của thiết bị mạng truyền dẫn định tuyến vùng biên (Site Router - SRT) Viettel đã phát triển và triển khai thực tế trên mạng lưới đánh giá tính khả thi khi triển khai phương pháp theo sáng chế dựa vào mã nguồn hiện tại và các tài liệu mô tả phần cứng. Tiến hành thiết kế sơ đồi khối phần mềm các thành phần của sáng chế và sự tương tác của các khối đó trên mã nguồn hiện tại.

Bước 2: triển khai mã nguồn phát triển tiến trình giám sát dịch vụ;

Tiến trình giám sát dịch vụ hay còn gọi là tiến trình quản lý lỗi (Process Management Fault - PFM) được triển khai trực tiếp trên mã nguồn của SRT. PFM bao gồm các phần chính như sau:

- Phần xử lý các tiến trình dịch vụ lỗi.

Đây là phần quan trọng và cốt lõi của PFM (Hình 2). Mã nguồn được triển khai để PFM liên tục giám sát các tiến trình dịch vụ để phát hiện lỗi xảy ra trong các tiến trình. Khi xác định được mức độ lỗi, dựa vào cấu hình được cài đặt sẵn từ trước, PFM gửi tín hiệu đến hệ điều hành, gián tiếp yêu cầu các tiến trình dịch vụ thực hiện mệnh lệnh tương ứng (ví dụ khởi động lại tiến trình lỗi hoặc một số các tiến trình liên quan).

- Phần gửi các sự kiện cảnh báo lên máy chủ.

Trong hệ thống mạng lưới của ISP, việc giám sát các thiết bị là bắt buộc, đặc biệt các sự kiện liên quan đến lỗi. Mã nguồn PFM được triển khai giúp PFM có thể sử dụng, đóng gói các bản tin trên giao thức SNMP (Hình 3), gửi các thông tin cảnh báo lên máy chủ đích được cài đặt hoặc hệ thống quản lý mạng (Network Management System - NMS). PFM sử dụng số định danh thực thể (Object Identifier - OID) riêng cho tính năng

PFM khi gửi bản tin bằng SNMP. Việc gửi thông tin lên NMS chỉ diễn ra khi có sự kiện xảy ra, không gửi liên tục để đảm bảo hiệu năng hệ thống.

- Phần xử lý đọc/ghi các bản ghi lưu lại các sự kiện và hành động khi xảy ra lỗi.

Mã nguồn PFM được triển khai giúp lưu lại các sự kiện (tiến trình lỗi, loại lỗi, mức độ quan trọng, thời gian xảy ra, …) và hành động (khởi động lại tiến trình, khởi động lại thiết bị, nguyên nhân, thời gian khởi động, …) vào các bản ghi (log file) ở Hình 3. Ngoài ra, các bản ghi này chứa dữ liệu bộ nhớ của tiến trình dịch vụ tại thời điểm xảy ra lỗi, điều này là cần thiết và quan trọng cho việc sửa lỗi sau này.

- Các tệp cấu hình và thao tác. Mã nguồn PFM cho phép người quản trị mạng có thể cấu hình các thông số sau đây:
    - Danh sách các tiến trình dịch vụ cần được giám sát, số lần bị lỗi tối đa của mỗi tiến trình.
    - Định nghĩa mức độ quan trọng cho các tiến trình dịch vụ, các hành động tương ứng khi tiến trình lỗi.
    - Giao diện cấu hình dòng lệnh cho người quản trị mạng thao tác.

Bước 3: triển khai mã nguồn phát triển tiến trình giám sát dịch vụ dự phòng;

Hình 4 là hình vẽ mô tả mối quan hệ giữa tiến trình giám sát PFM và tiến trình giám sát dự phòng (PFM Backup - PFMBK). Do chính tiến trình giám sát PFM cũng có khả năng xảy ra lỗi hoặc sụp đổ nên cần một tiến trình để giám sát PFM, đó chính là PFMBK. Nhiệm vụ duy nhất của PFMBK là giám sát PFM, cách thực hiện tương tự như PFM giám sát các tiến trình dịch vụ khác. Ngay khi PFM xảy ra lỗi hoặc sụp đổ, PFMBK sẽ khởi động lại tiến trình PFM.

