**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

****

**NGUYỄN THANH TÙNG – 23521744**

**ĐỖ ĐỨC MINH TRIẾT - 23521650**

**BÁO CÁO ĐỒ ÁN CUỐI KỲ**

**EVALUATING NETWORK CONGESTION CONTROL WITH IPERF3 AND LINUX TRAFFIC CONTROL (TC/NETEM)**

**GIẢNG VIÊN HƯỚNG DẪN**

**LÊ TRUNG QUÂN**

**NGUYỄN VĂN BẢO**

**TP. HỒ CHÍ MINH, 2025**

**Mục lục**

[I. CƠ SỞ LÝ THUYẾT 5](#_Toc212040778)

[**1.1. ARRIVAL PROCESSES (QUÁ TRÌNH ĐẾN) 5**](#_Toc212040779)

[**1.2. MÔ HÌNH HÀNG ĐỢI CƠ BẢN** 6](#_Toc212040780)

[**1.3. RED (Random Early Detection) 7**](#_Toc212040781)

[1. Nguyên lý hoạt động: 7](#_Toc212040782)

[2. Ưu điểm: 7](#_Toc212040783)

[**1.4. Cubic (TCP Congestion Control) 7**](#_Toc212040784)

[1. Ý tưởng chính: 7](#_Toc212040785)

[2. Ưu điểm: 8](#_Toc212040786)

**Hình ảnh**

[Hình 1. Sơ đồ mô hình 13](#_bookmark16)

[Hình 2. Giao diện Guacamole 14](#_bookmark19)

[Hình 3. Giao diện khi đăng nhập bằng tài khoản toàn quyền 15](#_bookmark20)

[Hình 4. Các user hiện tại có trong cơ sở dữ liệu 16](#_bookmark22)

[Hình 5. Các kết nối được tạo 16](#_bookmark23)

[Hình 6. Phân quyền cho từng user 17](#_bookmark24)

[Hình 7. Ví dụ về file và vị trí hiện tại 19](#_bookmark28)

[Hình 8. Sơ đồ thực hiện replication 20](#_bookmark29)

[Hình 9. Kết quả sau khi truy cập Guacamole web 22](#_bookmark41)

[Hình 10. Sơ đồ kết nối giữa 3 máy 24](#_bookmark48)

**Bảng**

[Bảng 1. Lệnh tạo chứng chỉ và khóa riêng 20](#_bookmark32)

[Bảng 2. Chuyển đổi certificate và key sang file keystore dạng PKCS12 21](#_bookmark34)

[Bảng 3. Cấu hình connector 21](#_bookmark36)

[Bảng 4. Khởi động lại tomcat 22](#_bookmark38)

[Bảng 5. Truy cập vào Guacamole web 22](#_bookmark40)

[Bảng 6. Cấu hình HAProxy 23](#_bookmark46)

[Bảng 7. Bảng phân công công việc 27](#_bookmark51)

# I. CƠ SỞ LÝ THUYẾT

## 1.1. ARRIVAL PROCESSES (QUÁ TRÌNH ĐẾN)

Trong lý thuyết hàng đợi, **arrival process** mô tả cách các gói tin (hoặc khách hàng) đến hệ thống theo thời gian.

Các đặc trưng chính của arrival process gồm:

* **Tốc độ đến trung bình (λ - arrival rate)**: số gói đến trung bình trong một đơn vị thời gian.
* **Phân phối thời gian giữa các lần đến (inter-arrival time)**: thời gian giữa hai gói tin liên tiếp.

**Các mô hình arrival phổ biến:**

* **Deterministic Arrival (D)**: gói đến theo chu kỳ cố định.
* **Poisson Process (M)**: thời gian giữa các gói đến tuân theo phân phối mũ — đây là mô hình phổ biến nhất do tính chất “không nhớ” (*memoryless*).
* **General Arrival (G)**: thời gian đến có phân phối bất kỳ.

Trong mô hình hàng đợi, ký hiệu M/D/1, M/M/1, v.v… biểu diễn:

* Chữ đầu: loại arrival process (M – Markov/Poisson, D – deterministic).
* Chữ thứ hai: loại service time distribution.
* Số cuối: số lượng server (thường là 1).

