**Mục Lục**

[**THUẬT NGỮ VIẾT TẮT 2**](#_Toc154502094)

[**MỞ ĐẦU 3**](#_Toc154502095)

[**CHƯƠNG 1. TỔNG QUAN VỀ MẠNG IP 4**](#_Toc154502096)

[**1.1. Giới thiệu tổng quan về mạng IP 4**](#_Toc154502097)

[**1.1.1. Lịch sự phát triển 4**](#_Toc154502098)

[**1.1.2. Định nghĩa về mạng IP 5**](#_Toc154502099)

[**1.2. Mô hình phân lớp TCP/IP 6**](#_Toc154502100)

[**1.2.1. Kiến trúc của TCP/IP 6**](#_Toc154502101)

[**1.2.2. Một số giao thức cơ bản trong mô hình TCP/IP 7**](#_Toc154502102)

[**1.2.3. Ưu điểm và nhược điểm của TCP/IP 14**](#_Toc154502103)

[**1.2.4. Địa chỉ IP 15**](#_Toc154502104)

[**1.3. Tổng quan về chất lượng dịch vụ QoS 18**](#_Toc154502105)

[**1.4. Kết luận chương 1 19**](#_Toc154502106)

[**CHƯƠNG 2. QUẢN LÝ CHẤT LƯỢNG DỊCH VỤ QoS TRONG MẠNG IP 21**](#_Toc154502107)

[**2.1. Tham số đánh giá chất lượng dịch vụ trong mạng IP 21**](#_Toc154502108)

[**2.1.1. Băng thông 21**](#_Toc154502109)

[**2.1.2. Thông lượng 23**](#_Toc154502110)

[**2.1.3. Độ trễ 23**](#_Toc154502111)

[**2.1.4. Độ biến thiên trễ 24**](#_Toc154502112)

[**2.1.5. Mất gói 26**](#_Toc154502113)

[**2.1.6. Độ tin cậy 27**](#_Toc154502114)

[**2.1.7. Bảo mật 29**](#_Toc154502115)

[**2.2. Kiến trúc của QoS 30**](#_Toc154502116)

[**2.3. Các yếu tố chung cho kiến trúc QoS 31**](#_Toc154502117)

[**2.3.1. Nguyên tắc QoS 31**](#_Toc154502118)

[**2.3.2. Cơ chế QoS 32**](#_Toc154502119)

[**2.4. Cải thiện chất lượng dịch vụ trong mạng IP 33**](#_Toc154502120)

[**2.4.1. Trường hợp mạng không áp dụng QoS 33**](#_Toc154502121)

[**2.4.2. Các yêu cầu chất lượng dịch vụ trong mạng IP 35**](#_Toc154502122)

[**2.4.3. Phân lớp lưu lượng trong mạng IP 35**](#_Toc154502123)

[**2.5. QoS trong một mô hình mạng 37**](#_Toc154502124)

[**2.6. Kết luận chương 2 38**](#_Toc154502125)

[**CHƯƠNG 3. MỘT SỐ GIẢI PHÁP ĐÁNH GIÁ TRUYỀN DẪN LƯU LƯỢNG TRONG MẠNG IP 40**](#_Toc154502126)

[**3.1. Cải thiện thông số QoS 40**](#_Toc154502127)

[**3.1.1. Kỹ thuật quản lý tắc nghẽn dữ liệu 40**](#_Toc154502128)

[**3.1.2. Tối ưu tốc độ truyền dẫn và tốc độ gói 41**](#_Toc154502129)

[**3.1.3. Bổ sung QoS 42**](#_Toc154502130)

[**3.2. Các cơ chế phân phối lưu lượng ra 43**](#_Toc154502131)

[**3.2.1. Nhập trước xuất trước (FIFO) 45**](#_Toc154502132)

[**3.2.2. Xếp hàng công bằng (FQ) 45**](#_Toc154502133)

[**3.2.3. Xếp hàng công bằng vòng tròn bit (BRFQ) 46**](#_Toc154502134)

[**3.2.4. Xếp hàng công bằng có trọng số (WFQ) 47**](#_Toc154502135)

[**3.2.5. Chất lượng dịch vụ hỗ trợ trong WFQ 48**](#_Toc154502136)

[**3.3. Mô hình đảm bảo chất lượng dịch vụ 48**](#_Toc154502137)

[**3.3.1. Mô hình IntServ (Intergrated Services) 49**](#_Toc154502138)

[**3.3.2. Mô hình và kiến trúc DiffServ (Differentiated Services) 50**](#_Toc154502139)

[**3.3.3. Các phương pháp xử lý gói trong DiffServ 52**](#_Toc154502140)

[**3.4. Giải pháp tối ưu lưu lượng trong mạng 53**](#_Toc154502141)

[**3.4.1. Bắt giữ và đánh dấu gói tin 53**](#_Toc154502142)

[**3.4.2. Hoạt động của chức năng bắt giữ và đánh dấu 53**](#_Toc154502143)

[**3.4.3. Giảm chiếm giữ hàng đợi 55**](#_Toc154502144)

[**3.5. Khả năng liên kết và bảo mật truyền dẫn trong mạng 57**](#_Toc154502145)

[**3.6. Kết luận chương 3 59**](#_Toc154502146)

[**CHƯƠNG 4. XÂY DỰNG BÀI TOÁN MÔ PHỎNG QOS TRÊN MẠNG IP 60**](#_Toc154502147)

[**4.1. Xây dựng kịch bản mô phỏng 60**](#_Toc154502148)

[**4.2. Thực hiện mô phỏng cho mô hình mạng 61**](#_Toc154502149)

[**4.2.1. Xây dựng mô phỏng 61**](#_Toc154502150)

[**4.2.2. Đánh giá kết quả thu được khi thực hiện mô phỏng 62**](#_Toc154502151)

[**4.3. Tổng quát đánh giá chất lượng truyền dẫn trong mạng 67**](#_Toc154502152)

[**4.4. Kết luận chương 4 72**](#_Toc154502153)

[**KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 73**](#_Toc154502154)

[**TÀI LIỆU THAM KHẢO 75**](#_Toc154502155)

# THUẬT NGỮ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **Từ viết tắt** | **Tiếng Anh** | **Tiếng Việt** |
| ARP | Address Resolution Protocol | Giao thức phân giải địa chỉ |
| RARP | Reverse ARP | Giao thức phân giải địa chỉ ngược |
| RSVP | Resource Reservation Protocol | Giao thức dành sẵn tài nguyên |
| BA | Behavior Aggregate | Tập hợp hành vi |
| TCP/IP | Transmission Control Protocol/Internet Protocol | giao thức điều khiển truyền nhận/ Giao thức liên mạng |
| SMTP | Simple Mail Transfer Protocol | Giao thức truyền thư điện tử |
| FTP | File Transfer Protocol | Giao thức truyền tải tệp tin |
| DNS | Domain Name System | Hệ thống phân giải tên miền |
| UDP | User Datagram Protocol | Giao thức dữ liệt người dùng |
| QoS | Quality of Service | Chất lượng dịch vụ |
| FIFO | First In First Out | Nhập trước xuất trước |
| CQ | Custom Queuing | Kỹ thuật xếp hàng tùy chỉnh |
| PQ | Priority Queuing | Xếp hàng ưu tiên |
| WFQ | Weighted Fair Queuing | Xếp hàng công bằng có trọng số |
| ECN | Explicit Congestion Notification | Thông báo tắc nghẽn rõ ràng |
| ECT | ECN Capable Transport | Truyền tải theo ECN |
| RTP | Real Time Protocol | Giao thức truyền tải thời gian thực |
| IPTV | Internet Protocol Television | Truyền hình giao thức Internet |
| ToS | Terms Of Service | Điều khoản Dịch vụ |
| VoIP | Voice over IP | Thoại trên nền IP |
| AF | Assured Forwarding | Chuyển tiếp đảm bảo |
| WRR | Weighted Round Robin | Quay vòng theo trọng số |
| WF | Wildcard Filter | Bộ lọc đại diện |

# MỞ ĐẦU

Chất lượng truyền dẫn mạng máy tính, đặc biệt là hệ thống truyền thông nói chung, luôn là một chủ đề vô cùng quan trọng và luôn thu hút sự quan tâm của cộng đồng chuyên gia trong lĩnh vực mạng. Sự bùng nổ nhanh chóng của Internet đã mở ra một loạt các thách thức liên quan đến chất lượng dịch vụ, đòi hỏi chúng ta phải tìm hiểu và đánh giá kỹ lưỡng. Phân tích và đánh giá hiệu năng mạng đã trở thành một công cụ quan trọng giúp chúng ta tiến gần hơn đến việc ứng dụng thực tế, cùng việc tối ưu hóa hiệu suất của các hệ thống mạng và truyền thông hiện đại.

Để thực hiện đánh giá chất lượng truyền dẫn trong mạng, cần phải xem xét và đánh giá một loạt các yếu tố quan trọng và nhận biết sự ảnh hưởng của chúng đối với hoạt động của hệ thống mạng. Sự hiệu quả của truyền dẫn mạng chịu ảnh hưởng từ nhiều yếu tố, bao gồm độ trễ, thông lượng, lưu lượng truy cập nhận được, số gói tin va chạm, và nhiều khía cạnh khác. Đồ án *“Tìm hiểu mô phỏng đánh giá hiệu năng truyền tải dữ liệu trong mạng IP”* góp một phần nhỏ để đánh giá được QoS nói trên. Đồ án gồm có 4 chương chính là:

Chương 1: Tổng quan về mạng IP

Chương 2: Quản lý chất lượng dịch vụ QoS trong mạng IP

Chương 3: Một số giải pháp đánh giá truyền dẫn lưu lượng trong mạng IP

Chương 4: Xây dựng bài toán mô phỏng và đánh giá

Kết luận và hướng phát triển đề tài

Dự kiến kết quả đạt được của đề tài là sẽ đánh giá được các yếu tố như độ trễ, thông lượng, lưu lượng gửi đi, lưu lượng truy cập, … từ đó có thể đưa ra những giải pháp tối ưu hóa chất lượng truyền dẫn lưu lượng trong mạng.