Ngược lại, nếu PFM sẽ giám sát PFMBK tương tự như các tiến trình dịch vụ khác. Việc giám sát hai chiều này đảm bảo hệ thống giám sát tiến trình dịch vụ gồm PFM và PFMBK luôn luôn hoạt động tốt, hạn chế tối đa khoảng thời gian mất giám sát.

Bước 4: chỉnh sửa mã nguồn các tiến trình dịch vụ để giao tiếp với các tiến trình giám sát qua cơ chế IPC khi có lỗi xảy ra;

Hình 5 là hình vẽ mô tả luồng hoạt động giao tiếp giữa tiến trình giám sát và tiến trình được giám sát (tiến trình dịch vụ).

PFM và tiến trình dịch vụ sử dụng cơ chế chia sẻ bộ nhớ (Shared Memory) để giao tiếp với nhau. Hai tiến trình cùng ánh xạ đến một vùng nhớ cố định, mọi thông tin hai tiến trình chia sẻ với nhau có thể được đọc/ghi vào vùng nhớ này.

Hiện tại, việc xử lý các lỗi liên quan đến tiến trình do hệ điều hành đảm nhiệm. Do vậy, sáng chế cần chỉnh sửa mã nguồn trên tất cả các tiến trình dịch vụ để tiến trình dịch vụ có thể thao tác và xử lý khi có lỗi xảy ra. Cụ thể, tiến trình dịch vụ cần ghi lỗi vào vùng nhớ chia sẻ chung với PFM, từ đó, PFM có thể phát hiện lỗi của tiến trình dịch vụ.

PFM cần liên tục kiểm tra các vùng nhớ chia sẻ chung với các tiến trình dịch vụ mà tiến trình này quản lý, đảm bảo việc phát hiện lỗi và thời gian bị mất dịch vụ là ngắn nhất. Mã nguồn PFM sử dụng cơ chế kiểm tra liên tục (polling) để đọc dữ liệu từ vùng nhớ chia sẻ.

Bước 5: chỉnh sửa mã nguồn cho phép tiến trình giám sát giao tiếp với hệ điều hành để điều khiển và thực hiện hành động đối với các tiến trình dịch vụ bị lỗi.

Hình 6 là mô hình mô tả quá trình khởi động lại các tiến trình dịch vụ. Tiến trình giám sát và các tiến trình dịch vụ là ngang hàng nên PFM không thể trực tiếp khởi động lại các tiến trình dịch vụ. Sau khi PFM phát hiện lỗi trên tiến trình dịch vụ, PFM gửi yêu cầu đến hệ điều hành yêu cầu khởi động lại tiến trình dịch vụ và các tiến trình liên quan (nếu có). Bên trong hệ điều hành chia làm hai giai đoạn:

- Tạo tín hiệu (Generate signal) theo yêu cầu của PFM.
- Gửi các tín hiệu (khởi động lại) tới các tiến trình dịch vụ theo yêu cầu của PFM.

Sau khi các tiến trình dịch vụ khởi động lại, PFM tiến hành lưu lại sự kiện này vào các tệp trong hệ thống.

Ví dụ thực hiện sáng chế

Sáng chế được thực hiện trên thiết bị mạng truyền dẫn định tuyến vùng biên (Site Router) do Tổng công ty công nghiệp công nghệ cao Viettel sản xuất. Sáng chế nhằm giúp đảm bảo sự ổn định của các tiến trình dịch vụ cốt lõi trên thiết bị SRT (chuyển tiếp lớp 2, định tuyến lớp 3, định tuyến nhãn, truyền hình, …), từ đó, đảm bảo các dịch vụ như 2G, 3G, 4G, truyền hình số, internet băng rộng không bị gián đoạn.

Hình 7 là hình vẽ mô tả ví dụ thực hiện sáng chế trên thiết bị SRT Viettel. Hai thiết bị SRT đấu nối trực tiếp, sử dụng giao thức OSPF (Open Shortest Path First) làm giao thức định tuyến lớp 3. Hai thiết bị thiết lập phiên kết nối OSPF với nhau và quảng bá các tuyến đường học được cho nhau qua giao thức này.

Trong trường hợp tiến trình dịch vụ OSPF trên thiết bị SRT02 xuất hiện lỗi, nếu không có sáng chế, phiên kết nối giữa SRT01 và SRT02 sẽ bị mất, điều này không chỉ gây ra lỗi cho thiết bị SRT02 mà sẽ gây ra lỗi cho toàn mạng lưới do dịch vụ bị gián đoạn trên thiết bị SRT02. SRT01 và SRT03 và các thiết bị khác sẽ mất toàn bộ dịch vụ định tuyến – là dịch vụ cốt lõi trên mạng lưới.