**1.2. MÔ HÌNH HÀNG ĐỢI CƠ BẢN**

**Hệ thống hàng đợi được mô tả bởi các thành phần:**

|  |  |
| --- | --- |
| **Thành phần** | **Ý nghĩa** |
| **Arrival Process** | Cách các gói tin đến hàng đợi |
| **Service Process** | Cách hệ thống xử lý (truyền) từng gói |
| **Queue Discipline** | Quy tắc chọn gói tiếp theo để phục vụ (ví dụ: FIFO, Priority, Round Robin) |
| **Number of Servers** | Số tiến trình phục vụ đồng thời |
| **System Capacity** | Số lượng gói tối đa hệ thống có thể chứa |
| **Population Source** | Tổng số nguồn có thể sinh gói (hữu hạn hoặc vô hạn) |

Bảng 1. Hệ thống hàng đợi

**1. Một số mô hình hàng đợi chuẩn:**

* **M/M/1**: Arrival Poisson, service time exponential, 1 server.

với .

* **M/M/1/K**: Có giới hạn hàng đợi K (mất gói khi hàng đầy).
* **M/D/1**: Service time cố định, giúp giảm độ dao động trễ.

Các mô hình này giúp mô phỏng và đánh giá **hiệu năng của bộ định tuyến hoặc link mạng**, như độ trễ trung bình, xác suất mất gói và thông lượng.

## 1.3. RED (RANDOM EARLY DETECTION)

**RED** là một cơ chế quản lý hàng đợi chủ động (**AQM – Active Queue Management**) nhằm tránh hiện tượng **tắc nghẽn toàn cục (global synchronization)** trong mạng TCP.

### 1. Nguyên lý hoạt động:

* RED không chờ hàng đợi đầy mới loại bỏ gói, mà **bắt đầu loại ngẫu nhiên sớm hơn**, khi độ dài trung bình của hàng vượt ngưỡng.
* Tính **độ dài trung bình (avg\_len)** bằng bộ lọc trung bình trượt theo hàm mũ:
* Khi vượt qua **min\_th** (ngưỡng dưới), gói sẽ bị **drop** hoặc **mark (ECN)** với xác suất tăng dần cho đến **max\_th** (ngưỡng trên).

### 2. Ưu điểm:

* Giảm hiện tượng đồng bộ hóa mất gói của TCP.
* Duy trì độ trễ ổn định.
* Tăng thông lượng và hiệu quả đường truyền.

**3. Nhược điểm:**

* Khó cấu hình các tham số (min\_th, max\_th, w\_q).
* Không tối ưu trong các mạng có tải thay đổi nhanh.

## 1.4. CUBIC (TCP CONGESTION CONTROL)

**Cubic** là thuật toán điều khiển tắc nghẽn TCP mặc định trong hầu hết các nhân Linux hiện nay (thay thế cho Reno và BIC).

### 1. Ý tưởng chính:

* Thay vì tăng tuyến tính như **Reno**, Cubic tăng theo **hàm bậc ba (cubic function)** của thời gian kể từ lần mất gói gần nhất.
  + : cửa sổ nghẽn tại thời điểm t
  + : cửa sổ tại thời điểm mất gói gần nhất
  + : hằng số tăng
  + : khoảng thời gian để cwnd đạt lại

### 2. Ưu điểm:

* Phục hồi nhanh sau mất gói.
* Tận dụng tốt băng thông trong mạng tốc độ cao – độ trễ lớn (high-BDP).
* Giữ ổn định khi tải cao.

## 1.5. Các hàng đợi (qdisc) phổ biến trong Linux

**Qdisc (Queueing Discipline)** là cơ chế trong Linux kernel để quản lý cách gói tin được xếp hàng và gửi đi. Một số qdisc thường dùng:

**1. pfifo\_fast / pfifo**

* **pfifo**: đơn giản nhất, xếp hàng theo **FIFO (First In First Out)**, bỏ gói khi đầy.
* Thích hợp cho thử nghiệm cơ bản hoặc môi trường không cần kiểm soát trễ.