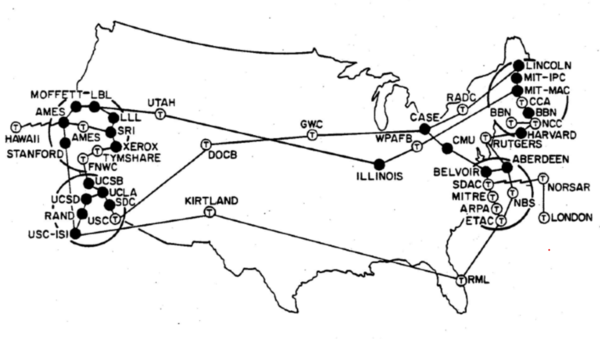
# CHƯƠNG 1. TỔNG QUAN VỀ MẠNG IP

## **1.1. Giới thiệu tổng quan về mạng IP**

### **1.1.1. Lịch sự phát triển**

Tiền thân của mạng Internet là mạng ARPANET của Bộ quốc phòng Mỹ. Mạng ARPANET ra đời với mục đích là kết nối các trung tâm nghiên cứu của một số Viện nghiên cứu và trường đại học nhằm chia sẻ, trao đổi tài nguyên thông tin. Số lượng các nút trên ARPANET đã tăng lên đáng kể trong vài năm sau đó, điều này dẫn đến nhiều vấn đề khác nhau mà phần lớn được coi là vấn đề của các hạn chế kỹ thuật.

Vào tháng 7 năm 1980, Văn phòng Bộ trưởng Quốc phòng Hoa Kỳ chỉ đạo rằng một bộ các giao thức chuẩn DoD được sử dụng trên tất cả các mạng quốc phòng. Các giao thức có các chỉ định chính thức sau: RFC 791 - Giao thức Internet và RFC 793 - Giao thức điều khiển truyền dẫn. Đây là những con số và mô tả RFC mới nhất, tổ chức có thẩm quyền trong ngày là Ban kiểm soát cấu hình Internet (ICCB), người đã chỉ định các bản phát hành ban đầu là RFC 760, Giao thức Internet tiêu chuẩn DoD và RFC 761, Giao thức điều khiển truyền dẫn tiêu chuẩn DoD.



Hình .. Sơ đồ mắc nối của mạng lưới ARPANET tháng 3 năm 1977Hình .

Vào giữa đến cuối những năm 1970, ITU và ISO đã làm việc độc lập để phát triển một bộ tiêu chuẩn mở cho kiến ​​trúc mạng. Điều này đưa ra những thách thức đáng kể mà DARPA không gặp phải, so sánh, hoạt động trong một môi trường được kiểm soát. Các kiến ​​trúc sư của ISO và ITU đã phải đối mặt với nhiệm vụ khó khăn là thuyết phục các nhà sản xuất thiết bị đồng ý với mỗi và mọi tiêu chuẩn.

ISO và ITU đã thiết lập mối quan hệ tích cực với nhà cung cấp với Hệ thống thông tin Honeywell, công ty đã làm việc với các nhóm quốc tế. Năm 1984, nhóm ITU và ISO đã hợp nhất các công việc tiêu chuẩn tương ứng của họ thành một tài liệu duy nhất và phần lớn sản phẩm cuối cùng đến từ các kỹ sư của Honeywell. Tài liệu tiêu chuẩn được phát hành dưới tên gọi là Open Systems Interconnection, hiện được gọi là Mô hình Tham chiếu OSI (hoặc đơn giản là Mô hình OSI).

Quá trình chuyển đổi ARPANET sang TCP/IP xảy ra từ tháng 10 năm 1981 đến tháng 10 năm 1983. Trong thời gian này, các giao thức được các nhà phát triển của họ nghiên cứu và xem xét kỹ lưỡng. Bản phát hành chính thức vào ngày 1 tháng 1 năm 1983 và Internet ra đời. Khởi đầu có được trong thời kỳ phát triển và ngày phát hành năm 1983 được cho là lý do TCP/IP hiện là tiêu chuẩn toàn cầu cho truyền thông Internet. Bây giờ bạn đã có kiến ​​thức tổng quát về lịch sử của Internet, đã đến lúc khám phá Mô hình OSI và TCP/IP.

### **1.1.2. Định nghĩa về mạng IP**

Trước đây, người ta định nghĩa “Internet là mạng của tất cả các mạng sử dụng giao thức IP”. Nhưng hiện nay điều đó không còn chính xác nữa vì nhiều mạng có kiến trúc khác nhau nhưng nhờ các cầu nối giao thức nên vẫn có thể kết nối vào Internet và vẫn có thể sử dụng đầy đủ các dịch vụ Internet. Internet không chỉ là một tập hợp các mạng được liên kết với nhau, Internet working còn có nghĩa là các mạng được liên kết với nhau trên cơ sở cùng đồng ý với nhau về các quy ước mà cho phép các máy tính liên lạc với nhau, cho dù con đường liên lạc sẽ đi qua những mạng mà chúng không được đấu nối trực tiếp tới. Như vậy, kỹ thuật Internet che dấu chi tiết phần cứng của mạng, và cho phép các hệ thống máy tính trao đổi thông tin độc lập với những liên kết mạng vật lý của chúng.

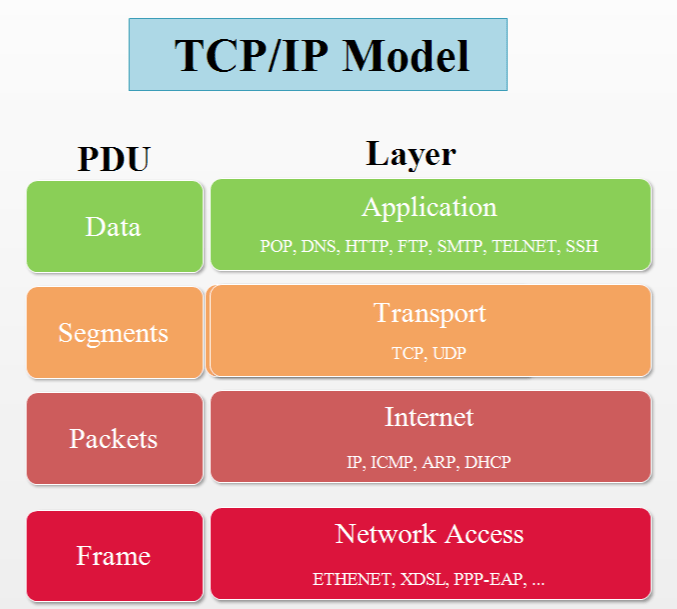
Internet Protocol (IP) là một [giao thức](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/), hoặc một tập hợp các quy tắc, để định tuyến và định địa chỉ các [gói](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) dữ liệu để chúng có thể di chuyển qua các mạng và đến đúng đích. Dữ liệu truyền qua Internet được chia thành các phần nhỏ hơn, được gọi là các gói. Thông tin IP được đính kèm trong mỗi gói và thông tin này giúp [các bộ định tuyến](https://www.cloudflare.com/learning/network-layer/what-is-a-router/) gửi gói đến đúng nơi. Mọi thiết bị hoặc [miền](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/) kết nối với Internet đều được gán một [địa chỉ IP](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) và khi các gói được chuyển hướng đến địa chỉ IP gắn liền với chúng, dữ liệu sẽ đến nơi cần thiết.

Khi các gói đến đích, chúng được xử lý khác nhau tùy thuộc vào giao thức truyền tải nào được sử dụng kết hợp với IP. Các giao thức truyền tải phổ biến nhất là TCP và UDP.

## **1.2. Mô hình phân lớp TCP/IP**

### **1.2.1. Kiến trúc của TCP/IP**

TCP/IP (Transmission Control Protocol/Internet Protocol) hay còn gọi là giao thức điều khiển truyền nhận/ Giao thức liên mạng. Đây là một bộ các giao thức truyền thông được sử dụng để kết nối các thiết bị mạng với nhau trên internet. TCP/IP cũng có thể được sử dụng như một giao thức truyền thông trong mạng máy tính riêng (mạng nội bộ).



Hình 1.2. Mô hình kiến trúc TCP/IP

*Network Access Layer:* Cung cấp các giao tiếp với mạng vật lý bao gồm các thiết bị hệ thống vận hành, các card giao diện mạng tương ứng. Lớp này thực hiện nhiệm vụ các chi tiết phần cứng hoặc các giao tiếp vật lý với cáp. Ngoài ra thực hiện việc kiểm soát lỗi dữ liệu phân bổ trên mạng vật lý. Lớp này không định nghĩa một giao thức riêng nào, nó hỗ trợ tất cả các giao thức chuẩn và độc quyền ví dụ như Ethenet, Token Ring, Wireless, IP…. Lớp này thực tế cũng quyết định khá nhiều tới chất lượng cung cấp dịch vụ của mạng, tuy nhiên việc cải tiến trên là khó khăn, do vậy người ta thường cải thiện theo hướng nâng cấp phần mềm.

*Internet Layer:* Lớp Internet chức năng cung cấp việc đánh địa chỉ một cách độc lập với phần cứng, cho phép dữ liệu được truyền qua các mạng vật lý có cấu trúc khác nhau. Nhiệm vụ quan trọng của lớp này là đảm bảo việc chuyển gói tin thông qua mạng và hỗ trợ các giao thức giao tiếp mạng, đặc biệt là giao thức IP. Hơn nữa, nó cũng chịu trách nhiệm về việc định tuyến các gói tin trong mạng, đảm bảo rằng chúng đi đúng đích trong mạng toàn cầu.

*Transport Layer:* Chịu trách nhiệm truyền thông điệp từ một tiến trình tới một tiến trình khác. Nó có hai giao thức rất khác nhau là: giao thức điều khiển truyền dẫn TCP và giao thức người sử dụng UDP (User Datagram Protocol).

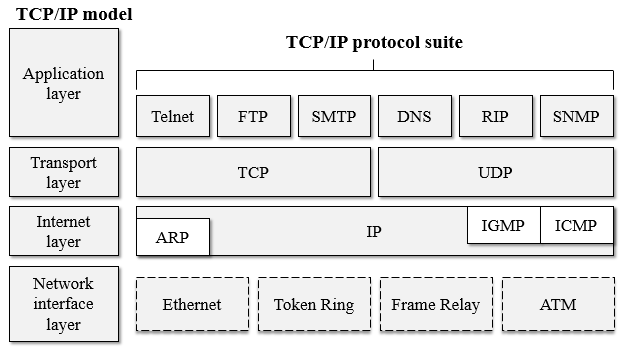
*Application Layer:* Điều khiển từng ứng dụng cụ thể, nó cũng bao gồm các giao thức mức cao, mã hóa điều khiển hội thoại… hiện nay có hàng trăm thậm chí đến hàng nghìn giao thức thuộc lớp này.

Dữ liệu gửi từ tầng ứng dụng đi xuống và khi qua mỗi tầng nó được định nghĩa riêng về dữ liệu mà nó sử dụng.