Nếu có sáng chế, ngay khi phát hiện tiến trình dịch vụ OSPF trên SRT02 xảy ra lỗi, ngay lập tức tiến trình này được khởi động lại, đảm bảo thời gian mất dịch vụ trong thời gian rất ngắn, dịch vụ được hồi phục nhanh chóng.

Hiệu quả đạt được của sáng chế

Bảng 1 mô tả sự khác nhau giữa phương pháp phục hồi tiến trình dịch vụ theo phương pháp đã biết và phương pháp theo sáng chế.

Bảng 1

	Phương pháp theo giải pháp kỹ thuật đã biết	Phương pháp theo sáng chế
Độ phức tạp của mô hình	Đơn giản	Phức tạp
Thao tác phục hồi dịch vụ	Phức tạp, phải thao tác bằng tay	Đơn giản, tự động, không cần can thiệp.
Thời gian phục hồi dịch vụ	Thời gian dài, phụ thuộc vào người quản trị	Phục hồi ngay khi phát hiện lỗi

Với phương pháp kỹ thuật hiện tại, người quản trị mạng chỉ biết tiến trình dịch vụ xảy ra lỗi khi lỗi đã xảy ra diện rộng trên mạng lưới, rất nghiêm trọng và ảnh hưởng trực tiếp đến nhiều khách hàng. Khi đó người quản trị phải xác định lỗi và quyết định thao tác để khởi động lại tiến trình dịch vụ hoặc thiết bị. Điều này khiến thời gian dịch vụ bị gián đoạn kéo dài, gây thiệt hại cao về kinh tế và an ninh.

Phương pháp theo sáng chế giải quyết được tất cả các vấn đề trên một các tự động, đảm bảo dịch vụ không bị gián đoạn.

Yêu cầu bảo hộ

1. Phương pháp bảo vệ các tiến trình dịch vụ trên thiết bị định tuyến trong mạng truyền dẫn, bao gồm các bước:

bước 1: phân tích và thiết kế phương pháp theo sáng chế trên mã nguồn hiện tại;

tại bước này, sử dụng mã nguồn của thiết bị mạng truyền dẫn định tuyến vùng biên (Site Router - SRT) do viettel đã phát triển và triển khai thực tế trên mạng lưới đánh giá tính khả thi khi triển khai phương pháp theo sáng chế dựa vào mã nguồn hiện tại và các tài liệu mô tả phần cứng; tiến hành thiết kế sơ đồi khối phần mềm các thành phần của sáng chế và sự tương tác của các khối đó trên mã nguồn hiện tại;

bước 2: triển khai mã nguồn phát triển tiến trình giám sát dịch vụ;

tiến trình giám sát dịch vụ hay còn gọi là tiến trình quản lý lỗi (process management fault - PFM) được triển khai trực tiếp trên mã nguồn của SRT; PFM bao gồm các phần chính như sau:

phần xử lý các tiến trình dịch vụ lỗi: mã nguồn được triển khai để PFM liên tục giám sát các tiến trình dịch vụ để phát hiện lỗi xảy ra trong các tiến trình; khi xác định được mức độ lỗi, dựa vào cấu hình được cài đặt sẵn từ trước, PFM gửi tín hiệu đến hệ điều hành, gián tiếp yêu cầu các tiến trình dịch vụ thực hiện mệnh lệnh tương ứng;

phần gửi các sự kiện cảnh báo lên máy chủ: mã nguồn PFM được triển khai giúp PFM có thể sử dụng, đóng gói các bản tin trên giao thức SNMP, gửi các thông tin cảnh báo lên máy chủ đích được cài đặt hoặc hệ thống quản lý mạng (network management system - NMS); PFM sử dụng số định danh thực thể (object identifier - OID) riêng cho tính năng PFM khi gửi bản tin bằng SNMP; việc gửi thông tin lên NMS chỉ diễn ra khi có sự kiện xảy ra, không gửi liên tục để đảm bảo hiệu năng hệ thống;