**2. RED (Random Early Detection)**

* Như mô tả ở trên, là qdisc AQM chủ động để giảm tắc nghẽn.
* Cấu hình trong Linux:

|  |
| --- |
| tc qdisc add dev eth0 root red limit 1000 min 200 max 600 avpkt 1000 burst 20 probability 0.02 |

Bảng 2. Ví dụ về cấu hình trong Linux của RED

**3. fq\_codel (Fair Queue Controlled Delay)**

* Là qdisc hiện đại, **kết hợp Codel (Controlled Delay)** và **Fair Queuing**.
* Tự động phát hiện và loại bỏ gói trễ quá lâu, giảm bufferbloat.
* Không cần tinh chỉnh tham số, hoạt động hiệu quả trong mạng thực tế.

|  |  |  |
| --- | --- | --- |
| **Qdisc** | **Đặc điểm chính** | **Loại** |
| **pfifo** | Đơn giản, FIFO | Passive |
| **RED** | Loại ngẫu nhiên sớm, chống tắc nghẽn | AQM |
| **fq\_codel** | Fair Queue + kiểm soát độ trễ tự động | AQM nâng cao |

Bảng 3. So sánh qdisc

## 1.6. iperf - Công Cụ Đo Băng Thông và Hiệu Năng

**Mục đích:** iperf3 là công cụ dòng lệnh được sử dụng rộng rãi để đo lường thông lượng tối đa (maximum throughput) trên mạng IP. Nó có thể kiểm tra hiệu năng của cả TCP và UDP.

**Nguyên lý hoạt động:**

* Thiết lập mô hình Client-Server. Máy chủ (server) lắng nghe kết nối, máy khách (client) khởi tạo và gửi dữ liệu.
* iperf3 tạo ra các luồng dữ liệu (streams) và gửi đi trong một khoảng thời gian xác định, sau đó báo cáo lại lượng dữ liệu đã truyền tải, từ đó tính toán ra băng thông đạt được.

**Các thông số quan trọng có thể đo được:**

* Bandwidth (Băng thông): Tốc độ truyền tải dữ liệu (Mbits/sec, MBytes/sec).
* Jitter (Độ biến động trễ): Sự thay đổi về độ trễ giữa các gói tin (chỉ cho UDP).
* Packet Loss (Tỷ lệ mất gói): Phần trăm gói tin bị mất trên đường truyền (chỉ cho UDP).

**Ứng dụng trong đồ án**: Dùng để kiểm chứng băng thông thực tế của liên kết mạng, so sánh hiệu năng giữa các cấu hình khác nhau (ví dụ: thay đổi kích thước cửa sổ TCP - window size), hoặc đánh giá hiệu quả của một giải pháp mạng mới.

## 1.7. tc (Traffic Control) và netem - Công Cụ Điều Khiển và Mô Phỏng Mạng

**Mục đích**: tc là công cụ mạnh mẽ trong Linux để điều khiển lưu lượng mạng. Kết hợp với module netem (Network Emulator), nó cho phép mô phỏng các điều kiện mạng không lý tưởng ngay trên một máy chủ.

**Nguyên lý hoạt động**:

* tc hoạt động bằng cách áp dụng các "qdisc" (queueing disciplines - kỷ luật xếp hàng) lên các giao diện mạng. Các qdisc này sẽ kiểm soát cách các gói tin được gửi đi, nhận về hoặc xử lý.
* netem là một loại qdisc đặc biệt, cung cấp khả năng thêm độ trễ, tỷ lệ mất gói, jitter, và nhiều hiện tượng mạng phức tạp khác.

**Các tình huống mạng có thể mô phỏng**:

* Độ trễ (Delay): netem delay 100ms 10ms
* Mất gói (Packet Loss): netem loss 5%
* Jitter: netem delay 100ms 20ms (độ trễ trung bình 100ms, dao động ±20ms).
* Gói tin trùng lặp (Duplication), Đảo thứ tự (Reordering), v.v.

**Ứng dụng trong đồ án**: Tạo ra một môi trường thử nghiệm có điều kiện mạng giống thực tế (ví dụ: mạng di động, đường truyền vệ tinh, hoặc mạng WAN có độ trễ cao) để đánh giá xem ứng dụng của bạn hoạt động như thế nào trong những điều kiện đó.