### **1.2.2. Một số giao thức cơ bản trong mô hình TCP/IP**

Trong hai giao thức chính của bộ Giao thức internet, mỗi giao thức đảm nhiệm các chức năng cụ thể. TCP xác định cách các ứng dụng có thể tạo ra các kênh truyền dẫn thông qua mạng. Đồng thời, TCP quản lý cách một tin nhắn được chia thành các packet nhỏ hơn trước khi truyền qua internet. Sau đó là cách chúng tập hợp lại theo đúng thứ tự ở nơi nhận.

Đối với IP, giao thức IP đảm bảo các gói được đi đến đúng địa chỉ đích. Mỗi gateway trên mạng sẽ kiểm tra địa chỉ IP này để xác định nơi chuyển tiếp.



Hình 1.3. Mô hình phân lớp bộ giao thức TCP/IP

*Tầng ứng dụng - Applycation Layer:*

SMTP (Simple Mail Transfer Protocol): Giao thức truyền thư điện tử giữa các máy tính. Đây là dạng đặc biệt của truyền tệp được sử dụng để gửi các thông báo tới một máy chủ qua thư hoặc giữa các máy với nhau. Nó được sử dụng rất phổ biến trên Internet, dùng để gửi các message “email” dựa trên địa chỉ của email.

FTP (File Transfer Protocol): Đây là một dịch vụ hướng kết nối và tin cậy, sử dụng TCP để cung cấp truyền tệp giữa các hệ thống hỗ trợ FTP.

Telnet: Cho phép các phiên đăng nhập từ xa giữa các máy tính. Do telnet hỗ trợ chế độ văn bản nên giao diện người dùng thường ở dạng dấu nhắc lệnh tương tác.

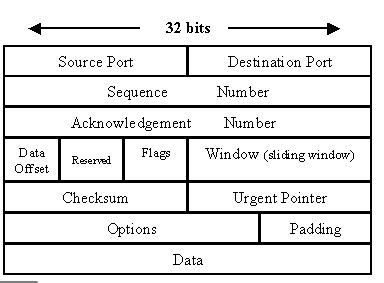
DNS (Domain Name System): Chuyển đổi tên miền thành địa chỉ IP. Giao thức này thường được các ứng dụng sử dụng khi người dùng ứng dụng này dùng tên chứ không dùng địa chỉ IP.

SNMP (Simple Network Monitoring Protocol): Giao thức quản trị mạng cung cấp những công cụ quản trị mạng từ xa. Nó cho phép quản trị viên mạng theo dõi và điều khiển các thiết bị mạng.

RIP (Routing Internet Protocol): Giao thức định tuyến.

*Tầng vận chuyển - Transport Layer:*

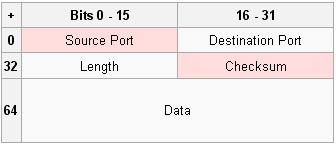
TCP (Transmission Control Protocol): Là một trong các giao thức cốt lõi của bộ giao thức TCP/IP. TCP hoạt động theo hướng kết nối Connection-Oriented, trước khi truyền dữ liệu giữa 2 máy, nó thiết lập một kết nối giữa 2 máy theo phương thức bằng cách gửi gói tin ACK từ máy đích sang máy nhận, trong suốt quá trình truyền gói tin, máy gửi yêu cầu máy đích xác nhận đã nhận đủ các gói tin đã gửi, nếu có gói tin bị mất, máy đích sẽ yêu cầu máy gửi gửi lại, thường xuyên kiểm tra gói tin có bị lỗi hay ko, ngoài ra còn cho phép quy định số lượng gói tin được gửi trong một lần gửi, điều này đảm bảo máy nhận nhận được đầy đủ các gói tin mà máy gửi gửi đi.



Hình 1.4. Cấu trúc gói tin TCP

UDP (User Datagram Protocol): Khác với TCP, UDP không cung cấp sự tin cậy và thứ tự truyền nhận, các gói dữ liệu có thể đến không đúng thứ tự hay bị mất mà không có thông báo. Tuy nhiên UDP nhanh và hiệu quả hơn đối với các ứng dụng truyền những file kích thước nhỏ và yêu cầu khắt khe về thời gian. Do bản chất không trạng thái nên UDP hữu dụng trong việc trả lời các truy vấn nhỏ cho số lượng lớn người yêu cầu. Được hỗ trợ bởi nhiều dịch vụ phổ biến như DNS, VoiIP, FTP.

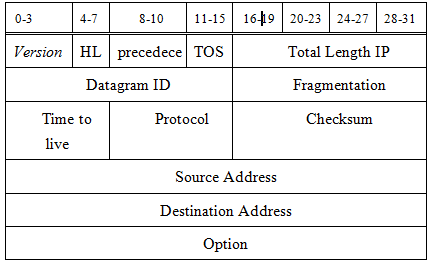
UDP không thực hiện quá trình bắt tay khi gửi và nhận thông tin, do đó được gọi là Connectionless. UDP không đảm bảo cho các tầng phía trên rằng thông điệp đã được gửi và người gửi cũng không có trạng thái thông điệp UDP một khi gói tin đã được gửi.



Hình 1.5. Cấu trúc gói tin UDP

*Internet Layer (Tầng Liên Mạng):*

Giao Thức IP (Internet Protocol): IP là một giao thức phi kết nối và không tin cậy, nó cung cấp dịch vụ chuyển gói nỗ lực nhất nghĩa là IP không cung cấp chức năng theo dõi và kiểm tra lỗi, nó chỉ cố gắng chuyển gói tới đích chứ không có sự đảm bảo. Nếu độ tin cậy là yếu tố quan trọng, IP phải hoạt động với giao thức tầng trên tin cậy chẳng hạn TCP.



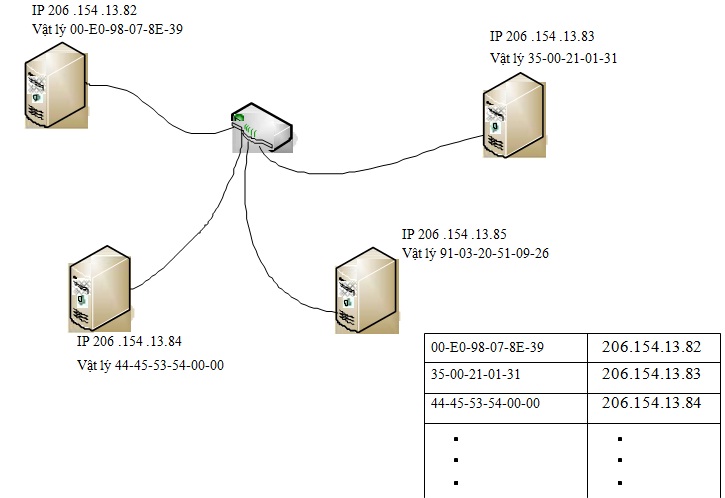
Hình 1.6. Tiêu đề IP datagram

Các gói dữ liệu tại tầng IP được gọi là datagram. Một datagram có chiều dài biến thiên, gồm hai phần: tiêu đề và dữ liệu. Phần tiêu đề có chiều dài từ 20 đến 60 byte, chứa các thông tin cần thiết cho định tuyến và chuyển phát dữ liệu.

* Phiên bản Version: Trường 4 bít này cho biết phiên bản IP tạo phần tiêu đề này. Phiên bản hiện tại là 4. Tuy nhiên phiên bản IPv6 sẽ thay thế IPv4 trong tương lai.
* Chiều dài tiêu đề HL: Trường 4 bit này cho biết chiều dài của phần tiêu đề IP Datagram, tính theo đơn vị từ (32 bit). Trường này là cần thiết vì chiều dài của phần tiêu đề thay đổi từ 20 đến 60 byte. Khi không có phần tuỳ chọn Option, chiều dài phần tiêu đề là 20 byte và giá trị của trường này là 5. Khi phần tuỳ chọn có kích thước tối đa thì giá trị của trường là 15.
* Độ ưu tiên Precedence: Trường này có chiều dài 3 byte, giá trị nằm trong khoảng từ 0 đến 7. Nó chỉ rõ độ ưu tiên của datagram trong trường hợp mạng có tắc nghẽn.
* Loại dịch vụ TOS: Trường 5 bit này đặc tả các tham số về dịch vụ.
* Độ dài tổng Total Length IP: Trường 16 bit này cho biết chiều dài tính theo byte của cả datagram.
* Số hiệu Datagram (Datagram ID): Trường 16 bit này cùng với các trường khác khác dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn tồn tại trên liên mạng. Giá trị này được tăng lên 1 đơn vị mỗi khi có datagram được trạm gửi đi. Do vậy giá trị này sẽ quay lại 0 mỗi khi trạm đã gửi 65535 datagram.
* Phân mảnh Fragmentation: Trường 16 bít này được sử dụng khi datagram được phân mảnh.
* Thời gian sống Time to Live: Trường 8 bit này quy định thời gian tồn tại của datagram trong liên mạng để tránh tình trạng datagram bị chuyển vòng quanh trên liên mạng. Thời gian này do trạm gửi đặt và bị giảm đi 1 mỗi khi datagram qua một router trên liên mạng.
* Giao thức Protocol: Trường 8 bit này cho biết giao thức tầng trên sử dụng dịch vụ của tầng IP. IP datagram có thể đóng gói dữ liệu từ nhiều giao thức tầng trên, chẳng hạn TCP, UDP và ICMP. Trường này chỉ rõ giao thức đích cuối cùng mà IP datagram phải chuyển.
* Tổng kiểm tra Checksum: Trường 16 bit này chứa mã kiểm tra lỗi theo phương pháp chỉ kiểm tra phần tiêu đề CRC.
* Địa chỉ nguồn Source Address: Trường 32 bit này chứa địa chỉ IP của trạm nguồn.
* Địa chỉ đích Destination Address: Trường 32 bit này chứa địa chỉ IP của trạm đích.
* Các tuỳ chọn IP Options: Trường này hỗ trợ một số thiết lập tiêu đề tuỳ ý sử dụng cho việc kiểm tra, gỡ rối và an toàn.

Giao thức phân giải địa chỉ (ARP): Các máy tính trên một mạng cục bộ sử dụng giao thức lớp Internet được gọi là giao thức phân giải địa chỉ để ánh xạ các địa chỉ IP vào các địa chỉ vật lý. Một host phải biết địa chỉ vật lý của bộ tương thích mạng đích để gửi bất kỳ dữ liệu nào đến nó. Vì lý do này, ARP là một giao thức rất quan trọng. Tuy nhiên, các mạng IP thực hiện theo cách thức sao cho ARP và tất cả các chi tiết của việc chuyển đổi địa chỉ hầu như vô hình đối với người sử dụng. Bộ tương thích mạng được xác định bởi địa chỉ IP của nó. Địa chỉ IP phải được ánh xạ đến một địa chỉ vật lý để một thông điệp đến đích của nó.