phần xử lý đọc/ghi các bản ghi lưu lại các sự kiện và hành động khi xảy ra lỗi: mã nguồn PFM được triển khai giúp lưu lại các sự kiện (tiến trình lỗi, loại lỗi, mức độ quan trọng, thời gian xảy ra, ...) và hành động (khởi động lại tiến trình, khởi động lại thiết bị, nguyên nhân, thời gian khởi động, ...) vào các bản ghi (log file); ngoài ra, các bản ghi này chứa dữ liệu bộ nhớ của tiến trình dịch vụ tại thời điểm xảy ra lỗi, điều này là cần thiết và quan trọng cho việc sửa lỗi sau này;

bước 3: triển khai mã nguồn phát triển tiến trình giám sát dịch vụ dự phòng;

do chính tiến trình giám sát PFM cũng có khả năng xảy ra lỗi hoặc sụp đổ nên cần một tiến trình để giám sát PFM, đó chính là PFMBK; nhiệm vụ duy nhất của PFMBK là giám sát PFM, cách thực hiện tương tự như PFM giám sát các tiến trình dịch vụ khác; ngay khi PFM xảy ra lỗi hoặc sụp đổ, PFMBK sẽ khởi động lại tiến trình PFM; ngược lại, PFM sẽ giám sát PFMBK tương tự như các tiến trình dịch vụ khác; việc giám sát hai chiều này đảm bảo hệ thống giám sát tiến trình dịch vụ gồm PFM và PFMBK luôn luôn hoạt động tốt, hạn chế tối đa khoảng thời gian mất giám sát;

bước 4: chỉnh sửa mã nguồn các tiến trình dịch vụ để giao tiếp với các tiến trình giám sát qua cơ chế IPC khi có lỗi xảy ra;

PFM và tiến trình dịch vụ sử dụng cơ chế chia sẻ bộ nhớ (Shared Memory) để giao tiếp với nhau; hai tiến trình cùng ánh xạ đến một vùng nhớ cố định, mọi thông tin hai tiến trình chia sẻ với nhau có thể được đọc/ghi vào vùng nhớ này;

tiến trình dịch vụ cần ghi lỗi vào vùng nhớ chia sẻ chung với PFM, từ đó, PFM có thể phát hiện lỗi của tiến trình dịch vụ;

PFM cần liên tục kiểm tra các vùng nhớ chia sẻ chung với các tiến trình dịch vụ mà tiến trình này quản lý, đảm bảo việc phát hiện lỗi và thời gian bị mất dịch vụ là ngắn nhất; mã nguồn PFM sử dụng cơ chế kiểm tra liên tục (polling) để đọc dữ liệu từ vùng nhớ chia sẻ;

bước 5: chỉnh sửa mã nguồn cho phép tiến trình giám sát giao tiếp với hệ điều hành để điều khiển và thực hiện hành động đối với các tiến trình dịch vụ bị lỗi;

tiến trình giám sát và các tiến trình dịch vụ là ngang hàng nên PFM không thể trực tiếp khởi động lại các tiến trình dịch vụ; sau khi PFM phát hiện lỗi trên tiến trình dịch vụ, PFM gửi yêu cầu đến hệ điều hành yêu cầu khởi động lại tiến trình dịch vụ và các tiến trình liên quan (nếu có); ên trong hệ điều hành chia làm hai giai đoạn:

tạo tín hiệu (generate signal) theo yêu cầu của PFM;

gửi các tín hiệu (khởi động lại) tới các tiến trình dịch vụ theo yêu cầu của PFM;

sau khi các tiến trình dịch vụ khởi động lại, PFM tiến hành lưu lại sự kiện này vào các tệp trong hệ thống.

