| logo (CMYK)-01 | **BỘ GIÁO DỤC VÀ ĐÀO TẠO**  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |
| --- | --- |

**ĐỒ ÁN CƠ SỞ**

**Xây dựng hệ thống quản lý cấu hình mạng tự động với AWS S3**

**Tên thương mại: CloudConfig Guardian**

Ngành: **CÔNG NGHỆ THÔNG TIN**

Giảng viên hướng dẫn: **TS**.**Nguyễn Quang Trung**

Sinh viên thực hiện: MSSV: Lớp:

1. Lê Nguyễn Minh Sang 2280602709 22DTHB1

TP. Hồ Chí Minh, 2025

[**LỜI NÓI ĐẦU 4**](#_ax778oy8i027)

[**CHƯƠNG 1:TỔNG QUAN VỀ ĐỀ TÀI 5**](#_481sn2plj6sv)

[1.1. Lý do chọn đề tài 5](#_9e4l5q721hdo)

[1.2. Yêu cầu đề tài 5](#_4bholmqln8v7)

[**CHƯƠNG 2:TỔNG QUAN VỀ ĐỀ TÀI 7**](#_21s2nwhvonax)

[2.1. Khái niệm cơ bản về quản lý cấu hình mạng (NCM) 7](#_rq89p8vynlkx)

[2.1.1. Sự hình thành và phát triển của hệ thống quản lý cấu hình mạng 7](#_7p0g8h5ndz7a)

[2.1.2. Thế nào là hệ thống quản lý cấu hình mạng 7](#_cqscjd759hi6)

[2.1.3. Phân loại hệ thống quản lý cấu hình mạng 8](#_19dzewj6k9lp)

[2.1.4. Phương pháp kết nối với thiết bị mạng 8](#_geqazr7igmrk)

[2.2. Tổng quan về hệ thống quản lý cấu hình mạng tự động (Automated NCM) 9](#_jfypzbqwwgxo)

[2.2.1. Tại sao cần tự động hóa quản lý cấu hình mạng 9](#_ipndtjpmz5lm)

[2.2.3. Đặc trưng của NCM tự động 10](#_ts679pl8tnbc)

[2.2.4. Ưu và nhược điểm của hệ thống NCM tự động 10](#_7fna31ihiexx)

[2.2.5. Các mô hình triển khai NCM 11](#_jro32vu05uwk)

[2.2.6. Lưu trữ cấu hình trên AWS S3 12](#_q0mz9fje8xt4)

[2.2.7. Phương pháp phát hiện thay đổi cấu hình 12](#_xhk1w33hhzje)

[2.2.8. Các thành phần chính của hệ thống NCM tự động 13](#_73eirgsymdm8)

[**CHƯƠNG 3. KHẢO SÁT, THIẾT KẾ VÀ CÀI ĐẶT HỆ THỐNG 15**](#_x8dea8yakcbm)

[3.1. Khảo sát nhu cầu và yêu cầu hệ thống 15](#_1pc3ujcvvrcp)

[3.2.1. Cấu trúc thư mục dự án 15](#_g6nnc4ce4v48)

[3.2.2. Mô hình dữ liệu 16](#_ixvnlfanwze3)

[3.2.3. Giao diện người dùng 17](#_fsvg4f4q0suj)

[3.3. Các thành phần chức năng 18](#_4rs55tawfbe1)

[3.3.1. Các controller và API 18](#_qn53aalimpfb)

[3.3.2. Dịch vụ xử lý nghiệp vụ 19](#_5d4fv15mndbd)

[3.3.3. Xử lý thông báo và giám sát 19](#_c52luqnqu2k7)

[3.4. Hướng dẫn cài đặt và triển khai 20](#_m0b50z9juv1k)

[**CHƯƠNG 4. ỨNG DỤNG THỰC TIỄN VÀ MÔ PHỎNG VẬN HÀNH 21**](#_kj2r84zi4mbr)

[4.1. Quản lý thiết bị mạng thực tế 21](#_krwootncuk70)

[4.2. Tự động phát hiện thay đổi và kiểm tra tuân thủ 21](#_s187uzg8i6dz)

[4.3. Tích hợp cloud và lưu trữ an toàn 22](#_on01rmaxn8lm)

[4.4. Xây dựng kịch bản kiểm thử 23](#_dtt9znmiscz7)

[**CHƯƠNG 5. KẾT LUẬN 28**](#_enyupw29klc7)

[5.1. Những kết quả đạt được 28](#_1dje7ny18cgm)

[5.2. Định hướng phát triển tương lai 28](#_jilivs4nfw09)

[**TÀI LIỆU THAM KHẢO 28**](#_h2uj5fd1vp4i)

**DANH MỤC CÁC KÝ HIỆU, CHỮ VIẾT TẮT**

| Ký hiệu | Giải thích |
| --- | --- |
| NCM | Network Configuration Management (Quản lý cấu hình mạng) |
| AWS S3 | Amazon Web Services Simple Storage Service (Dịch vụ lưu trữ đơn giản của Amazon Web Services) |
| SNMP | Simple Network Management Protocol (Giao thức quản lý mạng đơn giản) |
| API | Application Programming Interface (Giao diện lập trình ứng dụng) |
| ISR | Integrated Services Router (Bộ định tuyến dịch vụ tích hợp) |
| ASA | Adaptive Security Appliance (Thiết bị bảo mật thích ứng) |
| ITSM | IT Service Management (Quản lý dịch vụ công nghệ thông tin) |
| RBAC | Role-Based Access Control (Kiểm soát truy cập dựa trên vai trò) |
| SMB | Small and Medium Business (Doanh nghiệp vừa và nhỏ) |
| SaaS | Software as a Service (Phần mềm dưới dạng dịch vụ) |
| OID | Object Identifier (Định danh đối tượng) |
| SSE | Server-Side Encryption (Mã hóa phía máy chủ) |
| CQRS | Command Query Responsibility Segregation (Phân tách trách nhiệm truy vấn lệnh) |
| NETCONF | Network Configuration Protocol (Giao thức cấu hình mạng) |
| SOAP | Simple Object Access Protocol (Giao thức truy cập đối tượng đơn giản) |
| RTO | Recovery Time Objective (Mục tiêu thời gian phục hồi) |
| NTP | Network Time Protocol (Giao thức thời gian mạng) |

**DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ**

***Hình 3.1:*** *Sơ đồ ERD (Entity Relationship Diagram) cho hệ thống*

***Hình 3.2:*** *Ảnh chụp màn hình Trang Dashboard.*

***Hình 3.3:*** *Minh họa sơ đồ luồng xử lý cảnh báo khi phát hiện thay đổi cấu hình (sequence diagram).*

***Hình 4.1****: giao diện danh sách thiết bị mạng với trạng thái realtime.*

**hình 4.2**: *Ảnh chụp thông báo Telegram khi có thay đổi cấu hình, minh họa bảng*  *lịch sử thay đổi.*

***Ảnh 4.3****: minh họa dashboard AWS S3 hiển thị các file backup cấu hình.*

***hình 4.4****: Ảnh minh họa khi thêm router mới vào hệ thống.*

***Hình 4.5:*** *Ảnh minh họa trang khôi phục cấu hình router trước khi chọn cấu hình.*

***Hình 4.6:*** *sau khi chọn khi cấu hình*

***Hình 4.7:*** *sau khi đã khôi phục thành công*

***hình 4.8****: trang configuration history của route*r

***hình 4.9:*** *trang hiển thị chi tiết config đã lưu của router*

***hình 4.10****: trang so sánh cấu hình*

***hình 4.11****: trang kết quả so sánh*

***hình 4.12****: bảng CLI mở bằng PUTTY sử dụng SSH*

***hình 4.13****: thông báo telegram được gửi về*

# 

# **LỜI NÓI ĐẦU**

Ngày nay, khi công nghệ thông tin ngày càng phát triển mạnh mẽ và đóng vai trò then chốt trong sự vận hành của mọi tổ chức, doanh nghiệp, thì hệ thống mạng đã trở thành hạ tầng thiết yếu không thể thiếu. Trong môi trường kinh doanh hiện đại, bất kỳ sự cố mạng hay gián đoạn dịch vụ nào cũng có thể gây ra những thiệt hại đáng kể về tài chính và uy tín. Đặc biệt, các thay đổi cấu hình mạng không được ghi nhận, theo dõi và quản lý đúng cách thường là nguyên nhân chính dẫn đến các sự cố nghiêm trọng.

Các thiết bị mạng như router, switch đóng vai trò là xương sống của hạ tầng mạng doanh nghiệp, nhưng việc quản lý cấu hình của chúng vẫn còn nhiều hạn chế. Phần lớn các thay đổi cấu hình vẫn được thực hiện thủ công, quá trình sao lưu không được tự động hóa và khả năng phát hiện các thay đổi trái phép còn rất hạn chế. Điều này tạo ra những rủi ro lớn về an ninh mạng, tăng thời gian khắc phục sự cố và gây khó khăn trong việc tuân thủ các quy định về an toàn thông tin.

Dự án "CloudConfig Guardian" ra đời nhằm giải quyết những thách thức này. Bằng cách tự động hóa việc phát hiện, sao lưu và thông báo khi có thay đổi cấu hình, không chỉ giúp giảm thiểu rủi ro bảo mật mà còn nâng cao hiệu quả vận hành và tính ổn định của hệ thống mạng. Việc tích hợp với dịch vụ đám mây AWS S3 cũng đảm bảo dữ liệu cấu hình được lưu trữ an toàn, có thể truy cập từ bất kỳ đâu và sẵn sàng cho việc khôi phục khi cần thiết.

Qua đề tài này, em đã có cơ hội được nghiên cứu và ứng dụng những công nghệ hiện đại như ASP.NET Core, AWS SDK, SSH.NET và các giao thức mạng như SSH, SNMP để xây dựng một giải pháp toàn diện cho việc quản lý cấu hình mạng. Đây không chỉ là một đồ án học thuật mà còn là một giải pháp thực tế, có thể áp dụng vào môi trường doanh nghiệp để nâng cao hiệu quả quản lý và bảo mật hệ thống mạng.

Em xin chân thành cảm ơn **TS. Nguyễn Quang Trung** đã tận tình chỉ dạy và hỗ trợ em trong suốt quá trình thực hiện đồ án này. Những kiến thức và kinh nghiệm quý báu mà em tích lũy được sẽ là nền tảng vững chắc cho con đường nghề nghiệp tương lai của em trong lĩnh vực công nghệ thông tin và quản trị mạng.

# 

# **CHƯƠNG 1:TỔNG QUAN VỀ ĐỀ TÀI**

## **1.1. Lý do chọn đề tài**

Hiện nay, khi công nghệ thông tin đã trở thành một trong những lĩnh vực quan trọng bậc nhất trong sự phát triển kinh tếxã hội, thì việc đảm bảo hạ tầng mạng hoạt động ổn định và an toàn càng trở nên cấp thiết. Trong các hệ thống mạng hiện đại, không có khía cạnh nào quan trọng hơn việc quản lý chặt chẽ cấu hình của các thiết bị mạng yếu tố quyết định đến độ ổn định, hiệu suất và bảo mật của toàn bộ hệ thống.

Với đề tài "Xây dựng hệ thống quản lý cấu hình mạng tự động với AWS S3" được tiến hành nhằm giúp các tổ chức và doanh nghiệp giải quyết bài toán nan giải trong việc theo dõi, phát hiện và quản lý các thay đổi cấu hình thiết bị mạng. Khi số lượng thiết bị mạng ngày càng tăng, việc quản lý thủ công trở nên bất khả thi và tiềm ẩn nhiều rủi ro. Hệ thống sẽ giúp tự động hóa quy trình phát hiện thay đổi, sao lưu cấu hình và thông báo kịp thời, từ đó nâng cao khả năng phản ứng với sự cố, giảm thời gian khắc phục và đảm bảo tính liên tục trong hoạt động của doanh nghiệp.