Mỗi host trên một đoạn mạng duy trì một bảng trong bộ nhớ được gọi là Bảng ARP hay bộ nhớ nhanh ARP Cache. ARP liên kết các địa chỉ IP của các host khác trên đoạn mạng với các địa chỉ vật lý. Khi một host cần gửi dữ liệu đến một host khác trên đoạn, host kiểm tra bảng ARP để xác định địa chỉ vật lý của nơi nhận. Bảng ARP được hình thành một cách tự động. Nếu địa chỉ nhận dữ liệu hiện không được liệt kê trong bảng ARP, host gửi một broadcast được gọi là một khung yêu cầu ARP.



Hình 1.7. ARP ánh xạ các địa chỉ IP vào các địa chỉ vật lý

Khung yêu cầu ARP chưa được phân giải. Khung yêu cầu ARP cũng chứa địa chỉ IP và địa chỉ vật lý của host gửi yêu cầu. Các host khác trên đoạn mạng nhận yêu cầu ARP, và host có địa chỉ IP chưa phân giải hồi đáp bằng cách gửi địa chỉ vật lý của nó đến host gửi yêu cầu. Ánh xạ địa chỉ IP và địa chỉ vật lý được thêm vào bảng ARP của host yêu cầu.

Thông thường, các mục trong bảng ARP sẽ hết hạn sau một khoảng thời gian định trước. Khi thời gian sống của một mục ARP kết thúc, mục đó sẽ bị loại bỏ khỏi bảng. Tiến trình phân giải bắt đầu lại ở thời điểm kế khi mà host cần gửi dữ liệu đến địa chỉ IP của mục đã bị loại bỏ.

Giao thức phân giải địa chỉ ngược RARP: RARP trái ngược với ARP, ARP được sử dụng khi biết địa chỉ IP nhưng không biết địa chỉ vật lý. RARP thì được sử dụng khi biết địa chỉ vật lý nhưng không biết địa chỉ IP. Khi máy được bật, yêu cầu RARP được tạo ra và được gửi quảng bá trên mạng cục bộ. Một máy khác trên mạng biết về mọi địa chỉ IP sẽ trả lời yêu cầu bằng bản tin trả lời RARP. Máy yêu cầu RARP phải chạy chương trình RARP khách và máy trả lời RARP phải chạy chương trình RARP chủ.

*Tầng truy nhập mạng - Network Access Layer:*

Một số giao thức tiêu biểu thuộc tầng này gồm: ATM, Ethernet, Token Ring, Frame Relay.

Giao thức ATM (Asynchronous Transfer Mode) không thuộc lớp Network Access của mô hình TCP/IP. ATM là một công nghệ truyền dẫn dữ liệu độc lập với mô hình TCP/IP và thường được sử dụng trong mạng viễn thông và mạng WAN (Wide Area Network). Lớp Network Access trong mô hình TCP/IP thường liên quan đến giao thức Ethernet, PPP (Point-to-Point Protocol), và các công nghệ mạng khác để kết nối thiết bị vào mạng.

Giao thức Ethernet thuộc lớp Network Access của mô hình TCP/IP. Nó là một công nghệ mạng phổ biến được sử dụng để kết nối thiết bị trong mạng LAN (Local Area Network). Ethernet định các quy tắc về cách truyền dữ liệu trên các mạng có dây và không dây, bao gồm cách định địa chỉ MAC (Media Access Control) cho các thiết bị và quy định cách gói dữ liệu được đóng gói và truyền trong mạng.

Giao thức Token Ring thuộc lớp Network Access của mô hình TCP/IP. Nó là một công nghệ mạng đã lỗi thời, sử dụng mô hình truyền dữ liệu theo vòng (ring) và sử dụng mã hóa token để quản lý quyền truy cập vào mạng. Token Ring đã được thay thế bởi Ethernet trong hầu hết các mạng LAN hiện đại.

Giao thức Frame Relay không thuộc lớp Network Access của mô hình TCP/IP. Nó là một giao thức liên quan đến lớp liên kết dữ liệu (Data Link Layer) của mô hình OSI và thường được sử dụng trong mạng WAN (Wide Area Network) để kết nối các trạm trong mạng. Giao thức Frame Relay không liên quan trực tiếp đến mô hình TCP/IP và không được sử dụng trong môi trường mạng LAN (Local Area Network) cơ bản.

### **1.2.3. Ưu điểm và nhược điểm của TCP/IP**

* Ưu điểm:

Như đã đề cập ở trên, TCP/IP là một mô hình có tính thực tế cao. Những đặc điểm nổi bật của nó có thể được kể đến như:

* Thiết lập kết nối giữa các loại máy tính khác nhau.
* Hoạt động độc lập với hệ điều hành.
* Hỗ trợ nhiều giao thức định tuyến.
* Kiến trúc client – server, khả năng mở rộng cao.
* Có thể hoạt động độc lập.
* Nhẹ, không gây nhiều áp lực với máy tính hay mạng.
* Nhược điểm

Dẫu vậy không có mô hình nào hoàn hảo. TCP/IP cũng có một số điểm hạn chế cần được khắc phục:

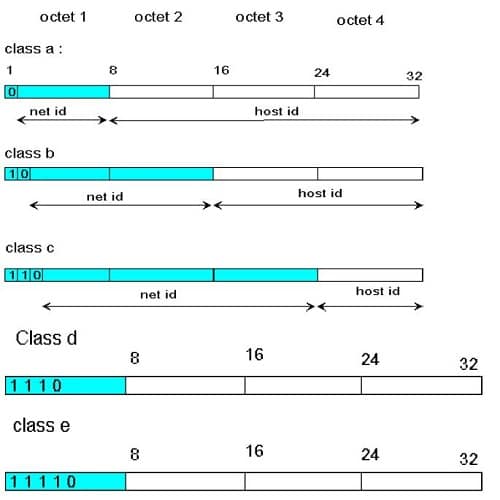
* Việc cài đặt khá phức tạp, khó để quản lý.
* Tầng transport không đảm bảo việc phân phối các gói tin.
* Các giao thức trong TCP/IP không dễ để có thể thay thế.
* Không tách biệt rõ ràng các khái niệm về dịch vụ, giao diện và giao thức. Do đó nó không hiệu quả để mô tả các công nghệ mới trong mạng mới.
* Dễ bị tấn công SYN – một kiểu tấn công từ chối dịch vụ.

### **1.2.4. Địa chỉ IP**

* Địa chỉ IPv4

Một địa chỉ IPv4 là một địa chỉ nhị phân 32 bit. Địa chỉ 32 bit này được phân chia thành 4 đoạn 8 bit được gọi là các octet. Con người không thoải mái khi làm việc với các địa chỉ nhị phân 32bit hay ngay cả các octet nhị phân 8 bit, vì thế địa chỉ IPv4 hầu như luôn luôn được biểu diễn dưới dạng chấm thập phân. Dưới dạng chấm thập phân, mỗi octet được gán một số thập phân tương ứng sau đó được phân biệt bằng các dấu chấm. Một địa chỉ IPv4 chấm thập phân có dạng: 209.121.131.14. Một phần của địa chỉ IPv4 được sử dụng cho định danh mạng, và một phần của địa chỉ được sử dụng cho định danh host. Sự phức tạp của địa chỉ IPv4 là phần định danh mạng biến đổi. Mỗi địa chỉ IP được chia làm 2 phần:

* Phần địa chỉ mạng Net ID: Dùng để nhận dạng những hệ thống trong cùng 1 khu vực vật lý còn được gọi là Segment. Mọi hệ thống trong cùng 1 Segment phải có cùng địa chỉ mạng và phần địa chỉ này phải là duy nhất trong số các mạng hiện có.
* Phần địa chỉ trạm Host ID: Dùng để nhận dạng một trạm làm việc, một máy chủ, nột router hoặc một trạm TCP/IP trong một phân đoạn. Phần địa chỉ trạm cũng phải là duy nhất trong một mạng. Sự kết hợp giữa Net ID và Host ID phải cho phép nhận dạng duy nhất mỗi máy tính riêng biệt.



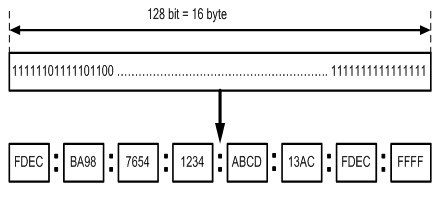
Hình 1.8. Cấu trúc các lớp địa chỉ IP

Địa chỉ IPv4 chia ra 5 lớp A, B, C, D, E. Hiện tại đã dùng hết lớp A, B và gần hết lớp C, còn lớp D và E tổ chức internet đang để dành cho mục đích khác không phân.

Bit nhận dạng là những bit đầu tiên: của lớp A là 0, của lớp B là 10, của lớp C là 110, của lớp D là 1110 còn của lớp E là 11110.

* Địa chỉ IPv6

Địa chỉ IPv6 dài 128 bít và được biểu diễn dưới dạng hexa hai chấm. Trong cách biểu diễn này, 128 bít được chia thành 8 phần, mỗi phần dài 2 byte. Hai byte được biểu diễn bằng 4 số hexa. Do đó, địa chỉ IP gồm 32 số hexa, cứ 4 số hexa có một dấu hai chấm để phân tách.

**

Hình 1.9. Định dạng gói IPv6

IPv6 gồm các loại chính sau đây:

Unicast Address: Dùng để xác định một Interface trong phạm vi các Unicast Address. Gói tin (Packet) có đích đến là Unicast Address sẽ thông qua Routing để chuyển đến 1 Interface duy nhất.

Anycast Address: Là địa chỉ đặc biệt có thể gán cho nhiều interface, gói tin chuyển đến Anycast Address sẽ được vận chuyển bởi hệ thống Routing đến Interface gần nhất. Hiện nay, địa chỉ Anycast được sử dụng rất hạn chế, rất ít tài liệu nói về cách sử dụng loại địa chỉ này. Hầu như Anycast addresss chỉ được dùng để đặt cho Router, không đặt cho Host, bởi vì hiện nay địa chỉ này chỉ được sử dụng vào mục đích cân bằng tải.