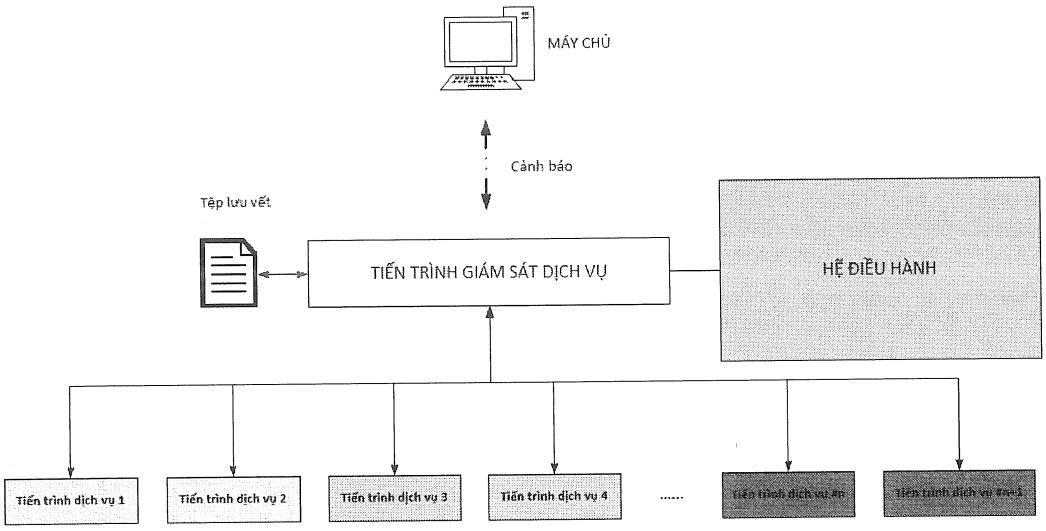
2. Phương pháp bảo vệ các tiến trình dịch vụ trên thiết bị định tuyến trong mạng truyền dẫn theo điểm 1, trong đó:

tại bước 2: các tệp cấu hình và thao tác, mã nguồn PFM cho phép người quản trị mạng có thể cấu hình các thông số sau đây:

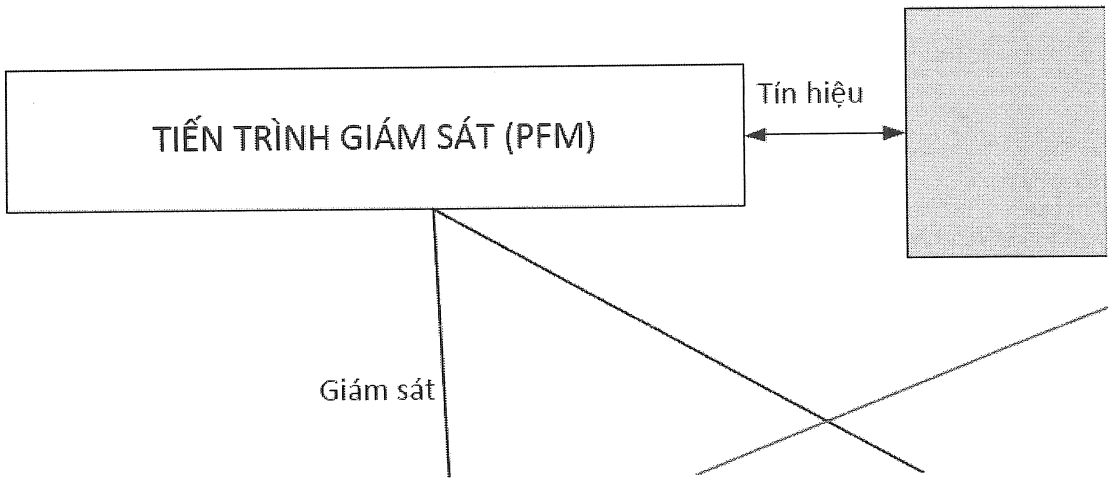
danh sách các tiến trình dịch vụ cần được giám sát, số lần bị lỗi tối đa của mỗi tiến trình;

định nghĩa mức độ quan trọng cho các tiến trình dịch vụ, các hành động tương ứng khi tiến trình lỗi;