Bên cạnh đó, qua đề tài này đã giúp em củng cố kiến thức và hiểu sâu hơn về các khái niệm cơ bản trong quản lý cấu hình mạng, phát triển ứng dụng web với ASP.NET Core, và tích hợp với các dịch vụ đám mây như AWS S3. Đề tài cũng cung cấp cho em cái nhìn toàn diện về cách các công nghệ hiện đại có thể được kết hợp để giải quyết các vấn đề thực tế trong quản lý mạng doanh nghiệp, góp phần nâng cao kỹ năng chuyên môn và khả năng áp dụng vào thực tiễn công việc trong tương lai.

## **1.2. Yêu cầu đề tài**

Trong thời đại số hóa hiện nay, sự phụ thuộc vào hệ thống mạng của các doanh nghiệp ngày càng tăng cao, trong khi đó các rủi ro về bảo mật và gián đoạn dịch vụ cũng không ngừng gia tăng. Các thay đổi cấu hình mạng không được kiểm soát có thể dẫn đến sự cố nghiêm trọng, gây thiệt hại về tài chính và uy tín cho doanh nghiệp. Nhận thức được tầm quan trọng của vấn đề này, đề tài "Xây dựng hệ thống quản lý cấu hình mạng tự động với AWS S3" hướng đến việc phát triển một giải pháp toàn diện để giám sát, sao lưu và khôi phục cấu hình mạng.

Hệ thống được yêu cầu phải đáp ứng các nhu cầu thiết yếu trong quản trị mạng hiện đại như: tự động phát hiện thay đổi cấu hình trên nhiều thiết bị đồng thời, sao lưu an toàn lên đám mây, cung cấp khả năng so sánh trực quan giữa các phiên bản, và thông báo kịp thời khi phát hiện thay đổi. Việc tích hợp với AWS S3 không chỉ đảm bảo dữ liệu được lưu trữ an toàn mà còn tạo điều kiện cho việc truy cập từ xa và khôi phục nhanh chóng khi cần thiết.

## 1.3. Ý nghĩa thực tiễn

**Giảm thiểu rủi ro và thời gian phản ứng**: Hệ thống có khả năng phát hiện và cảnh báo kịp thời khi có thay đổi cấu hình thiết bị mạng, giúp giảm thiểu thời gian phản ứng với sự cố từ hàng giờ xuống còn vài phút. Việc này không chỉ giảm thiểu rủi ro mà còn nâng cao tính sẵn sàng của hệ thống mạng.

**Tối ưu hóa quy trình quản lý**: Bằng cách tự động hóa các tác vụ lặp đi lặp lại như sao lưu, kiểm tra tuân thủ và phát hiện thay đổi, hệ thống giải phóng thời gian cho đội ngũ IT để tập trung vào các nhiệm vụ chiến lược quan trọng hơn. Theo ước tính, giải pháp này có thể giảm đến 70% thời gian dành cho các tác vụ quản lý cấu hình thủ công.

**Tăng cường khả năng khôi phục**: Việc lưu trữ lịch sử cấu hình an toàn trên AWS S3 đảm bảo khả năng khôi phục nhanh chóng khi cần thiết, với thời gian khôi phục giảm từ hàng giờ xuống còn vài phút. Hệ thống cung cấp nhiều phiên bản cấu hình để lựa chọn, tăng độ linh hoạt trong quá trình khôi phục.

**Hỗ trợ tuân thủ quy định**: Hệ thống theo dõi và lưu trữ đầy đủ lịch sử thay đổi cấu hình, tạo điều kiện thuận lợi cho công tác kiểm toán và chứng minh việc tuân thủ các tiêu chuẩn an toàn thông tin như ISO 27001, PCI DSS, NIST. Các báo cáo tuân thủ tự động giúp đơn giản hóa quy trình đánh giá và kiểm toán.

**Tiết kiệm chi phí vận hành**: Bằng cách giảm thời gian xử lý sự cố và ngừng hoạt động của hệ thống, giải pháp giúp tiết kiệm đáng kể chi phí vận hành. Theo nghiên cứu của Ponemon Institute, chi phí trung bình cho mỗi phút ngừng hoạt động của hệ thống CNTT là khoảng $5,600, do đó việc giảm thời gian ngừng hoạt động có thể mang lại lợi ích tài chính đáng kể.

**Cung cấp cái nhìn tổng quan về hạ tầng mạng**: Hệ thống cung cấp dashboard trực quan hiển thị trạng thái của toàn bộ thiết bị mạng, lịch sử thay đổi, và các cảnh báo quan trọng. Điều này giúp quản trị viên nhanh chóng nắm bắt tình hình và đưa ra quyết định kịp thời.

## 1.4. Mục tiêu nghiên cứu

## *1.4.1 Dự án đặt ra các mục tiêu cụ thể sau:*

1. *Xây dựng hệ thống quản lý cấu hình mạng tự động toàn diện với các tính năng:*

* Phát hiện thay đổi cấu hình tự động và theo thời gian thực trên nhiều thiết bị đồng thời
* Sao lưu tự động theo lịch trình và ngay lập tức khi phát hiện thay đổi
* So sánh trực quan giữa các phiên bản cấu hình, làm nổi bật các thay đổi quan trọng
* Khôi phục cấu hình từ bản sao lưu một cách nhanh chóng và an toàn
* Kiểm tra tuân thủ cấu hình theo các mẫu quy chuẩn được định nghĩa trước
* Tích hợp với dịch vụ đám mây AWS S3 để:
* Lưu trữ cấu hình an toàn, dài hạn với độ bền dữ liệu lên đến 99.999999999%
* Quản lý phiên bản và lịch sử thay đổi đầy đủ, dễ dàng truy xuất
* Truy cập và khôi phục từ xa khi cần thiết, không phụ thuộc vào vị trí địa lý
* Tận dụng các lớp lưu trữ khác nhau của S3 để tối ưu chi phí (Standard, Infrequent Access, Glacier)
* Áp dụng các chính sách bảo mật và quản lý vòng đời dữ liệu (lifecycle policies)

1. *Xây dựng hệ thống thông báo đa kênh qua:*

* Telegram cho cảnh báo tức thời với khả năng tương tác hai chiều
* Webhook để tích hợp với các hệ thống khác như ITSM, ticketing systems
* Email và thông báo trong ứng dụng cho các thông tin chi tiết
* Phân loại thông báo theo mức độ ưu tiên (severity levels) để tối ưu hóa quy trình xử lý

1. *Phát triển giao diện CLI tích hợp trong web app cho phép:*

* Thực hiện lệnh trực tiếp từ trình duyệt web đến thiết bị mạng
* Theo dõi kết quả thực thi trong thời gian thực với khả năng cuộn và tìm kiếm
* Phân tích cú pháp lệnh và cung cấp gợi ý thông minh
* Lưu trữ lịch sử lệnh để tham khảo và tái sử dụng

1. *Đảm bảo tính bảo mật cao thông qua:*

* Mã hóa thông tin xác thực và dữ liệu nhạy cảm trong cơ sở dữ liệu
* Kiểm soát truy cập dựa trên vai trò (Role-Based Access Control)
* Ghi log đầy đủ các hoạt động và thay đổi để phục vụ audit
* Áp dụng các biện pháp bảo mật tốt nhất cho web application

## *1.4.2 Đối tượng nghiên cứu:*

1. *Đề tài tập trung nghiên cứu các đối tượng sau:*

* Các thiết bị mạng Cisco (router, switch) hỗ trợ giao thức SSH và SNMP, bao gồm:
* Dòng ISR (Integrated Services Router) như 1900, 2900, 3900, 4000 series
* Dòng Catalyst switch như 2960, 3560, 3750, 9000 series
* Các thiết bị ASA (Adaptive Security Appliance)
* Các thiết bị mạng khác có khả năng kết nối qua SSH/Telnet

1. *Công nghệ lưu trữ đám mây AWS S3 và tích hợp với ứng dụng quản lý mạng:*

* Kiến trúc và đặc điểm của dịch vụ AWS S3
* Các lớp lưu trữ và chính sách quản lý vòng đời
* Cơ chế bảo mật và kiểm soát truy cập
* Phương pháp tối ưu chi phí khi sử dụng S3

1. *Các giao thức mạng và phương pháp kết nối với thiết bị:*

* Giao thức SSH (Secure Shell) và cơ chế xác thực
* Giao thức SNMP (Simple Network Management Protocol)
* Phương pháp phân tích và xử lý đầu ra của lệnh
* Kỹ thuật tự động hóa tương tác với CLI (Command Line Interface)

1. *Các công nghệ hiện đại trong phát triển ứng dụng web*:

* ASP.NET Core và Entity Framework Core
* SignalR cho giao tiếp thời gian thực
* Các mẫu thiết kế phần mềm như Repository Pattern, CQRS
* Kỹ thuật responsive design và progressive web application

## *1.4.3 Phạm vi giới hạn:*

Để đảm bảo tính khả thi và hiệu quả của đề tài, các giới hạn sau được xác định:

1. *Về thiết bị hỗ trợ:*

* Tập trung chủ yếu vào thiết bị mạng Cisco với khả năng kết nối SSH
* Có thể mở rộng sang các nhà sản xuất khác như Juniper, HP, Huawei trong các phiên bản tương lai
* Chỉ hỗ trợ các thiết bị có khả năng thực thi lệnh CLI thông qua SSH/Telnet
* Không hỗ trợ các thiết bị mạng cổ không có giao diện quản lý từ xa

1. *Về giao thức kết nối:*

* Chủ yếu sử dụng SSH làm giao thức kết nối chính do tính bảo mật cao
* SNMP được sử dụng bổ sung để giám sát trạng thái và phát hiện thay đổi
* Telnet chỉ được hỗ trợ như một phương án dự phòng khi SSH không khả dụng
* Không hỗ trợ các giao thức độc quyền hoặc không phổ biến

1. *Về dịch vụ đám mây:*

* Tích hợp chủ yếu với AWS S3 do tính phổ biến và độ tin cậy cao
* Có thể mở rộng sang các dịch vụ đám mây khác như Azure Blob Storage, Google Cloud Storage trong tương lai
* Không phụ thuộc vào các tính năng đặc biệt chỉ có ở AWS
* Thiết kế theo kiến trúc cho phép dễ dàng thay đổi nhà cung cấp dịch vụ đám mây

1. *Về phân tích cấu hình:*

* Tập trung vào phát hiện thay đổi và so sánh cấu hình
* Phân tích tuân thủ dựa trên các mẫu quy chuẩn được định nghĩa trước
* Chưa đi sâu vào phân tích ngữ nghĩa tự động của cấu hình
* Không bao gồm việc tự động tạo ra các đề xuất cải thiện cấu hình

1. *Về quy mô triển khai:*

* Thiết kế cho môi trường có đến 20 thiết bị mạng
* Có thể mở rộng lên quy mô lớn hơn thông qua tùy chỉnh cấu hình
* Yêu cầu kết nối internet để sử dụng đầy đủ tính năng

## *1.4.4 Cấu trúc đồ án*

Chương 1: TỔNG QUAN VỀ ĐỀ TÀI

Chương này trình bày tổng quan về đề tài, lý do chọn đề tài và các yêu cầu cơ bản. Đầu tiên, chương giới thiệu tầm quan trọng của quản lý cấu hình mạng trong môi trường doanh nghiệp hiện đại, phân tích các thách thức trong quản lý cấu hình mạng truyền thống như thiếu giải pháp quản lý tập trung, quản lý thủ công gây nhiều rủi ro, và khó khăn trong việc tuân thủ quy định. Tiếp theo, chương này nêu bật tính cấp thiết của việc xây dựng hệ thống quản lý cấu hình tự động để giải quyết các vấn đề nêu trên, đồng thời củng cố kiến thức về quản lý cấu hình mạng và tích hợp với các dịch vụ đám mây. Cuối cùng, chương này trình bày nhiệm vụ và cấu trúc của toàn bộ đồ án.