Multicast Address: Trong địa chỉ IPv6 không còn tồn tại khái niệm địa chỉ Broadcast. Mọi chức năng của địa chỉ Broadcast trong IPv4 được đảm nhiệm thay thế bởi địa chỉ IPv6 Multicast. Địa chỉ Multicast giống địa chỉ Broadcast ở chỗ điểm đích của gói tin là một nhóm các máy trong một mạng, song không phải tất cả các máy. Trong khi Broadcast gửi trực tiếp tới mọi host trong một subnet thì Multicast chỉ gửi trực tiếp cho một nhóm xác định các host, các host này lại có thể thuộc các subnet khác nhau. Host có thể lựa chọn có tham gia vào một nhóm Multicast cụ thể nào đó hay không (thường được thực hiện với thủ tục quản lý nhóm internet - Internet Group Management Protocol), trong khi đó với Broadcast, mọi host là thành viên của nhóm Broadcast bất kể nó có muốn hay không.

## **1.3. Tổng quan về chất lượng dịch vụ QoS**

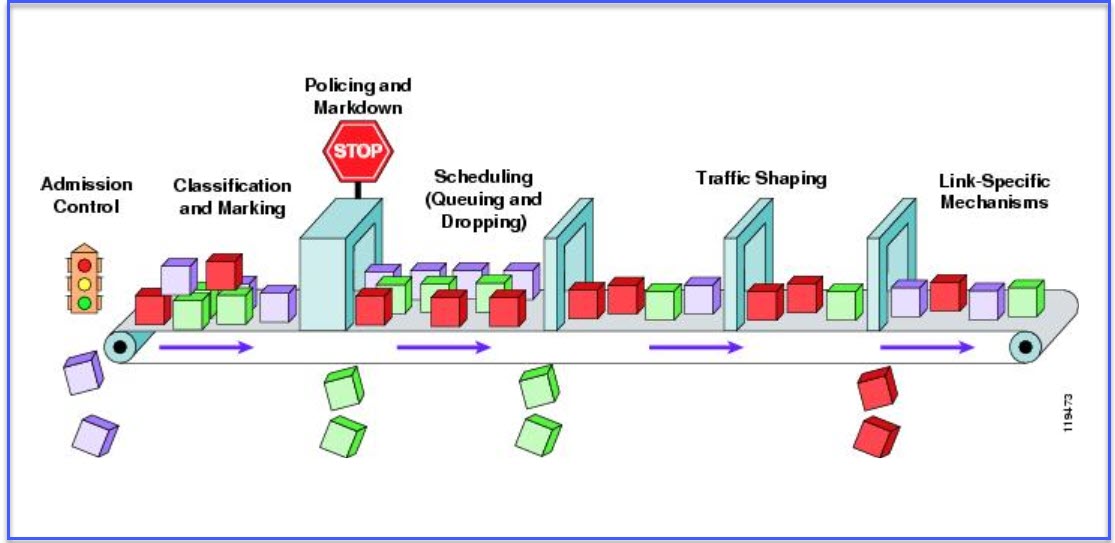
Chất lượng dịch vụ (QoS) là một khái niệm phức tạp và có thể được tiếp cận từ nhiều góc độ khác nhau. Từ góc độ của người sử dụng dịch vụ mạng, QoS đại diện cho mức độ hài lòng về chất lượng dịch vụ mà họ nhận được từ nhà cung cấp dịch vụ mạng đối với các dịch vụ cụ thể mà họ sử dụng hoặc các ứng dụng mà nhà cung cấp dịch vụ cam kết đối với khách hàng.

Các dịch vụ khách hàng này có thể bao gồm nhưng không giới hạn trong việc cung cấp voice, video và dữ liệu. QoS trong ngữ cảnh này phản ánh sự đáp ứng của mạng và dịch vụ đối với các yêu cầu và mong muốn của người dùng, đảm bảo rằng chất lượng trải nghiệm của họ là tối ưu và đáp ứng được đúng các tiêu chuẩn đã cam kết.

Từ góc độ của nhà cung cấp dịch vụ mạng, QoS liên quan đến khả năng cung cấp và đảm bảo các yêu cầu về chất lượng dịch vụ đối với người sử dụng. Để thực hiện điều này, cần tồn tại hai khía cạnh quan trọng về khả năng của mạng trong việc cung cấp chất lượng dịch vụ trong mạng chuyển mạch gói.

Chất lượng dịch vụ (QoS) là một phần quan trọng của mô hình dịch vụ đảm bảo trong mạng Internet. Nó đại diện cho việc cung cấp dịch vụ một cách minh bạch, đảm bảo rằng các yêu cầu ứng dụng của khách hàng được đáp ứng một cách đáng tin cậy và có thể quan sát từ người dùng cuối. Dịch vụ QoS có thể được cung cấp bởi một loạt các ứng dụng hoặc máy chủ lưu trữ, hoặc thậm chí bởi các thành phần bộ định tuyến trong hệ thống của nhà cung cấp dịch vụ. Tất cả các tầng mạng trong mô hình hợp tác từ tầng cao đến tầng thấp để đảm bảo rằng các yêu cầu dịch vụ được thực hiện tốt nhất, theo những cam kết đã được thỏa thuận trong các thỏa thuận về mức độ dịch vụ. Ngoài ra, chất lượng dịch vụ cũng có thể được hiểu như sự khác biệt giữa các gói dữ liệu có mục đích xử lý đặc biệt so với các gói khác trong mạng Internet, để đảm bảo rằng những yêu cầu đặc biệt này được đối xử một cách ưu tiên và đạt được chất lượng dịch vụ tối ưu.

Sự xuất hiện của chuyển mạch gói qua kênh đã đại diện cho một tiến bộ quan trọng trong việc truyền tải dữ liệu văn bản, bao gồm tệp tin văn bản và email. Mô hình truyền dẫn của Internet, dựa trên dịch vụ nỗ lực cao nhất cho việc phân phối các gói tin, đã được xem xét là một phương pháp tiên tiến so với chuyển mạch kênh truyền thống. Tuy nhiên, theo thời gian, với sự phát triển mạnh mẽ của dịch vụ thoại và video qua giao thức Internet, mô hình dịch vụ nỗ lực tốt nhất trở nên không còn đáng tin cậy và không đáp ứng đầy đủ nhu cầu của người dùng cuối. Nhằm đáp ứng những yêu cầu ngày càng đa dạng của người dùng, đã có nhiều mô hình dịch vụ giao hàng được đề xuất. Chúng cung cấp dịch vụ theo yêu cầu của người dùng cuối và có mục tiêu cải thiện chất lượng cung cấp dịch vụ, đảm bảo rằng mọi yêu cầu đều được thỏa mãn một cách hiệu quả và đáng tin cậy.



Hình 1.10. Quản lý chất lượng dịch vụ mạng QoS

Chất lượng mạng dịch vụ liên quan đến khả năng của một mạng cung cấp dịch vụ tốt hơn so với các mạng cơ bản khác. Nó đo lường mức độ hiệu quả trong việc truyền tải dữ liệu đúng thời gian từ nguồn đến đích. Thước đo chất lượng dịch vụ này thường được xác định và đảm bảo trong các thỏa thuận về mức độ dịch vụ, đây là các tài liệu hợp đồng chặt chẽ giữa người dùng cuối và các nhà cung cấp dịch vụ. Chất lượng mạng dịch vụ là yếu tố quan trọng xác định sự khác biệt giữa các mạng và đóng vai trò quan trọng trong việc đáp ứng nhu cầu của người dùng. Điều này đòi hỏi mạng phải cung cấp khả năng truyền tải dữ liệu một cách đáng tin cậy và đúng thời gian, giúp đảm bảo rằng dịch vụ đáp ứng được các tiêu chuẩn đã cam kết trong các thỏa thuận mức độ dịch vụ.

## **1.4. Kết luận chương 1**

Hệ thống mạng máy tính ngày nay đang phát triển mạnh mẽ để đáp ứng nhu cầu ngày càng tăng của con người. Mặc dù có nhiều ưu điểm đáng kể, nhưng cũng không thiếu những thách thức và vấn đề phức tạp. Để giải quyết các khó khăn và đảm bảo sự phát triển và hiệu suất của hệ thống truyền thông mạng, các chuyên gia đã nghiên cứu và đề xuất nhiều giải pháp quan trọng.

Việc hiểu sâu hơn về cách mà gói tin được truyền tải trong mạng máy tính, cùng với việc xử lý các lỗi phát sinh trong quá trình truyền dữ liệu, đóng một vai trò quan trọng. Để xây dựng mạng tối ưu cho từng tổ chức, đơn vị, cơ quan hoặc trường học, chúng ta cần tìm hiểu kỹ hơn về các tiêu chí và vấn đề quan trọng để đánh giá chất lượng truyền dẫn trong mạng cụ thể.

Những nghiên cứu và khám phá này giúp tối ưu hóa hệ thống mạng, đảm bảo rằng mọi yêu cầu và định hướng được thỏa mãn một cách hiệu quả và đáng tin cậy.