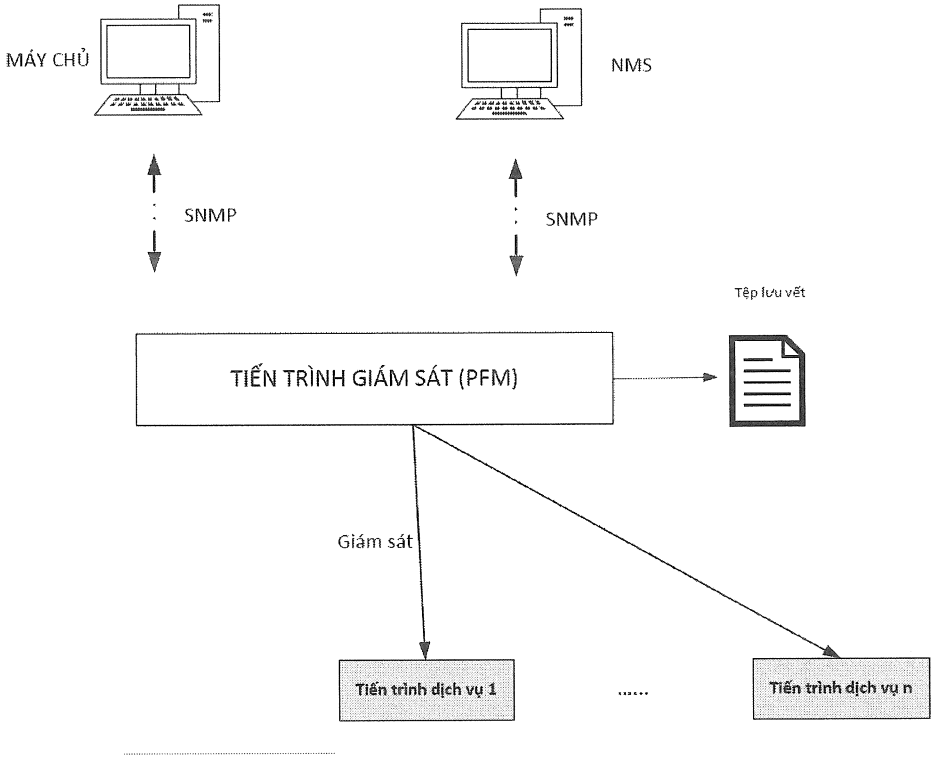
giao diện cấu hình dòng lệnh cho người quản trị mạng thao tác.


MÁY CHỦ
Cảnh báo
Tệp lưu vết
TIẾN TRÌNH GIÁM SÁT DỊCH VỤ
HỆ ĐIỀU HÀNH
Tiến trình dịch vụ 1
Tiến trình dịch vụ 2
Tiến trình dịch vụ 3
Tiến trình dịch vụ 4
.....