Chương 2: TỔNG QUAN VỀ QUẢN LÝ CẤU HÌNH MẠNG

Chương này đi sâu vào các khái niệm cơ bản về quản lý cấu hình mạng (Network Configuration Management - NCM), bắt đầu từ lịch sử phát triển của NCM từ những năm 1990 đến nay. Chương này giải thích chi tiết về hệ thống NCM, bao gồm các chức năng chính như phát hiện và sao lưu tự động, theo dõi thay đổi, so sánh cấu hình, và khôi phục cấu hình. Chương cũng phân loại các hệ thống NCM theo phương thức triển khai, quy mô hỗ trợ, và nhà sản xuất thiết bị. Đặc biệt, chương này phân tích sâu về các phương pháp kết nối với thiết bị mạng (SSH, SNMP, Telnet, API), giải thích tại sao cần tự động hóa quản lý cấu hình mạng, và trình bày các đặc trưng, ưu nhược điểm của NCM tự động. Ngoài ra, chương này cũng giới thiệu về lưu trữ cấu hình trên AWS S3, phương pháp phát hiện thay đổi cấu hình, và các thành phần chính của hệ thống NCM tự động.

Chương 3: KHẢO SÁT, THIẾT KẾ VÀ CÀI ĐẶT HỆ THỐNG NCM

Chương này mô tả chi tiết quá trình khảo sát nhu cầu thực tế tại các doanh nghiệp vừa và trường đại học, từ đó xác định các yêu cầu cụ thể cho hệ thống . Tiếp theo, chương này trình bày kiến trúc tổng thể của hệ thống, bao gồm cấu trúc thư mục dự án được tổ chức theo chức năng (Controllers, Services, Models, Views, Middleware, Validators, Extensions). Chương cũng mô tả chi tiết mô hình dữ liệu của hệ thống, trong đó các bảng chính như Routers, RouterConfigurations, ConfigTemplates, ComplianceRules, và NotificationHistory được thiết kế với quan hệ dạng 1-nhiều. Về giao diện người dùng, chương này trình bày các màn hình chính như Dashboard tổng quan, trang quản lý thiết bị, trang backup/history, trang compliance, và trang settings. Đặc biệt, chương này đi sâu vào các thành phần chức năng của hệ thống, bao gồm các controller và API (RoutersController, ConfigManagementController, RestoreController, SettingsController), dịch vụ xử lý nghiệp vụ (ConfigurationManagementService, TelegramNotificationService, S3BackupService, AutomaticConfigurationChangeDetector), và hệ thống xử lý thông báo và giám sát. Cuối cùng, chương này cung cấp hướng dẫn chi tiết về cài đặt và triển khai hệ thống trong môi trường thực tế.

Chương 4: ỨNG DỤNG THỰC TIỄN VÀ MÔ PHỎNG VẬN HÀNH

Chương này trình bày các kịch bản sử dụng thực tế của hệ thống NCM, minh họa cách hệ thống giúp doanh nghiệp quản lý tập trung toàn bộ thiết bị mạng, theo dõi trạng thái thiết bị theo thời gian thực, chủ động sao lưu cấu hình, và ghi nhận mọi thao tác của quản trị viên. Chương này cũng mô tả chi tiết cách hệ thống tự động phát hiện thay đổi cấu hình và kiểm tra tuân thủ thông qua cơ chế giám sát liên tục, so sánh với template chuẩn, và gửi thông báo tức thì qua Telegram khi có thay đổi. Về tích hợp cloud, chương này giải thích cách hệ thống tự động sao lưu cấu hình lên AWS S3 để đảm bảo an toàn dữ liệu. Đặc biệt, chương này cung cấp các kịch bản kiểm thử chi tiết cho từng chức năng của hệ thống, từ việc thêm router mới, backup/restore cấu hình, xem lịch sử thiết bị, so sánh các phiên bản cấu hình, đến việc kiểm tra cảnh báo qua Telegram khi có thay đổi cấu hình.

Chương 5: KẾT LUẬN

Chương kết luận tổng kết các kết quả đã đạt được của đồ án, bao gồm việc xây dựng thành công hệ thống quản lý cấu hình mạng tự động với giao diện thân thiện và khả năng mở rộng tốt. Hệ thống đã đáp ứng được các nhu cầu nghiệp vụ thực tế như quản lý, backup, phục hồi, kiểm tra compliance, và cảnh báo đa kênh. Quan trọng hơn, hệ thống giúp giảm thiểu tối đa rủi ro do thao tác thủ công, tiết kiệm thời gian, tăng độ ổn định cho hệ thống mạng doanh nghiệp, và tăng cường khả năng audit và minh bạch trong mọi thao tác. Về định hướng phát triển tương lai, chương này đề xuất các hướng nghiên cứu và phát triển tiếp theo như bổ sung AI/Machine Learning để tự động nhận diện bất thường và dự đoán lỗi cấu hình, đa dạng hóa giao thức hỗ trợ để mở rộng cho nhiều loại thiết bị và OS mạng, phát triển mobile app để quản lý và nhận cảnh báo mọi lúc mọi nơi, tăng cường bảo mật thông qua xác thực đa lớp và mã hóa dữ liệu mạnh hơn, và tích hợp dashboard realtime và báo cáo phân tích nâng cao.

**CHƯƠNG 2:TỔNG QUAN VỀ ĐỀ TÀI**

## **2.1. Khái niệm cơ bản về quản lý cấu hình mạng (NCM)**

## ***2.1.1. Sự hình thành và phát triển của hệ thống quản lý cấu hình mạng***

## Quản lý cấu hình mạng (Network Configuration Management NCM) ra đời từ nhu cầu ngày càng tăng trong việc quản lý và kiểm soát các thay đổi trên thiết bị mạng. Ban đầu, việc quản lý cấu hình được thực hiện hoàn toàn thủ công thông qua việc lưu trữ các file văn bản. Với sự phức tạp ngày càng tăng của hệ thống mạng, các giải pháp tự động đầu tiên xuất hiện vào những năm 1990s, chủ yếu tập trung vào việc sao lưu cấu hình.

Sự bùng nổ của Internet và các dịch vụ đám mây trong thập kỷ 2010 đã dẫn đến sự ra đời của các hệ thống NCM thế hệ mới, có khả năng tự động phát hiện thay đổi, so sánh cấu hình và cảnh báo theo thời gian thực. Việc tích hợp với các dịch vụ đám mây như AWS S3 đã mở ra một kỷ nguyên mới trong việc lưu trữ và quản lý cấu hình mạng một cách an toàn và hiệu quả.

## ***2.1.2. Thế nào là hệ thống quản lý cấu hình mạng***

Hệ thống quản lý cấu hình mạng (NCM) là giải pháp phần mềm cho phép quản trị viên theo dõi, quản lý và kiểm soát các thay đổi cấu hình trên các thiết bị mạng như router, switch, firewall, v.v. Một hệ thống NCM hiện đại thường bao gồm các chức năng chính:

* Phát hiện và sao lưu tự động cấu hình thiết bị mạng
* Theo dõi và ghi nhật ký các thay đổi cấu hình
* So sánh cấu hình giữa các phiên bản hoặc với template chuẩn
* Cảnh báo khi phát hiện thay đổi không mong muốn
* Khôi phục cấu hình từ bản sao lưu khi cần thiết

## ***2.1.3. Phân loại hệ thống quản lý cấu hình mạng***

Các hệ thống NCM có thể được phân loại theo nhiều cách khác nhau:

*a) Theo phương thức triển khai:*

* Giải pháp Onpremises: Được cài đặt và vận hành trong môi trường nội bộ
* Giải pháp Cloudbased: Được cung cấp dưới dạng dịch vụ (SaaS)
* Giải pháp Hybrid: Kết hợp cả hai phương thức trên

*b) Theo quy mô hỗ trợ:*

* Giải pháp cho doanh nghiệp nhỏ (SMB)
* Giải pháp cho doanh nghiệp vừa và lớn (Enterprise)
* Giải pháp cho nhà cung cấp dịch vụ (Service Provider)

*c) Theo nhà sản xuất thiết bị được hỗ trợ:*

* Giải pháp đặc thù cho một nhà sản xuất (Cisco, Juniper, v.v.)
* Giải pháp đa nền tảng hỗ trợ nhiều nhà sản xuất khác nhau

## *2.1.4. Phương pháp* ***kết nối với thiết bị mạng***

Các hệ thống NCM sử dụng nhiều phương pháp khác nhau để kết nối và tương tác với thiết bị mạng:

*a) Kết nối SSH (Secure Shell):*

* Kết nối an toàn, mã hóa dữ liệu
* Cho phép thực thi lệnh từ xa và lấy cấu hình
* Hỗ trợ xác thực bằng username/password hoặc keybased

*b) Giao thức SNMP (Simple Network Management Protocol):*

* Cho phép giám sát và quản lý thiết bị mạng
* Hỗ trợ đọc các thông số hệ thống (SNMP GET)
* Phát hiện thay đổi qua các OID đặc biệt

*c) Telnet:*

* Phương thức kết nối đơn giản nhưng không bảo mật
* Ít được sử dụng trong môi trường hiện đại

*d) API (Application Programming Interface):*

* Cung cấp giao diện lập trình cho phép tương tác với thiết bị
* Hỗ trợ REST, SOAP, NETCONF, v.v.
* Phù hợp với các thiết bị mạng thế hệ mới

## **2.2. Tổng quan về hệ thống quản lý cấu hình mạng tự động (Automated NCM)**

## ***2.2.1. Tại sao cần tự động hóa quản lý cấu hình mạng***

Việc tự động hóa quản lý cấu hình mạng mang lại nhiều lợi ích:

* Giảm thiểu lỗi do con người: Loại bỏ các lỗi thường gặp khi thực hiện thủ công
* Tiết kiệm thời gian và chi phí: Giảm thời gian thực hiện các tác vụ lặp đi lặp lại
* Phản ứng nhanh với sự cố: Phát hiện và cảnh báo thay đổi cấu hình theo thời gian thực
* Nâng cao khả năng tuân thủ: Đảm bảo cấu hình tuân thủ các chính sách và tiêu chuẩn
* Sao lưu nhất quán: Đảm bảo tất cả thiết bị được sao lưu theo lịch định sẵn

***2.2.2. Khái niệm NCM tự động***

NCM tự động là hệ thống quản lý cấu hình mạng có khả năng thực hiện các tác vụ một cách tự động mà không cần sự can thiệp trực tiếp của quản trị viên. Các tính năng tự động bao gồm:

* Phát hiện thay đổi tự động: Sử dụng các cơ chế giám sát để phát hiện khi cấu hình thiết bị thay đổi
* Sao lưu tự động: Tự động sao lưu cấu hình theo lịch hoặc khi phát hiện thay đổi
* Phân tích tự động: So sánh và phân tích sự khác biệt giữa các phiên bản cấu hình
* Thông báo tự động: Gửi cảnh báo khi phát hiện thay đổi không mong muốn
* Khắc phục tự động: Khôi phục cấu hình trước đó khi phát hiện vấn đề