# CHƯƠNG 2. QUẢN LÝ CHẤT LƯỢNG DỊCH VỤ QoS TRONG MẠNG IP

## **2.1. Tham số đánh giá chất lượng dịch vụ trong mạng IP**

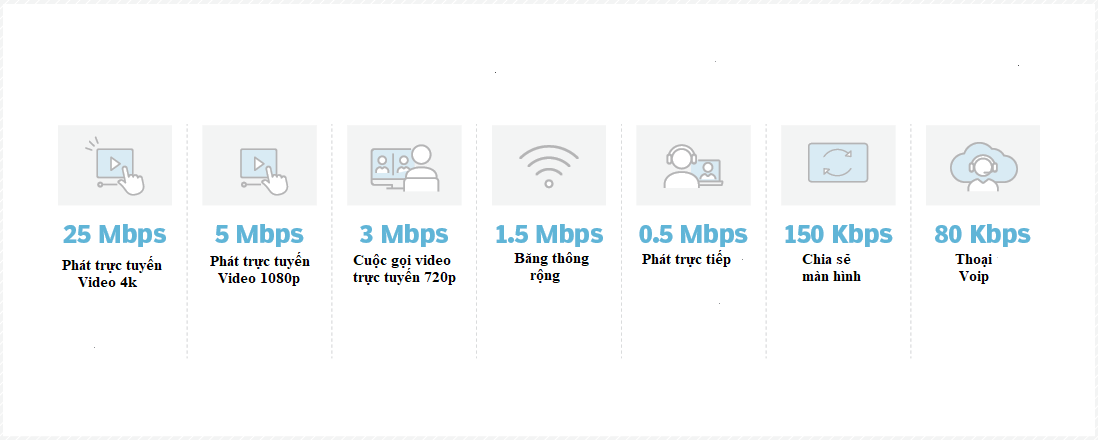
Internet được thiết kế để cung cấp dịch vụ tốt nhất nhưng thời gian trôi qua sự gia tăng đáng kể về lưu lượng truy cập và đặc biệt là sự tiến bộ của đa phương tiện lưu lượng truy cập qua Internet thì vấn đề tắc nghẽn xảy ra và việc truyền tải các gói tin trở nên chậm lại. Để khắc phục vấn đề này, một vấn đề về chất lượng dịch vụ đã được nghiên cứu như thông lượng, mất gói, độ trễ và chập chờn, …

Bảng 2.1 Các thông số của QoS

|  |  |
| --- | --- |
| **Thông số QoS** | **Các giá trị thực tiễn** |
| Băng thông (Nhỏ nhất) | 64Kb/s, 1.5Mb/s, 45Mb/s |
| Trễ (Lớn nhất) | 50ms trễ vòng, 150ms trễ vòng |
| Jitter (Biến động trễ) | 10% của trễ lớn nhất, 5ms biến động |
| Loss (Mất thông tin) | 1 trong 1000 gói chưa chuyển giao |
| Tính sẵn sàng (Tin cậy) | 99.99% |
| Bảo mật | Mã hóa và nhận thực trên tất cả các luồng lưu lượng |

### **2.1.1. Băng thông**

Băng thông là một tham số đơn giản biểu thị lượng dung lượng mà mạng phải đảm bảo cho ứng dụng trên cơ sở đầu cuối. Nói một cách đơn giản, tham số băng thông thể hiện tốc độ dữ liệu mà mạng phải đảm bảo cho ứng dụng. Mặc dù theo truyền thống, băng thông được biểu thị bằng bit trên giây (bps), nhưng các liên kết mạng hiện đại hiện có dung lượng lớn hơn nhiều, đó là lý do tại sao băng thông hiện nay thường được biểu thị bằng Mbps hoặc Gbps.



Hình 2.1. Băng thông yêu cầu cho một vài dịch vụ

Băng thông không phải là tài nguyên không giới hạn, vậy thì sự thiếu hụt băng thông sẽ có ảnh hưởng như thế nào? Sự thiếu hụt băng thông là một trong nhiều nguyên nhân làm giảm hiệu năng của các dịch vụ chạy trên mạng; đặc biệt là các dịch vụ liên quan đến thời gian như voice hoặc các dịch vụ yêu cầu băng thông cao như video.

Sự thiếu hụt băng thông trong mạng Internet thường xuyên xảy ra do nhiều nguyên nhân: Nguồn tài nguyên của mạng không đủ đáp ứng hay là sự tranh chấp tài nguyên của các luồng lưu lượng. Băng thông khả dụng được xác định bằng băng thông của đường định tuyến chia cho số luồng lưu lượng.

Chúng ta có thể dùng một vài giải pháp ngăn chặn sự thiếu hụt và cải thiện hiệu năng của băng thông:

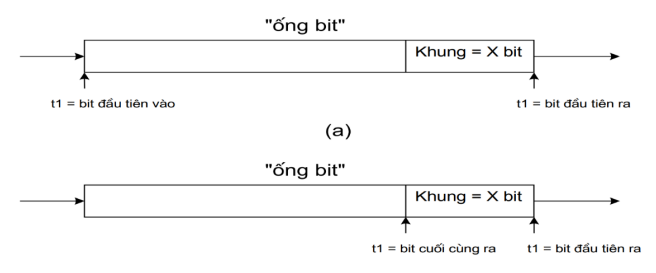
* Tăng băng thông: Cách tốt nhất để ngăn chặn sự thiếu hụt của băng thông là nâng cao tốc độ kết nối của tất cả các dịch vụ của nhà cung cấp dịch vụ cung cấp cho người sử dụng. Tuy nhiên nó không phải một phương pháp được sử dụng nhiều bởi vì một số điều kiện khách quan như chi phí cao, thời gian thực thi và giới hạn của công nghệ.
* Chuyển tiếp các gói tin sắp xếp theo độ ưu tiên: Giải pháp này thường được sử dụng hiện tại, nó liên quan đến việc sử dụng các kĩ thuật đảm bảo QoS. Giải pháp này phân loại lưu lượng thành các lớp QoS, sắp xếp theo thứ tự ưu tiên các luồng lưu lượng quan trọng đến ít quan trọng và các luồng lưu lượng có độ ưu tiên quan trọng sẽ được chuyển đi trước. Đây là một trong những kĩ thuật cơ bản được sử dụng của QoS và hàng đợi.
* Nén: Giải pháp này sẽ tối ưu đường liên kết bằng cách nén nội dung của các frame nhằm tăng băng thông khả dụng. Việc nén dữ liệu có thể được thực hiện bằng phần cứng hoặc phần mềm thông qua các thuật toán nén. Ngoài ra, nén trường tiêu đề (header) của gói tin cũng là một phương pháp đặc biệt hiệu quả đối với đường truyền có các gói tin có tỉ số header/gói tin là lớn. Phương pháp nén nội dung sẽ hiệu quả cho các mạng đầu cuối - đầu cuối, còn phương pháp nén tiêu đề sẽ hiệu quả với các liên kết bước - bước.

### **2.1.2. Thông lượng**

Thông lượng (Throughput) là một chỉ số quan trọng dùng để đo lường tốc độ truyền dữ liệu thành công trung bình trong điều kiện bình thường của một kết nối mạng. Nó là một yếu tố quan trọng để hiểu cách một kết nối hoạt động và khả năng truyền thông của nó. Để tính thông lượng, chúng ta lấy kích thước của các gói tin dữ liệu đã truyền đi chia cho thời gian mà quá trình truyền tải hoàn tất. Thông lượng thường được đo bằng byte mỗi giây, và nó có thể được sử dụng để so sánh với băng thông hiệu dụng và băng thông tối đa lý thuyết. Thông qua thông lượng, chúng ta có khả năng đánh giá hiệu suất của kết nối mạng và xác định xem liệu kết nối đang hoạt động tốt như thế nào.

### **2.1.3. Độ trễ**

Trễ (Delay) liên quan chặt chẽ với băng thông. Với các ứng dụng giới hạn băng thông thì băng thông càng lớn trễ sẽ càng nhỏ. Đối với các ứng dụng giới hạn trễ như là tín hiệu thoại 64kb/s, tham số QoS trễ lớn nhất các bit gặp phải khi truyền qua mạng. Tất nhiên là các bit có thể đến với độ trễ nhỏ hơn. Mối quan hệ giữa băng thông và trễ trong mạng được chỉ ra trong hình vẽ sau:



Hình 2.2 Trễ băng thông trong mạng

Trong phần (a), t2 – t1 = số giây trễ. Trong phần (b), X bit/(t2 – t1)=bit/s băng thông. Nếu có nhiều băng thông hơn tức là có nhiều bit đến hơn trong một đơn vị thời gian thì trễ tổng thể nhỏ hơn.

Băng thông và trễ của mạng có mối quan hệ với nhau và có thể tính toán tại nhiều nơi trong mạng, thậm chí từ đầu cuối tới đầu cuối. Thông tin truyền đi dưới dạng một chuỗi các khung truyền (gói tin IP cũng có thể sử dụng cho mục đích này), khoảng thời gian trôi qua kể từ khi bit đầu tiên của một khung đi vào mạng cho đến khi bit đầu tiên ra khỏi mạng gọi là trễ. Vì con đường của khung qua cả bộ chuyển mạch và bộ định tuyến, nên trễ có thể biến đổi, có các giá trị lớn nhất, nhỏ nhất, trung bình, độ lệch chuẩn….

Băng thông được định nghĩa là số bit của một khung chia cho thời gian trôi qua kể từ khi bit đầu tiên rời khỏi mạng cho tới khi bit cuối cùng rời khỏi mạng. Trên thực tế, đây chỉ là một trong số những cách đo có thể. Vì các khung có đường truyền đi từ liên kết truy nhập tới mạng xương sống nên băng thông mà khung truyền đi biến đổi đáng kể. Các mạng chuyển mạch gói cung cấp cho các ứng dụng các băng thông biến đổi phụ thuộc vào hoạt động và sự bùng nổ của ứng dụng. Băng thông biến đổi tức là trễ cũng biến đổi trên mạng.

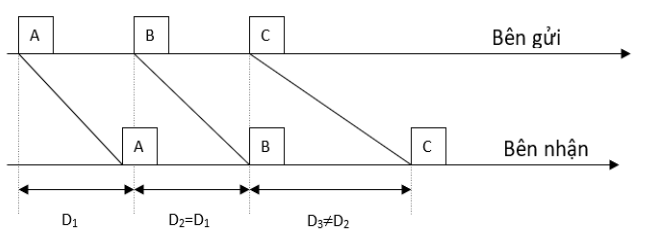
Các nút mạng được nhóm với nhau cũng có thể đóng góp vào sự thay đổi của trễ. Tại các nút mạng đều có quá trình xếp hàng. Trễ xảy ra do cần thời gian để chuyển gói tới hàng đợi đầu ra (output queue) và trễ do gói bị giữ trong hàng đợi. Tuy nhiên với các thuật toán xếp hàng có ưu tiên có thể giảm trễ xuống dưới 10ms. Ngoài ra cũng có thể kể đến trễ khi các bridge, switch và router chuyển dữ liệu, nó phụ thuộc vào tốc độ của hệ thống mạch, CPU cũng như kiến trúc bên trong các thiết bị mạng. Tham số QoS trễ chỉ xác định được trễ lớn nhất mà không đặt bất kì một giới hạn nhỏ hơn nào cho trễ của mạng.

### **2.1.4. Độ biến thiên trễ**

Thông số QoS jitter thiết lập giới hạn lên lượng biến đổi của trễ mà một ứng dụng có thể gặp trên mạng. Một cách đúng đắn hơn thì jitter được xem như là biến động trễ, bởi vì thuật ngữ jitter cũng được sử dụng trong mạng với nghĩa là sự khác biệt thời gian mức thấp trong kỹ thuật mã đường dây. Tuy nhiên, sử dụng thuật ngữ jitter đồng nghĩa với biến động trễ cũng là phổ biến, và ngữ cảnh sẽ phân biệt nghĩa nào đang được đề cập. Jitter không đặt một giới hạn nào cho các giá trị tuyệt đối của trễ, nó có thể tương đối thấp hoặc cao phụ thuộc vào giá trị của thông số trễ.