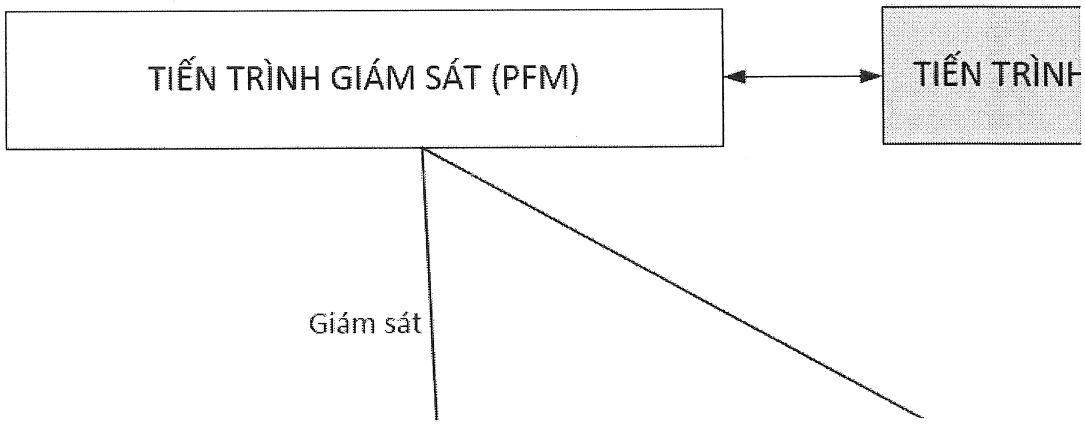
Hình 1


TIẾN TRÌNH GIÁM SÁT (PFM)
Tín hiệu
Giám sát

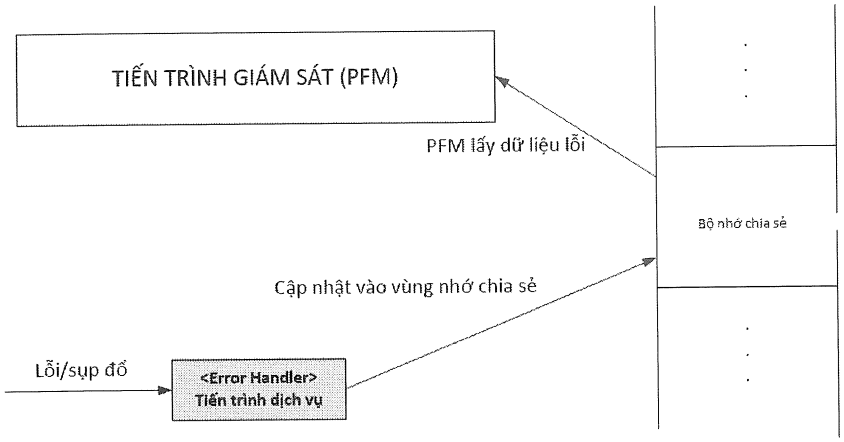
Hình 2


MÁY CHỦ
NMS
SNMP
SNMP
Tệp lưu vết
TIẾN TRÌNH GIÁM SÁT (PFM)
Giám sát
Tiến trình dịch vụ 1
.....
Tiến trình dịch vụ n

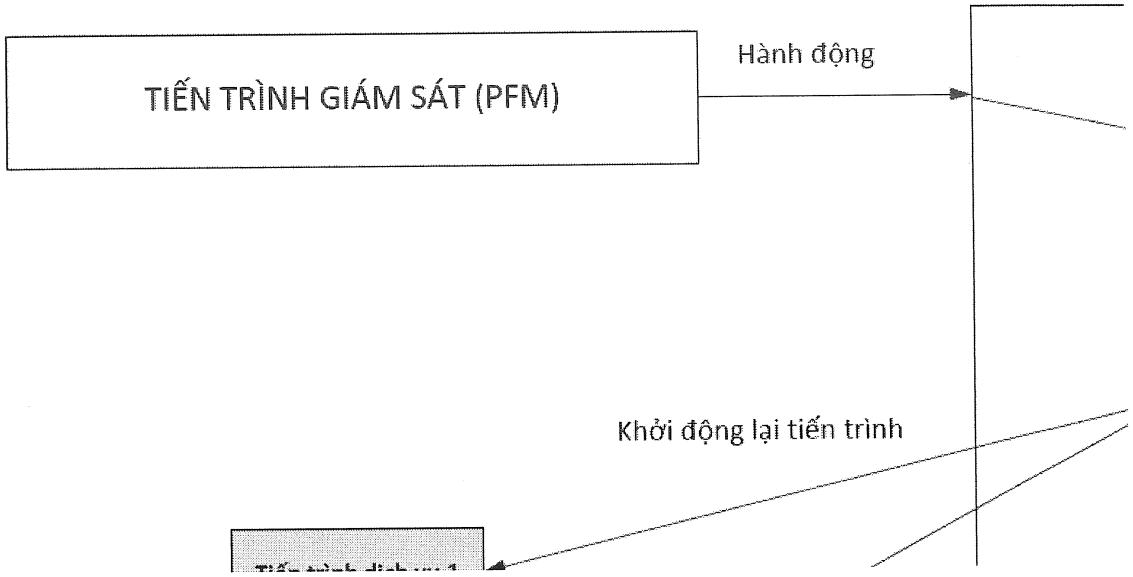
Hình 3


TIẾN TRÌNH GIÁM SÁT (PFM)
TIẾN TRÌNH
Giám sát

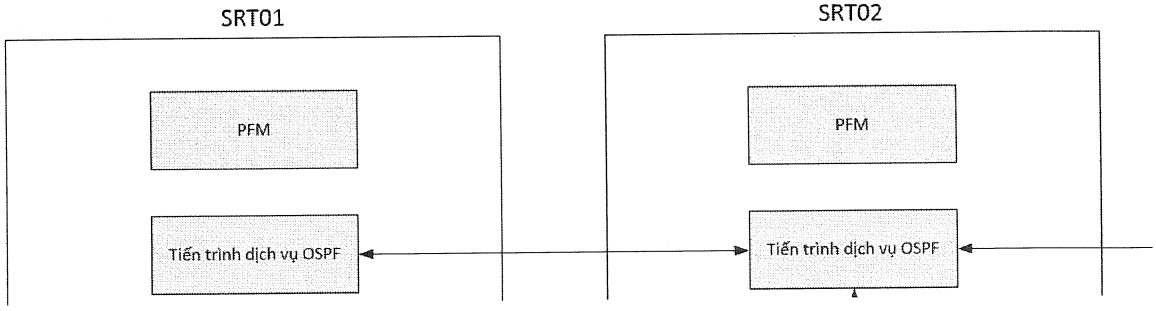
Hình 4



Hình 5



Hình 6



Hình 7