## ***2.2.3. Đặc trưng của NCM tự động***

Một hệ thống NCM tự động hiện đại có các đặc trưng sau:

* Tính chủ động: Chủ động phát hiện và xử lý thay đổi thay vì phản ứng sau sự cố
* Khả năng mở rộng: Dễ dàng mở rộng để hỗ trợ nhiều thiết bị và nhà sản xuất khác nhau
* Tích hợp đa dịch vụ: Tích hợp với các hệ thống khác như ITSM, giám sát, cảnh báo
* Lập lịch linh hoạt: Cho phép thiết lập lịch sao lưu tự động theo nhiều tiêu chí
* Bảo mật cao: Đảm bảo các thông tin cấu hình và thông tin xác thực được bảo vệ

## ***2.2.4. Ưu và nhược điểm của hệ thống NCM tự động***

Ưu điểm:

* Giảm thiểu thời gian và công sức quản lý cấu hình mạng
* Phát hiện và khắc phục sự cố nhanh chóng
* Đảm bảo tính nhất quán và tuân thủ chính sách
* Lưu trữ lịch sử thay đổi đầy đủ, hỗ trợ kiểm toán
* Giảm thiểu thời gian chết của hệ thống khi xảy ra sự cố

Nhược điểm:

* Chi phí triển khai ban đầu có thể cao
* Yêu cầu kỹ năng kỹ thuật để cài đặt và cấu hình
* Phụ thuộc vào kết nối mạng để hoạt động
* Có thể gặp khó khăn với các thiết bị mạng cũ hoặc không tiêu chuẩn
* Cần được cập nhật liên tục để đảm bảo tính bảo mật

## ***2.2.5. Các mô hình triển khai NCM***

1. Mô hình Onpremises:

* Triển khai trên hạ tầng nội bộ của tổ chức
* Toàn quyền kiểm soát dữ liệu và quy trình
* Phù hợp với tổ chức có yêu cầu bảo mật cao

2. Mô hình Cloudbased:

* Triển khai trên nền tảng đám mây (AWS, Azure, GCP)
* Dễ dàng mở rộng và cập nhật
* Tiết kiệm chi phí đầu tư hạ tầng

3. Mô hình Hybrid:

* Kết hợp giữa onpremises và cloud
* Tận dụng ưu điểm của cả hai mô hình
* Phù hợp với nhiều tổ chức có nhu cầu đa dạng

## ***2.2.6. Lưu trữ cấu hình trên AWS S3***

AWS S3 (Simple Storage Service) là dịch vụ lưu trữ đối tượng của Amazon Web Services, cung cấp một nền tảng lý tưởng để lưu trữ các bản sao lưu cấu hình mạng:

1. Đặc điểm của AWS S3:

* Tính khả dụng cao (99.99%)
* Độ bền dữ liệu vượt trội (99.999999999%)
* Khả năng mở rộng không giới hạn
* Hỗ trợ nhiều lớp lưu trữ với chi phí khác nhau
* Tích hợp với nhiều dịch vụ AWS khác

2. Cơ chế bảo mật của S3:

* Mã hóa phía máy chủ (SSE)
* Chính sách truy cập (Bucket Policy)
* Danh sách kiểm soát truy cập (ACL)
* Xác thực đa yếu tố (MFA Delete)
* Quản lý phiên bản (Versioning)

3. Ứng dụng S3 trong NCM:

* Lưu trữ dài hạn các bản sao lưu cấu hình
* Quản lý phiên bản và lịch sử thay đổi
* Khôi phục nhanh chóng khi cần thiết

Truy cập an toàn từ bất kỳ đâu

## ***2.2.7. Phương pháp phát hiện thay đổi cấu hình***

1. Phát hiện dựa trên SNMP:

* Sử dụng OID đặc biệt để theo dõi thời gian thay đổi cuối cùng
* Polling định kỳ để kiểm tra thay đổi
* Ít tạo tải trên thiết bị mạng

2. Phát hiện dựa trên SSH:

* Kết nối trực tiếp đến thiết bị để lấy cấu hình hiện tại
* So sánh với phiên bản được lưu trữ trước đó
* Cung cấp thông tin chi tiết về thay đổi

3. Phát hiện dựa trên Syslog:

* Theo dõi các thông báo syslog từ thiết bị
* Phát hiện sự kiện liên quan đến thay đổi cấu hình
* Gần như theo thời gian thực

## ***2.2.8. Các thành phần chính của hệ thống NCM tự động***

1. Thành phần quản lý kết nối:

* Thiết lập và duy trì kết nối đến các thiết bị mạng
* Xử lý xác thực và phân quyền
* Đảm bảo kết nối an toàn và hiệu quả

2. Thành phần phát hiện thay đổi:

* Giám sát liên tục các thiết bị mạng
* Phát hiện khi có thay đổi cấu hình
* Kích hoạt các quy trình sau khi phát hiện thay đổi

3. Thành phần sao lưu và lưu trữ:

* Thực hiện sao lưu cấu hình
* Quản lý lưu trữ cục bộ và đám mây (AWS S3)
* Duy trì lịch sử phiên bản

4. Thành phần phân tích và so sánh:

* So sánh các phiên bản cấu hình
* Phân tích sự khác biệt
* Đánh giá tác động của thay đổi

5. Thành phần thông báo và cảnh báo:

* Gửi thông báo khi phát hiện thay đổi
* Tích hợp với các kênh thông báo như Email, SMS, Telegram
* Phân loại mức độ ưu tiên của cảnh báo

# 

# **CHƯƠNG 3. KHẢO SÁT, THIẾT KẾ VÀ CÀI ĐẶT HỆ THỐNG**

## **3.1. Khảo sát nhu cầu và yêu cầu hệ thống**

Trước khi xây dựng một hệ thống NCM tự động, nhóm phát triển đã tiến hành khảo sát thực tế ở một số doanh nghiệp quy mô vừa (hơn 50 thiết bị mạng) và trường đại học, nhận thấy những vấn đề chủ yếu sau:

* Thiếu giải pháp quản lý tập trung, mỗi thiết bị lưu file cấu hình riêng biệt.
* Chưa có công cụ kiểm tra thay đổi cấu hình tự động, mọi thao tác đều thủ công.
* Việc phục hồi cấu hình khi gặp sự cố chậm, ảnh hưởng lớn tới dịch vụ, hoạt động nội bộ.
* Đội ngũ IT phải thường xuyên kiểm tra lại cấu hình bằng tay, dễ bỏ sót hoặc bị lỗi do thao tác lặp lại.

Những vấn đề trên là động lực thúc đẩy việc xây dựng hệ thống , đáp ứng nhu cầu quản lý tự động, minh bạch, hiệu quả, dễ mở rộng trong thực tiễn.

**3.2. Phân tích thiết kế kiến trúc hệ thống**

## ***3.2.1. Cấu trúc thư mục dự án***

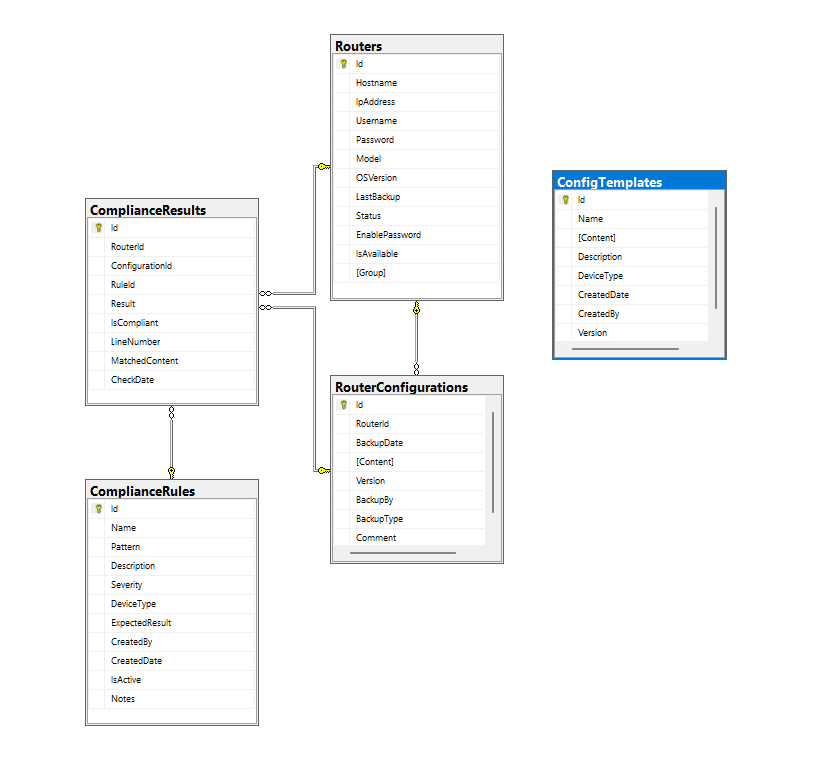
Dự án được tổ chức với cấu trúc logic, phân chia theo chức năng để thuận tiện phát triển, bảo trì:

* **Controllers/**: Chứa các bộ điều khiển xử lý yêu cầu HTTP, chia theo chức năng chính như quản lý thiết bị, cấu hình, backup, khôi phục, settings, v.v.
* **Services/**: Đảm nhiệm xử lý nghiệp vụ như so sánh cấu hình, kiểm tra compliance, gửi thông báo, giao tiếp với AWS S3.
* **Models/**: Định nghĩa các lớp dữ liệu, ánh xạ với database.
* **Views/**: Tập hợp các giao diện Razor View cho website.
* **Middleware/**: Xử lý các chức năng trung gian như logging, kiểm soát truy cập, quản lý ngoại lệ.
* **Validators/**: Kiểm tra, xác thực dữ liệu đầu vào, đảm bảo logic đúng.
* **Extensions/**: Các hàm mở rộng, tiện ích bổ trợ cho hệ thống.

## ***3.2.2. Mô hình dữ liệu***

Thiết kế cơ sở dữ liệu của bao gồm các bảng chính như:

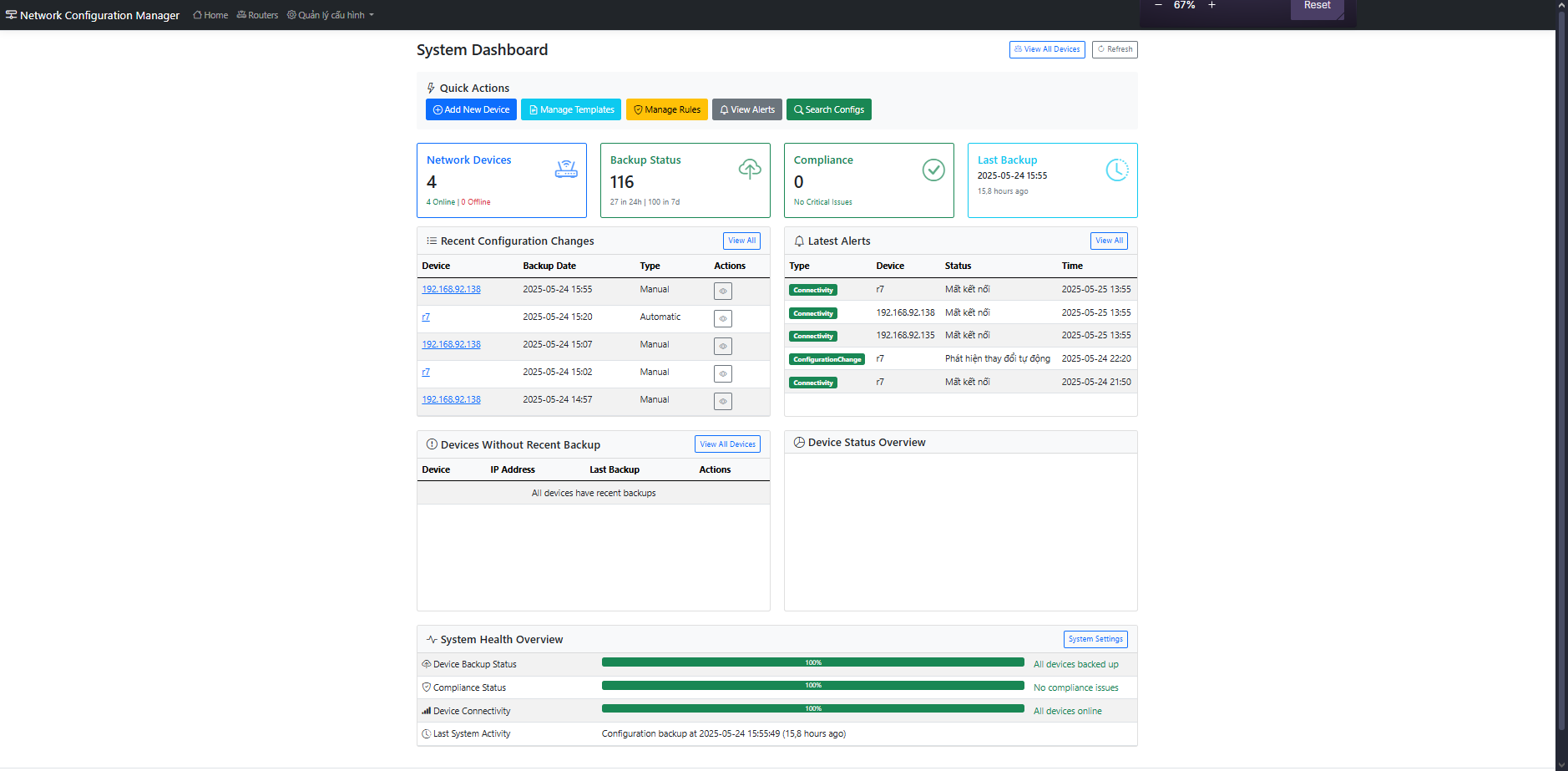
* **Routers**: Lưu thông tin thiết bị mạng (IP, loại thiết bị, trạng thái, mô hình, credentials).
* **RouterConfigurations**: Lưu trữ các bản sao lưu cấu hình thiết bị theo từng thời điểm.  
  **ConfigTemplates**: Các mẫu cấu hình chuẩn dùng để kiểm tra compliance.
* **ComplianceRules**: Bộ quy tắc kiểm tra cấu hình.
* **NotificationHistory**: Lịch sử gửi cảnh báo, sự kiện.  
   Quan hệ giữa các bảng thiết kế dạng quan hệ 1nhiều, đảm bảo dễ mở rộng, truy vấn, audit.

 ***Hình 3.1:*** *Sơ đồ ERD (Entity Relationship Diagram) cho hệ thống*

## ***3.2.3. Giao diện người dùng***

Giao diện được xây dựng theo hướng tối ưu trải nghiệm:

* **Dashboard tổng quan:** Thống kê số lượng thiết bị, trạng thái backup, lịch sử thay đổi, cảnh báo mới nhất.
* **Trang quản lý thiết bị:** Danh sách thiết bị, thêm mới, chỉnh sửa, kiểm tra kết nối, backup trực tiếp.
* **Trang backup/history:** Liệt kê các bản cấu hình đã backup, cho phép xem chi tiết, so sánh với mẫu chuẩn hoặc phục hồi nhanh.
* **Trang compliance:** Hiển thị kết quả kiểm tra tuân thủ, liệt kê lỗi, trạng thái từng thiết bị.
* **Trang settings:** Cài đặt thông báo, thông tin AWS S3, thiết lập lịch backup.

 ***Hình 3.2:*** *Ảnh chụp màn hình Trang Dashboard.*

## **3.3. Các thành phần chức năng**

## ***3.3.1. Các controller và API***

Mỗi controller phụ trách một nhóm chức năng riêng biệt, giao tiếp với frontend qua các API RESTful. Tiêu biểu:

* **RoutersController:** CRUD thiết bị, kiểm tra kết nối, backup thủ công.
* **ConfigManagementController:** So sánh cấu hình, kiểm tra compliance.
* **RestoreController:** Danh sách, chọn bản backup để phục hồi.
* **SettingsController:** Quản lý các cấu hình thông báo, kết nối cloud, tùy chỉnh hệ thống.

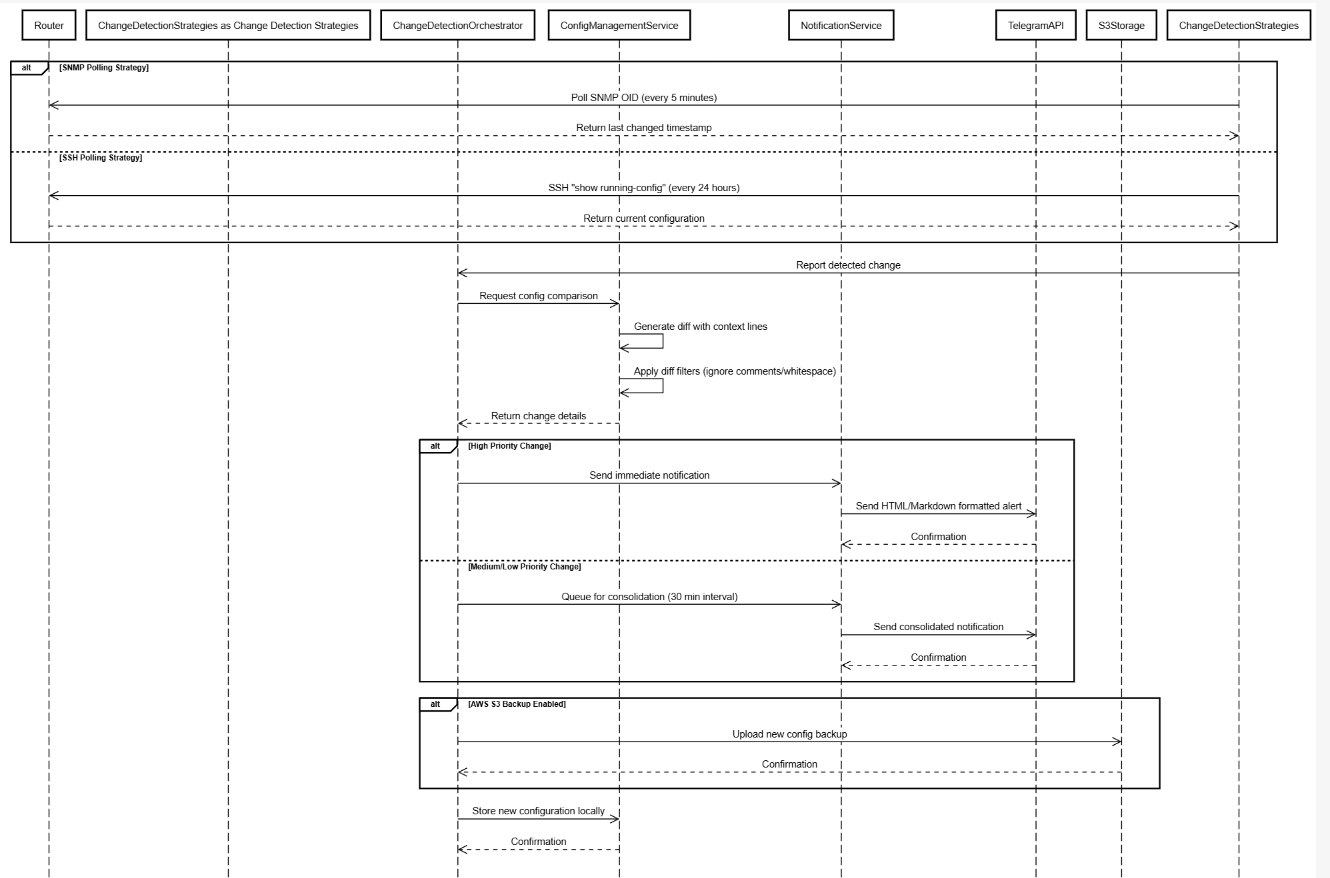
Các API được bảo vệ bằng xác thực (authentication), phân quyền (authorization), đảm bảo an toàn khi thao tác với thiết bị thực.

## ***3.3.2. Dịch vụ xử lý nghiệp vụ***

* **ConfigurationManagementService:** Quản lý nghiệp vụ cấu hình, kiểm tra compliance, tự động hóa backup.
* **TelegramNotificationService:** Gửi thông báo thay đổi, cảnh báo về cấu hình, trạng thái thiết bị đến nhóm quản trị viên.
* **S3BackupService:** Tích hợp lưu trữ backup lên AWS S3, đảm bảo backup không chỉ tồn tại tại chỗ mà còn an toàn trên cloud.
* **AutomaticConfigurationChangeDetector:** Theo dõi liên tục, phát hiện bất kỳ thay đổi nào về cấu hình, từ đó chủ động backup hoặc gửi cảnh báo.

## ***3.3.3. Xử lý thông báo và giám sát***

Hệ thống ghi nhận mọi sự kiện, thao tác trên thiết bị/network, tạo log tập trung, truy vết mọi thay đổi cho audit, kiểm tra bảo mật định kỳ.

 ***Hình 3.3:*** *Minh họa sơ đồ luồng xử lý cảnh báo khi phát hiện thay đổi cấu hình (sequence diagram).*

## **3.4. Hướng dẫn cài đặt và triển khai**

Quy trình triển khai được chuẩn hóa, dễ thao tác:

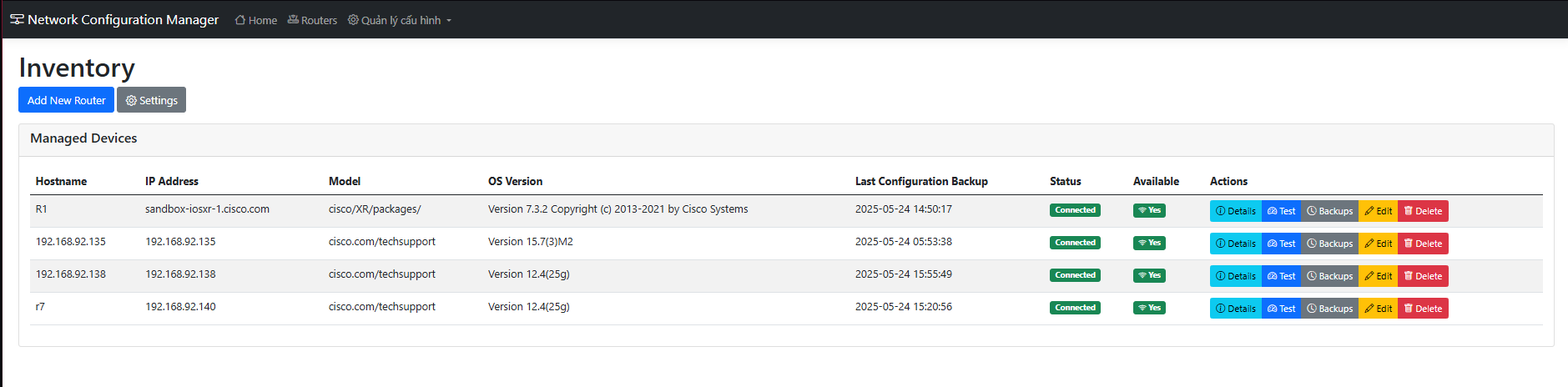
* **Cài đặt môi trường:** Chuẩn bị .NET Core 8.0, SQL Server, đăng ký tài khoản AWS S3, Telegram Bot.
* **Cấu hình file appsettings.json:** Khai báo chuỗi kết nối DB, thông tin AWS S3, token Telegram.  
  **Tích hợp thiết bị thực tế:** Thêm danh sách thiết bị, nhập thông tin đăng nhập, kiểm tra kết nối thực tế.