## 1.8. tcpdump - Công Cụ Phân Tích Gói Tin Mạng

**Mục đích**: tcpdump là công cụ phân tích giao thức mạng dựa trên dòng lệnh. Nó cho phép "bắt" (capture) và hiển thị các gói tin đang được truyền đi hoặc nhận về trên một giao diện mạng.

**Nguyên lý hoạt động**:

* tcpdump sử dụng thư viện libpcap để lấy các gói tin từ lớp driver của card mạng.
* Nó có thể lọc và hiển thị nội dung của các gói tin dựa trên nhiều tiêu chí (địa chỉ IP, cổng, giao thức, cờ TCP, v.v.).

**Thông tin chi tiết có thể thu thập**:

* Toàn bộ header của gói tin (Ethernet, IP, TCP/UDP, v.v.).
* Dữ liệu payload (nếu không mã hóa).
* Thời gian chính xác khi gói tin được gửi/ nhận.
* Các sự kiện trong quá trình bắt tay TCP (SYN, SYN-ACK, ACK) và kết thúc kết nối (FIN, RST).

**Ứng dụng trong đồ án**: Phân tích sâu các vấn đề về hiệu năng (ví dụ: xác định nguyên nhân độ trễ bằng cách phân tích các khoảng thời gian giữa các gói tin, phân tích hiện tượng tắc nghẽn thông qua cờ TCP Window, hoặc gỡ lỗi các kết nối không thành công).

## 1.9. ss - Công Cụ Thống Kê Socket

**Mục đích**: ss (socket statistics) là công cụ hiện đại thay thế cho netstat. Nó dùng để điều tra thông tin về socket, kết nối mạng, và các bảng routing.

**Nguyên lý hoạt động**:

* ss lấy thông tin trực tiếp từ nhân Linux thông qua giao diện netlink, làm cho nó nhanh hơn và hiệu quả hơn netstat trên các hệ thống có nhiều kết nối.

**Các thông tin quan trọng**:

* Danh sách tất cả các kết nối TCP, UDP, và UNIX socket.
* Trạng thái của kết nối (ESTABLISHED, TIME-WAIT, LISTEN, v.v.).
* Thông tin về bộ nhớ sử dụng (send/receive buffer), số gói tin đang chờ,...
* Thông tin chi tiết về cài đặt TCP (như rtt, cwnd - congestion window).

**Ứng dụng trong đồ án**: Giám sát trạng thái kết nối thời gian thực, phân tích vấn đề về kết nối (ví dụ: quá nhiều kết nối ở trạng thái TIME-WAIT), và thu thập các chỉ số hiệu năng cấp độ socket như kích thước cửa sổ tắc nghẽn.

## 1.10. ifstat - Công Cụ Thống Kê Lưu Lượng Giao Diện Mạng

**Mục đích**: ifstat là công cụ đơn giản để giám sát lưu lượng mạng trên các giao diện (interface) theo thời gian thực.

**Nguyên lý hoạt động:**

* ifstat định kỳ đọc các bộ đếm trong file /proc/net/dev (chứa thống kê về từng giao diện mạng) và tính toán tốc độ truyền tải dựa trên sự chênh lệch giữa các lần đọc.

**Các thông tin hiển thị**:

* Băng thông inbound (KB/s, MB/s) và outbound (KB/s, MB/s) của từng giao diện.
* Tổng số byte/packet đã truyền đi và nhận về.

**Ứng dụng trong đồ án**: Cung cấp một cái nhìn tổng quan, trực quan về việc sử dụng băng thông trên các giao diện mạng. Hữu ích để xác nhận xem liệu lưu lượng thử nghiệm từ iperf3 có thực sự được tạo ra hay không, hoặc để giám sát mức độ tải tổng thể của hệ thống.

# II. MÔ HÌNH TRIỂN KHAI

## 2.1. MÔ HÌNH TỔNG QUAN

- 3 máy ảo Ubuntu 22.04 LTS: Client, Bottleneck, Server.

## 2.2. SƠ ĐỒ HỆ THỐNG

A screenshot of a computer

AI-generated content may be incorrect.

2.3. Kịch bản thử nghiệm

Chạy các kịch bản với băng thông bình thường với 1 flow TCP/UDP ở fq\_codel, pfifo, RED