Jitter theo lí thuyết có thể là một giá trị mạng tương đối hay tuyệt đối. Ví dụ, nếu trễ mạng cho một ứng dụng được thiết lập là 100ms, jitter có thể đặt là cộng hoặc trừ 10% của giá trị này. Theo đó nếu mạng có trễ trong khoảng từ 90 đến 110ms thì vẫn đạt được yêu cầu về jitter (trong trường hợp này rõ ràng trễ không phải là lớn nhất). Nếu trễ là 200ms, thì 10% giá trị jitter sẽ cho phép bất kỳ giá trị trễ nào trong khoảng 180 đến 220ms. Mặt khác jitter tuyệt đối giới hạn cộng trừ 5ms sẽ giới hạn jitter ở các ví dụ trên trong khoảng từ 95 đến 105ms và từ 195 tới 205ms.

Các ứng dụng nhạy cảm nhất đối với các giới hạn của jitter là các ứng dụng thời gian thực như thoại hay video. Nhưng đối với các trang Web hay với truyền tập tin qua mạng thì lại ít quan tâm hơn đến jitter. Internet là gốc của mạng dữ liệu có ít khuyến nghị về jitter. Các biến đổi của trễ tiếp tục là vấn đề gây bực mình nhất gặp phải đối với các ứng dụng video và thoại dựa trên Internet. Jitter xảy ra do sự thay đổi khoảng thời gian giữa hai lần gói đến:



Hình 2.3. Sự thay đổi thời điểm đến gói

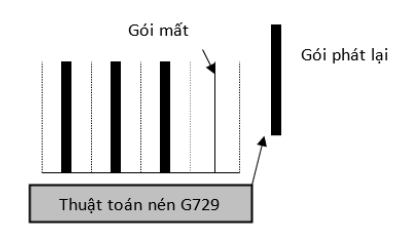
Jitter là vấn đề cố hữu trong các mạng chuyển mạch gói. Nguyên nhân từ cơ chế xử lý lưu giữ và chuyển gói tại các nút mạng. Ngoài ra, còn do các gói đi đến đích theo các đường truyền khác nhau trên mạng. Loại bỏ jitter đòi hỏi phải thu thập các gói và giữ chúng đủ lâu để cho phép các gói chậm nhất đến đích để được phát lại đúng thứ tự, điều này làm cho tổng độ trễ tăng lên.

Ngay cả khi trễ tuyệt đối có thể giảm nhỏ tối thiểu, một sự thay đổi độ trễ từ gói này đến gói sau cũng làm giảm chất lượng dịch vụ. Để khử jitter người ta dung một bộ đệm gọi là jitter buffer, đó có thể là một hàng đợi động với kích thước thay đổi phụ thuộc vào khoảng thời gian giữa hai lần gói đến của các gói trước vì bộ đệm cố định nếu quá lớn thì làm tăng trễ nếu quá nhỏ thì làm mất gói.

### **2.1.5. Mất gói**

Tại sao các mạng không chỉ Internet lại bị mất thông tin? Thực sự là có nhiều lí do, nhưng hầu hết trong số chúng có thể truy nguyên từ các ảnh hưởng của lỗi trên mạng. Ví dụ, nếu một kết nối bị hỏng, thì tất cả các bit đang truyền trên liên kết này sẽ không thể tới được đích. Nếu một nút mạng ví dụ như bộ định tuyến hỏng thì tất cả các bit ở trong bộ đệm và đang được xử lý tại nút đó sẽ biến mất không để lại dấu vết. Do những loại hư hỏng này có thể xảy ra trên mạng bất cứ lúc nào nên việc một vài thông tin bị mất độ trễ lỗi trên mạng là không thể tránh khỏi.

Ví dụ việc truyền tín hiệu thoại:



Hình 2.4. Phát lại gói cuối cùng thay thế gói bị mất

Gói thứ nhất, thứ hai, thứ ba đều đến được đích nhưng gói thứ tư bị mất trên đường truyền. Sau khi bên thu đợi một khoảng thời gian, nó sử dụng thuật toán “che dấu” ví dụ bằng cách phát lại gói thứ 3. Người nghe hầu như không cảm nhận được vì tín hiệu thoại bị mất chỉ là 20ms (ví dụ). Tuy nhiên, nếu mất gói liên tục hoặc tỉ lệ mất gói lớn thì chất lượng thoại sẽ bị giảm vì các kiểu “làm giả” gói thoại như vậy không thể kéo dài. Sự tổn thất gói trên 10% nói chung không thể chấp nhận được.

Tác động của mất thông tin tuỳ thuộc vào ứng dụng . Điều khiển lỗi trên mạng là một quá trình gồm hai bước: Bước đầu tiên là xác định lỗi. Bước thứ hai là khắc phục lỗi, nó có thể đơn giản là bên gửi truyền lại đơn vị bị mất thông tin. Một vài ứng dụng, đặc biệt là các ứng dụng thời gian thực, không thể đạt hiệu quả khắc phục lỗi bằng cách gửi lại đơn vị thông tin bị lỗi. Các ứng dụng không phải thời gian thực thì thích hợp hơn đối với cách truyền lại thông tin bị lỗi, tuy nhiên cũng có một số ngoại lệ (ví dụ các hệ thống quân sự tấn công mục tiêu trên không không thể sử dụng hiệu quả với cách khắc phục lỗi bằng truyền lại.

Vì những lý do này, tham số QoS Loss không những nên định rõ một giới hạn trên đối với ảnh hưởng của lỗi mà còn nên cho phép người sử dụng xác định xem có lựa chọn cách sửa lỗi bằng việc truyền lại hay không? Tuy nhiên, hầu hết các mạng (đặc biệt là mạng IP) chỉ cung cấp phương tiện vận chuyển thụ động còn việc xác định lỗi, khắc phục lỗi thường được để lại cho các ứng dụng (hay người dùng).

### **2.1.6. Độ tin cậy**

Các mạng tồn tại để phục vụ người sử dụng. Tuy nhiên mạng cần có biện pháp bảo dưỡng và phòng ngừa nếu các tình huống hỏng hóc tiềm tàng được phát hiện và được dự đoán trước. Một chiến lược đúng đắn bằng cách định kỳ tạm thời tách các thiết bị ra khỏi mạng để thực hiện các công việc bảo dưỡng và chẩn đoán trong một thời gian ngắn để có thể giảm thời gian ngừng hoạt động do hỏng hóc. Thậm chí, với biện pháp bảo dưỡng hoàn hảo nhất cũng không thể tránh được các lỗi không tiên đoán trước và các lỗi nghiêm trọng của kết nối và thiết bị theo thời gian.

Không lâu trước đây, mạng PSTN có lịch trình thời gian và bảo dưỡng nghiêm khắc hơn nhiều mạng dữ liệu . PSTN phải có khả năng truyền tải các cuộc gọi vào mọi thời điểm. Có những khoảng thời gian chỉ có rất ít cuộc gọi, như khoảng thời gian 3 đến 4 giờ sáng, nhưng lại có cuộc gọi hầu như tất cả các khoảng thời gian. Đương nhiên phải có những nguyên tắc để bảo dưỡng và phòng ngừa với mạng PSTN . Một số hoạt động có thể thực hiện lúc lưu lượng biết trước là tạm vắng và một số hoạt động có thể không bao giờ được thực hiện trong các giờ hoặc trong các ngày bận.

Mạng dữ liệu thực hiện công việc đó dễ hơn. Hầu hết mạng dữ liệu dành cho kinh doanh, thường là từ 8 giờ sáng đến 5 giờ chiều, từ Thứ Hai dến Thứ Sáu. Hoạt động bổ trợ có thể thực hiện ngoài giờ, và một tập kiểm tra đầy đủ với mục đích phát hiện ra các vấn đề có thể xảy ra trong các ngày nghỉ.

Internet và Web đã thay đổi tất cả. Một mạng toàn cầu phải giải quyết vấn đề rằng thực sự có một số người luôn cố gắng truy nhập vào mạng tại một số địa điểm. Và thậm chí Internet có ích ở nhà vào 10 giờ tối hơn là ở cơ quan vào 2 giờ chiều.

Tuy nhiên, nếu người sử dụng nhận thức rõ ràng rằng họ không thể có một mạng như mong muốn vào tất cả các khoảng thời gian. Và khi hỏng hóc xảy ra, dịch vụ sẽ được khôi phục nhanh chóng đến mức độ nào. Cả hai là khía cạnh chủ yếu của thông số QoS độ khả dụng hay độ tin cậy của mạng.

Một năm có 60\*60\*24\*365 hay 31.536.000 giây. Giả thiết một mạng khả dụng 99 phần trăm thời gian. Điều này cho phép nhà cung cấp dịch vụ có 315.360 giây, hay 87,6 giờ mạng không hoạt động trong một năm. Khoảng thời gian này là tương đối lớn. Giá trị 99.99 phần trăm sẽ tốt hơn nhiều, và thời gian ngừng hoạt động của mạng giảm xuống chỉ còn khoảng 50 phút trong một năm. Tât nhiên nhà cung cấp dịch vụ cần nhiều cơ chế dự phòng và khắc phục lỗi hơn để đạt được điều này. Bảng 2.2 cho thấy phần trăm sẵn sàng được biểu diễn dưới dạng thời gian ngừng hoạt động hàng năm.

Bảng 2.2. Tính sẵn sàng của mạng và thời gian ngừng hoạt động

|  |  |
| --- | --- |
| **Tính sẵn sàng của mạng** | **Tổng thời gian ngừng hoạt động trong một năm** |
| 99% | 3.65 ngày |
| 99.5% | 1.825 ngày |
| 99.9% | 8.76 giờ |
| 99.95% | 4.38 giờ |
| 99.99% | 52.56 phút |
| 99.995% | 26.28 phút |
| 99.999% | 5.25 phút |

Ngày nay, thông số QoS khả dụng của mạng thường vào khoảng 99.995%, hay khoảng 26 phút ngừng hoạt động trong một năm, kết nối khôi phục nhỏ hơn 4 giờ. Cũng có sự khác nhau giữa độ khả dụng và độ tin của mạng từ góc nhìn của từng người sử dụng và từ góc nhìn mạng thể. Ngày nay, toàn bộ mạng không hỏng tất cả và do đó làm cho tất cả người sử dụng bị cô lập cùng một lúc. Thông số QoS khả dụng thường được quy cho mỗi vị trí hoặc liên kết riêng lẻ. Một người sử dụng khó tính có thể than phiền rằng một liên kết chỉ sẵn sàng 99.7% trong tháng sẽ được nhắc nhở rằng 99.99% sẵn sàng như được quảng cáo và hứa hẹn là áp dụng cho toàn bộ mạng.