# **CHƯƠNG 4. ỨNG DỤNG THỰC TIỄN VÀ MÔ PHỎNG VẬN HÀNH**

## **4.1. Quản lý thiết bị mạng thực tế**

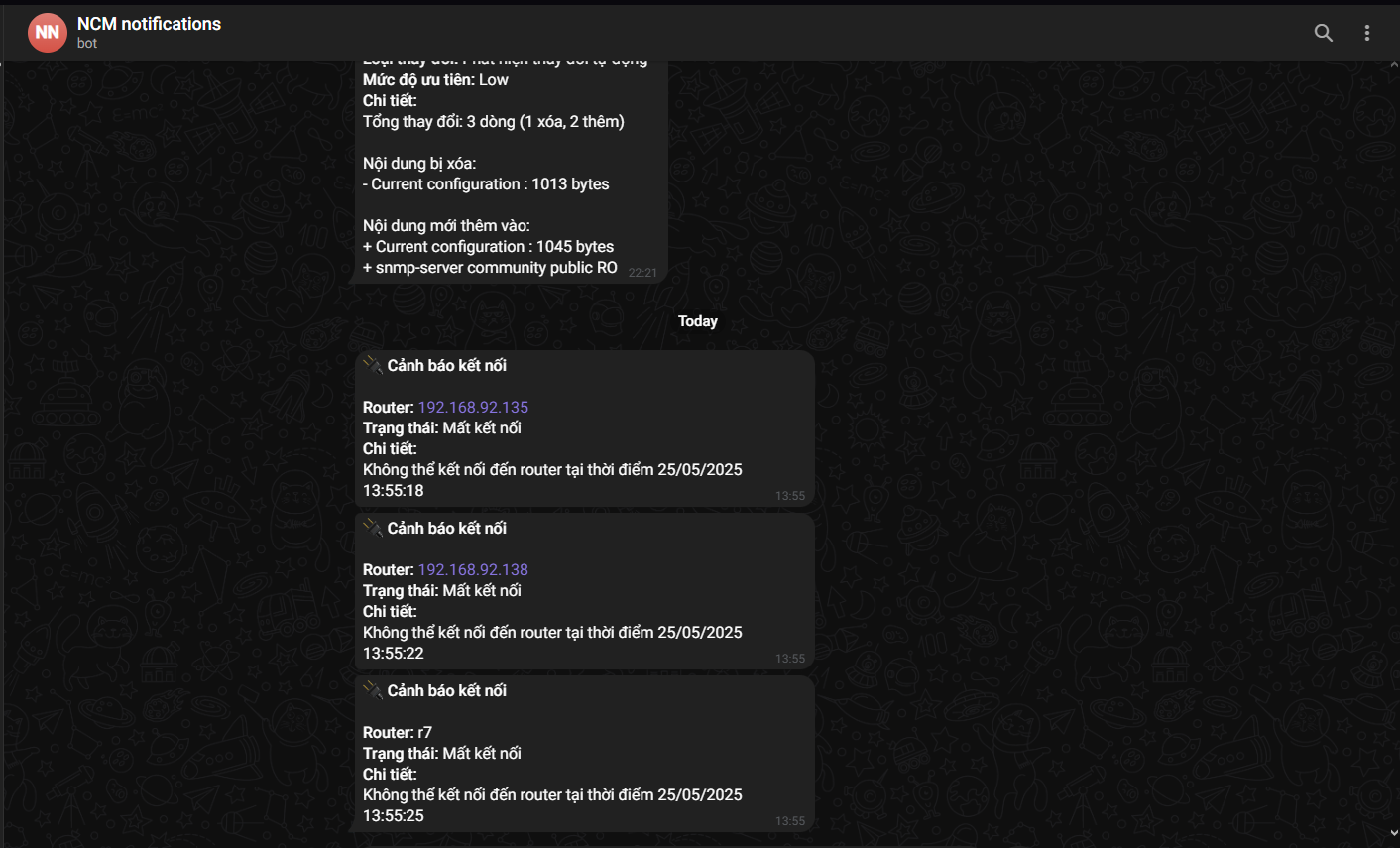
Sau khi triển khai hệ thống, doanh nghiệp dễ dàng:

* **Quản lý tập trung** toàn bộ thiết bị mạng ở các phòng ban/văn phòng chi nhánh, không cần phải truy cập từng thiết bị riêng lẻ.
* **Theo dõi trạng thái thiết bị** realtime, kiểm tra tình trạng online, offline, phiên bản phần mềm/hardware.  
  **Chủ động backup**: Lập lịch backup định kỳ, hoặc backup ngay khi phát hiện sự thay đổi.
* **Audit thao tác**: Ghi nhận, truy vết mọi thao tác của quản trị viên trên thiết bị.

  ***Hình 4.1****: giao diện danh sách thiết bị mạng với trạng thái realtime.*

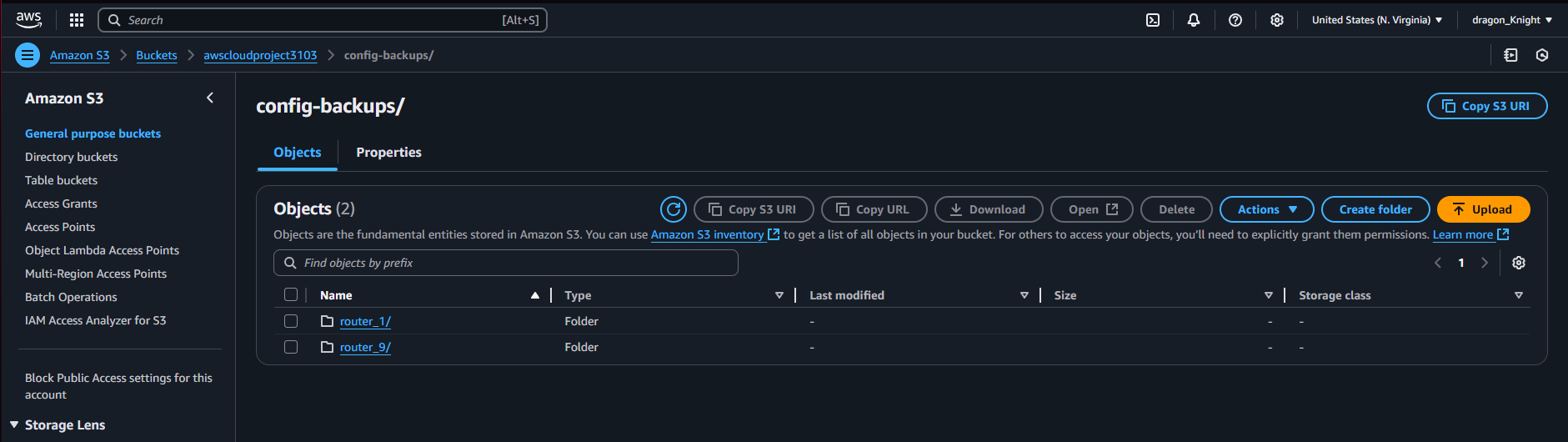
## **4.2. Tự động phát hiện thay đổi và kiểm tra tuân thủ**

* **Cơ chế giám sát liên tục**: Dịch vụ theo dõi cấu hình thiết bị, bất kỳ thay đổi nào cũng lập tức được ghi nhận.
* **So sánh với template chuẩn**: Tự động đối chiếu cấu hình mới với mẫu quy chuẩn, phát hiện lệch chuẩn.
* **Thông báo tức thì**: Khi có thay đổi, hệ thống gửi cảnh báo qua Telegram, webhook đến nhóm quản trị viên.
* **Lưu vết lịch sử**: Mọi thay đổi đều lưu vào database, thuận tiện kiểm tra, audit.

 **hình 4.2**: *Ảnh chụp thông báo Telegram khi có thay đổi cấu hình, minh họa bảng*  *lịch sử thay đổi.*

## **4.3. Tích hợp cloud và lưu trữ an toàn**

* **Sao lưu trên AWS S3**: Khi backup cấu hình, hệ thống tự động đẩy lên AWS S3, đảm bảo dữ liệu an toàn khi xảy ra sự cố hạ tầng cục bộ (cháy nổ, mất điện, v.v.).
* **Có thể mở rộng** sang các dịch vụ cloud khác như Azure, Google Cloud tùy yêu cầu.

 ***Ảnh 4.3****: minh họa dashboard AWS S3 hiển thị các file backup cấu hình.*

## **4.4. Xây dựng kịch bản kiểm thử**

## 4.4.1. Kiểm thử chức năng quản lý thiết b**ị:** Thêm router mới vào hệ thống

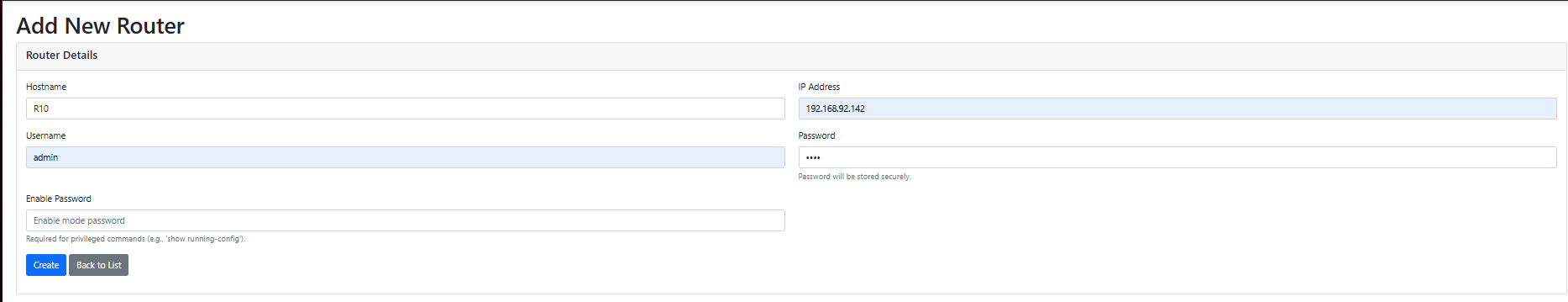
Kịch bản kiểm thử này đánh giá khả năng thêm mới thiết bị router vào hệ thống . Quy trình bắt đầu bằng việc truy cập vào menu "Routers" hoặc "Quản lý Router" từ thanh điều hướng chính. Sau đó người dùng nhấp vào nút "Thêm Router" để mở biểu mẫu nhập thông tin.

bước 1 . Truy cập menu "Routers" hoặc "Quản lý Router"

bước 2. Nhấp vào nút "Thêm Router"

bước 3. Nhập thông tin router: Hostname, địa chỉ IP, thông tin xác thực (username, password, enable password)

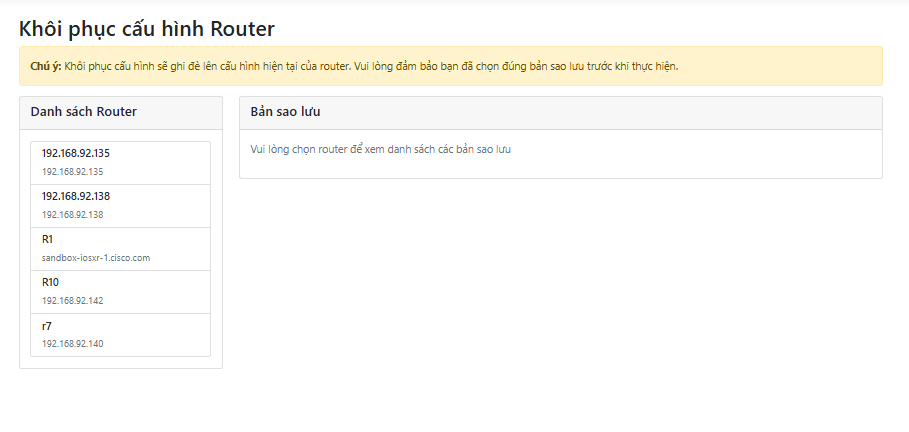
bước 4. Lưu thông tin router mới

  ***hình 4.4****: Ảnh minh họa khi thêm router mới vào hệ thống.*

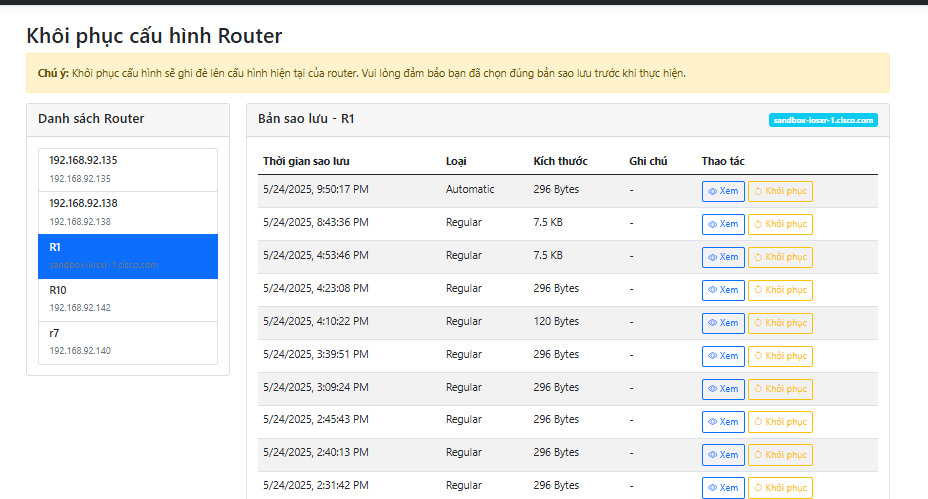
## 4.4.2. Kiểm thử backup/restore: khôi cấu hình thủ công

Kịch bản này kiểm tra khả năng sao lưu và khôi phục cấu hình router theo cách thủ công. Quy trình bắt đầu khi người dùng truy cập vào menu "Config Management" từ thanh điều hướng chính, nơi hiển thị danh sách các router đã được cấu hình trong hệ thống.

bước 1. Truy cập menu "Config Management"

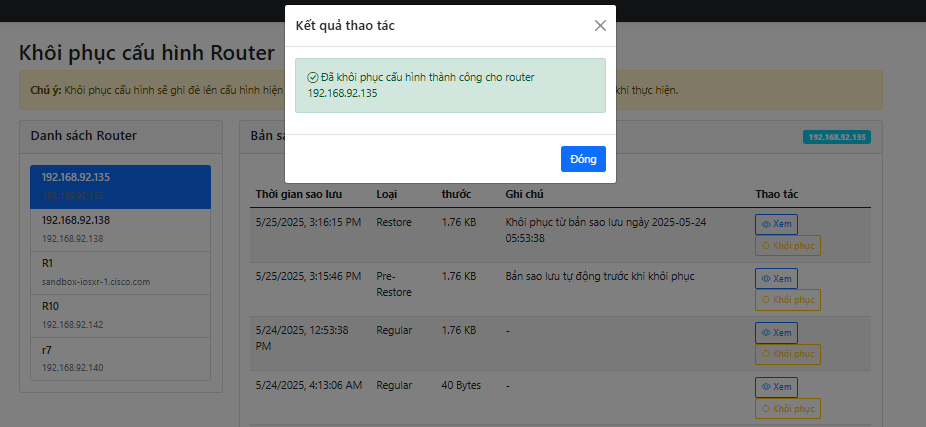
 ***Hình 4.5:*** *Ảnh minh họa trang khôi phục cấu hình router trước khi chọn cấu hình.*

bước 2. Chọn router cần backup

 *Hình 4.6: sau khi chọn khi cấu hình*

bước 3. Nhấp vào nút "khôi phục" để tạo bản sao lưu thủ công

bước 4. Xem kết quả backup



*Hình 4.7: sau khi đã khôi phục thành công*

## 

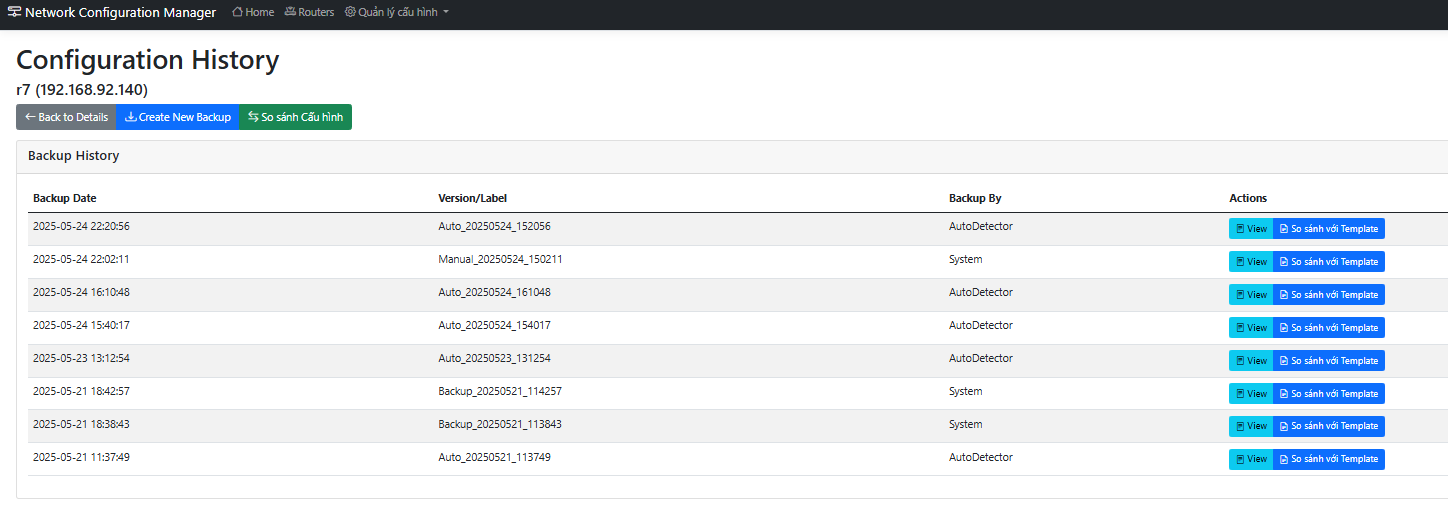
## 4.4.3. Kiểm thử xem lịch sử thiết bị: xem lại những config cũ đã được cấu hình

## Kịch bản này kiểm tra chức năng xem lịch sử cấu hình của thiết bị. Quy trình bắt đầu khi người dùng truy cập vào menu "Config Management" và chọn router cần xem lịch sử cấu hình từ danh sách thiết bị có sẵn.

## bước 1. Truy cập menu "Config Management"

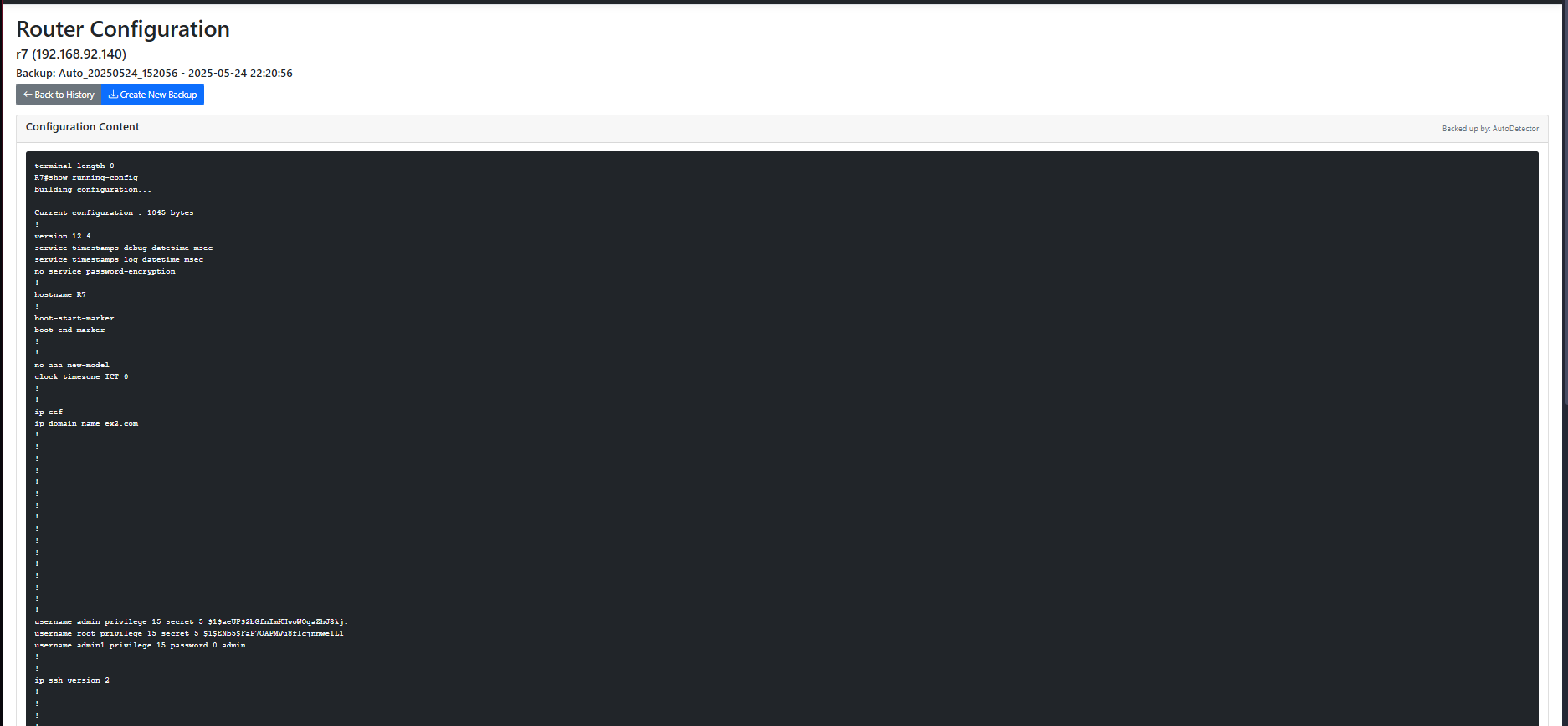
bước 2. Chọn router cần xem lịch sử

bước 3. Xem danh sách các bản backup theo thời gian



*hình 4.8: trang configuration history của router*

bước 4. Chọn bản backup để xem chi tiết cấu hình

*hình 4.9: trang hiển thị chi tiết config đã lưu của router*

## 4.4.4. Kiểm thử so sánh các phiên bản cấu hình:

Kịch bản này kiểm tra chức năng so sánh giữa các phiên bản cấu hình khác nhau của cùng một thiết bị. Quy trình bắt đầu khi người dùng truy cập chức năng "So sánh cấu hình" từ menu "Config Management" hoặc từ trang lịch sử cấu hình của một router cụ thể.

Để mô phỏng tình huống thực tế, người kiểm thử truy cập trực tiếp vào router thông qua kết nối SSH (không thông qua hệ thống ) và thực hiện một số thay đổi cấu hình, ví dụ như thêm một ACL mới hoặc thay đổi cấu hình VLAN. Sau khi thay đổi được áp dụng và lưu vào router, người kiểm thử đợi hệ thống phát hiện thay đổi.

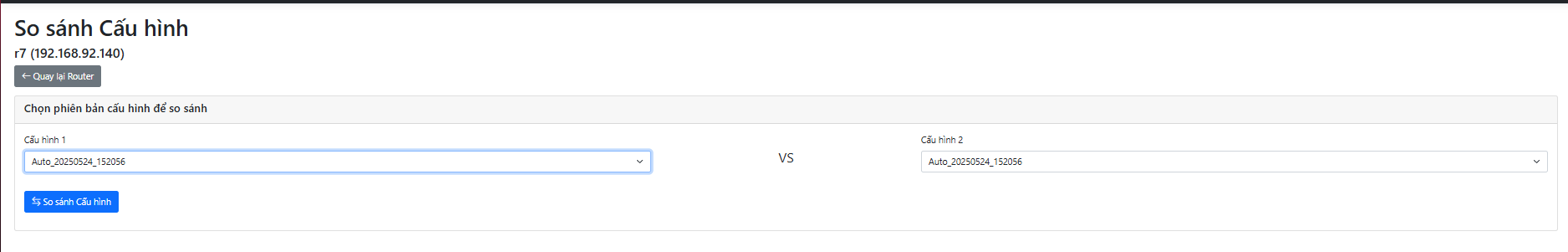
Hệ thống , thông qua dịch vụ giám sát định kỳ (mặc định chạy 5-15 phút một lần), sẽ kết nối đến router, lấy cấu hình hiện tại và so sánh với bản sao lưu gần nhất. Khi phát hiện thay đổi, hệ thống sẽ:

* Tạo một bản sao lưu mới của cấu hình hiện tại
* Phân tích sự khác biệt để xác định loại và mức độ quan trọng của thay đổi
* Gửi thông báo qua Telegram với thông tin chi tiết về thay đổi phát hiện được
* Lưu sự kiện vào lịch sử cảnh báo của hệ thống

Thông báo Telegram sẽ bao gồm tên router, thời gian phát hiện thay đổi, tóm tắt các thay đổi quan trọng, và đường dẫn để xem chi tiết trong hệ thống . Người kiểm thử xác nhận rằng thông báo được nhận chính xác và kịp thời, và các thay đổi đã thực hiện được báo cáo đúng.

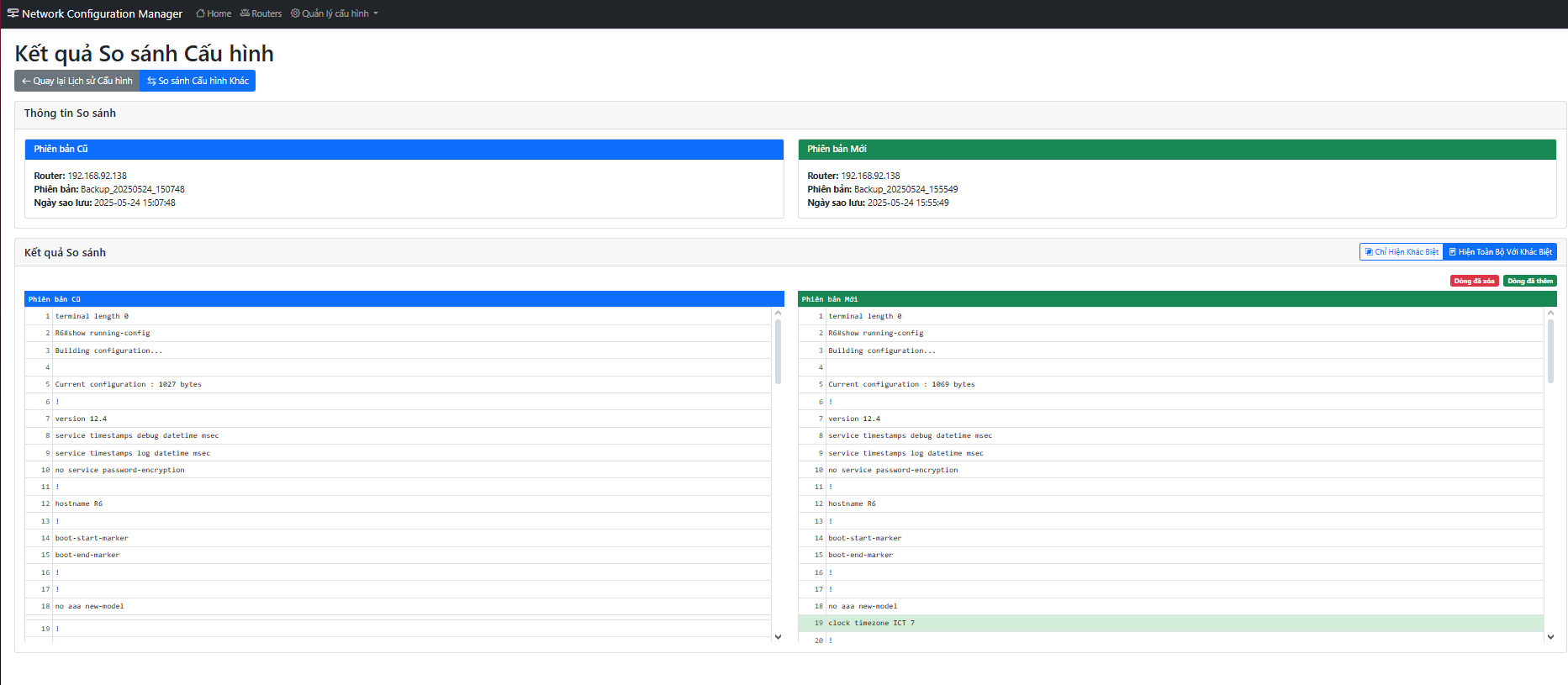
bước **1.** Chọn phiên bản cấu hình để so sánh

bước **2.** Chọn router và hai phiên bản cấu hình cần so sánh



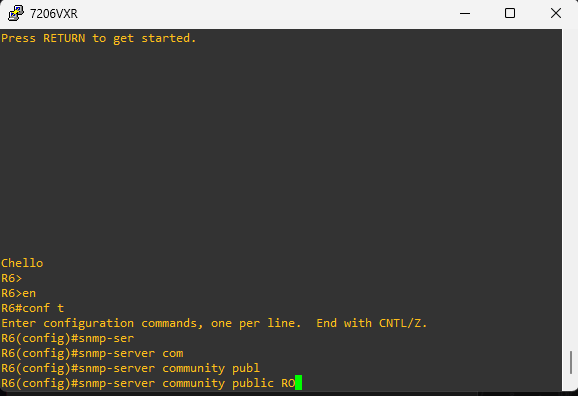
*hình 4.10: trang so sánh cấu hình*

bước **3**.xem sự khác biệt giữa 2 cấu hình đã chọn

  
*hình 4.11: trang kết quả so sánh*

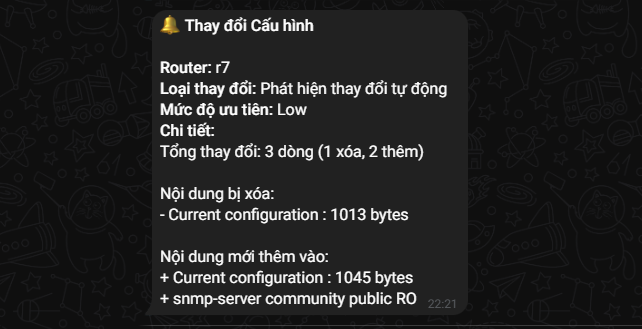
## 4.4.5. Kiểm thử cảnh báo: Ngắt kết nối, sửa cấu hình sai chuẩn, kiểm tra Telegram có thông báo đúng thời gian thực.

Kịch bản này kiểm tra khả năng phát hiện thay đổi cấu hình và gửi thông báo tự động của hệ thống. Quy trình bắt đầu bằng việc thiết lập môi trường kiểm thử với một router được giám sát bởi hệ thống , đã cấu hình hệ thống cảnh báo qua Telegram.

bước 1.Chỉnh sửa cấu hình qua kết nối ssh bằng CLI trên router.  


*hình 4.12: bảng CLI mở bằng PUTTY sử dụng SSH*

bước 2.Kết quả nhận về Telegram



*hình 4.13: thông báo telegram được gửi về*

# 

# **CHƯƠNG 5. KẾT LUẬN**

## **5.1. Những kết quả đạt được**

* Đã xây dựng thành công hệ thống quản lý cấu hình thiết bị mạng tự động hóa, giao diện thân thiện, khả năng mở rộng tốt.
* Hệ thống đáp ứng được các nhu cầu nghiệp vụ thực tế: quản lý, backup, phục hồi, kiểm tra compliance, cảnh báo đa kênh.
* Giảm thiểu tối đa rủi ro do thao tác thủ công, tiết kiệm thời gian, tăng độ ổn định cho hệ thống mạng doanh nghiệp.
* Tăng cường khả năng audit, minh bạch hóa mọi thao tác, dễ truy vết khi có sự cố.

## **5.2. Định hướng phát triển tương lai**

* **Bổ sung AI, Machine Learning**: Tự động nhận diện bất thường, dự đoán lỗi cấu hình dựa trên hành vi, lịch sử.
* **Đa dạng hóa giao thức hỗ trợ**: Mở rộng cho nhiều loại thiết bị, OS mạng (Linux, Windows Server, thiết bị IoT).
* **Phát triển mobile app**: Quản lý, nhận cảnh báo mọi lúc mọi nơi.
* **Tăng cường bảo mật**: Xác thực đa lớp (2FA), mã hóa dữ liệu mạnh hơn, RBAC chi tiết.
* **Tích hợp dashboard realtime, báo cáo phân tích nâng cao**.

# **TÀI LIỆU THAM KHẢO**

1. Amazon Web Services (2023). AWS SDK for .NET Documentation. <https://docs.aws.amazon.com/sdkfornet>
2. SolarWinds (2022). Network Configuration Manager Documentation. <https://www.solarwinds.com/networkconfigurationmanager>
3. SSH.NET Documentation:

<https://sshnet.github.io/SSH.NET/>

1. Telegram (2023). Telegram Bot API Documentation. [https://core.telegram.org/bots/ap](https://core.telegram.org/bots/api)i
2. Cisco SNMP OID Reference: <https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do>
3. AWS S3 .NET SDK Documentation: <https://docs.aws.amazon.com/sdkfornet/v3/developerguide/s3apisintro.html>
4. IHostedService Documentation: <https://docs.microsoft.com/enus/aspnet/core/fundamentals/host/hostedservice>
5. Cisco Configuration Best Practices: <https://www.cisco.com/c/en/us/support/docs/ip/accesslists/1360821.html>
6. Phan Văn Đức, (2021), Xây dựng hệ thống mạng lan cho doanh nghiệp, đồ án đại học,TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM.  
   [docs.google.com/document/d/1ePYrCp6IAEOVfZ3jqr7XSF-r20m-uhYO/edit?usp=drive\_web&ouid=102507029811748393777&rtpof=true](http://docs.google.com/document/d/1ePYrCp6IAEOVfZ3jqr7XSF-r20m-uhYO/edit?usp=drive_web&ouid=102507029811748393777&rtpof=true)