### **2.1.7. Bảo mật**

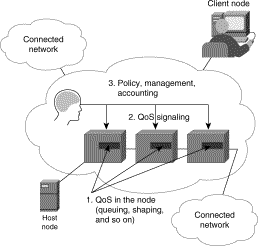
Bảo mật, một yếu tố mới trong danh sách về Chất lượng Dịch vụ (QoS), nhưng lại đóng một vai trò vô cùng quan trọng. Trên thực tế, trong một số trường hợp, mức độ bảo mật thậm chí có thể được xem xét ngay sau băng thông. Trong thời kỳ gần đây, sự bùng nổ của các mối đe dọa từ các hacker và sự lan tràn của virus trên mạng Internet toàn cầu đã làm cho bảo mật trở thành một vấn đề hàng đầu. Hầu hết các vấn đề liên quan đến bảo mật tập trung vào sự bảo vệ tính riêng tư, sự tin cậy và xác thực giữa khách hàng và máy chủ.

Các vấn đề liên quan đến bảo mật thường được liên kết với các phương pháp mật mã như mã hóa và giải mã. Tuy nhiên, không phải lúc nào các phương pháp mật mã cũng liên quan trực tiếp đến việc giải mã.

Một ví dụ cụ thể về một tham số QoS bảo mật có thể là "mã hóa và xác thực yêu cầu trên tất cả các luồng lưu lượng". Tuy nhiên, tùy thuộc vào tình huống, truyền dữ liệu có thể chỉ cần mã hóa mà không cần xác thực, trong khi các kết nối điện thoại trên Internet có thể chỉ cần xác thực để ngăn chặn gian lận. Ngày nay, tầm quan trọng của bảo mật như một tham số QoS không thể bị xem nhẹ, và nó đã trở thành một phần quan trọng không thể thiếu trong đánh giá và quản lý các hệ thống mạng hiện đại.

## **2.2. Kiến trúc của QoS**

Kiến trúc tổng quan về chất lượng cung cấp dịch vụ đòi hỏi tuân theo một loạt các yếu tố quan trọng. Đối với việc thực hiện QoS trong một mạng đơn lẻ, việc triển khai các tính năng xếp hàng, lập lịch và định hình lưu lượng là tất yếu. Cần sử dụng các kỹ thuật báo hiệu để đảm bảo sự phối hợp về chất lượng dịch vụ giữa các mạng khác nhau. Ngoài ra, cần có các cơ chế chính sách và chức năng quản lý để kiểm soát lưu lượng mạng trên các mạng đó.



Hình 2.5. Mô hình điều khiển QoS

Chủ đề trọng tâm của kiến trúc chất lượng dịch vụ là quản lý toàn bộ sự phức tạp liên quan đến việc truyền tải dữ liệu tại các nút cuối, thay vì ở mức mạng trung gian. Sự phức tạp có thể khác nhau giữa các nhà cung cấp và phụ thuộc vào yêu cầu cụ thể của người dùng cuối. Đôi khi, quản lý toàn bộ sự phức tạp tại các nút cuối có thể là lựa chọn tốt hơn, trong khi đôi khi yêu cầu can thiệp tại mức mạng hệ thống, chẳng hạn qua việc quản lý bộ định tuyến.

Sự lựa chọn giữa việc xử lý tất cả sự phức tạp trên bộ định tuyến mạng hay bộ định tuyến biên có thể phụ thuộc vào nhiều yếu tố khác nhau. Một số có thể cho rằng việc xử lý toàn bộ sự phức tạp trên bộ định tuyến mạng là hợp lý, bởi vì bộ định tuyến mạng chịu trách nhiệm gửi lưu lượng qua đường truyền tối ưu nhất qua mạng. Trong khi đó, người khác có thể cho rằng các kỹ thuật QoS không phải lúc nào cũng phù hợp cho bộ định tuyến mạng, và thay vào đó, nên tập trung vào bộ định tuyến biên.

Do đó, để cung cấp dịch vụ tốt nhất, đặc biệt đối với lưu lượng thoại thời gian thực, cần xem xét cả vai trò của cả hai thành phần: bộ định tuyến biên và bộ định tuyến mạng. Bộ định tuyến biên thường thực hiện các chức năng như phân loại gói tin, kiểm soát quyền truy cập và quản lý cấu hình, trong khi bộ định tuyến mạng thực hiện các chức năng kiểm soát, quản lý và tránh tắc nghẽn.

## **2.3. Các yếu tố chung cho kiến trúc QoS**

Trong kiến ​​trúc chất lượng dịch vụ, các yếu tố quan trọng bao gồm các nguyên tắc, khuôn khổ, đặc điểm kỹ thuật và cơ chế cho dịch vụ đầu cuối.

### **2.3.1. Nguyên tắc QoS**

*Nguyên tắc tích hợp:* Cho thấy rằng QoS phải có khả năng cấu hình được, có thể dự đoán trước và duy trì được trên toàn bộ các lớp cấu trúc để đáp ứng QoS từ đầu cuối đến đầu cuối. Các luồng di chuyển dọc theo các module tài tại mỗi lớp từ thiết bị truyền thông nguồn, đi xuống ngăn xếp giao thức nguồn, đi xuyên qua mạng, đi lên ngăn xếp giao thức phía thu và tới thiết bị bên ngoài. Mỗi module nguồn mà luồng đi qua phải cung cấp khả năng cấu hình QoS dựa trên các đặc tính kỹ thuật của QoS, sự đảm bảo nguồn được cung cấp bởi cơ cấu điều khiển QoS và duy trì các luồng đang truyền.

*Nguyên tắc phân tách:* Cho thấy các việc truyền, điều khiển và quản lý là các hoạt động cấu trúc phân biệt về chức năng. Nguyên lý này cho thấy rằng các ngăn xếp đó phải được phân tách theo cấu trúc QoS Framework. Một khía cạnh của hoạt động này là sự phân biệt giữa báo hiệu và dữ liệu truyền. Thường luồng dữ liệu yêu cầu cấp băng thông cao, trễ nhỏ như, nhưng có những luồng dữ liệu chỉ yêu cầu băng thông thấp như báo hiệu và các dịch vụ thuộc loại được đảm bảo.

*Nguyên tắc minh bạch:* Cho thấy rằng các ứng dụng được bảo vệ khỏi sự phức tạp của các đặc tính kỹ thuật cơ bản của QoS và việc quản lý QoS. Một khía cạnh quan trọng của tính trong suốt đó là API dựa trên cơ sở QoS mà tại đó các mức QoS cần thiết được khai báo. Lợi ích của tính trong suốt là nó giảm nhu cầu đưa các chức năng vào ứng dụng, giấu đi các chi tiết của đặc tính kỹ thuật cơ bản khỏi ứng dụng và nó giao phó sự phức tạp của việc xử lý các hoạt động quản lý QoS cho Framework nằm dưới.

*Nguyên tắc quản lý tài nguyên không đồng bộ:* Hướng dẫn sự phân chia chức năng giữa các module cấu trúc gắn liền với mô hình của cơ chế điều khiển và quản lý. Đây là việc bắt buộc nó phản ánh trực tiếp tính chính xác thời gian gốc, việc bắt buộc theo thời gian gốc là hoạt động song song cùng với các hoạt động quản lý nguồn trong môi trường truyền thông phân tán.

*Nguyên tắc hoạt động:* Gộp rất nhiều các quy tắc bổ sung vào các hệ thống truyền thông được thực hiện bởi QoS được công nhận rộng rãi mà các hệ thống đó hướng dẫn sự phân chia chức năng trong việc cấu trúc nên các giao thức truyền thông để có hiệu quả cao tuỳ theo các nguyên lý thiết kế hệ thống, tránh phải ghép kênh, khuyến nghị cho việc cấu trúc nên các giao thức truyền thông, và sử dụng các trợ giúp phần cứng cho quá trình xử lý giao thức có hiệu quả.

### **2.3.2. Cơ chế QoS**

Chất lượng của cơ chế dịch vụ được thiết kế dựa trên các đặc điểm kỹ thuật của người dùng cuối. Có hai loại chất lượng cho cơ chế dịch vụ: tĩnh và động. Trong cơ chế tĩnh, chúng ta xử lý chất lượng dịch vụ đã được cung cấp, trong khi trong cơ chế động, quản lý và kiểm soát chất lượng dịch vụ được mô tả dựa trên nhu cầu của người dùng cuối. Có ba cơ chế chính liên quan đến chất lượng dịch vụ: cơ chế cung cấp, cơ chế kiểm soát và cơ chế quản lý.

*Cơ chế cung cấp:* bao gồm ba thành phần: Các giao thức bảo lưu tài nguyên mạng; Chất lượng dịch vụ lập bản đồ; Kiểm soát truy cập lưu lượng mạng.

*Cơ chế kiểm soát:* cung cấp khả năng kiểm soát các luồng lưu lượng khác nhau. Mức độ kiểm soát được xác định trong giai đoạn cung cấp chất lượng dịch vụ. Các cơ chế kiểm soát lưu lượng cơ bản như định hình dòng chảy, lập kế hoạch dòng chảy, chính sách dòng, kiểm soát lưu lượng, đồng bộ hóa luồng.

*Cơ chế quản lý*: các yếu tố được bao gồm trong cơ chế này là giám sát, bảo trì, suy giảm, tín hiệu, khả năng mở rộng của QoS.

## **2.4. Cải thiện chất lượng dịch vụ trong mạng IP**

### **2.4.1. Trường hợp mạng không áp dụng QoS**

QoS mạng IP là nói đến các kỹ thuật xử lý lưu lượng trong mạng truyền số liệu sử dụng bộ giao thức IP (Internet Protocol) nhằm đảm bảo các loại lưu lượng có yêu cầu chất lượng dịch vụ khác nhau được đối xử ưu tiên khác nhau. Chẳng hạn, trong một mạng IP có ba ứng dụng là truyền file FTP, dịch vụ gọi điện thoại Voice IP và Video Conferencing.

Như trước đây, khi mà nhu cầu sử dụng mạng của con người chưa cao bởi vì sự mới mẻ, chưa phổ biến và các ứng dụng chưa nhiều thì lưu lượng trên mạng có thể đáp ứng cho hầu hết các ứng dụng lúc bây giờ, nhưng khi nó trở nên phổ biến số người dùng nhiều và các ứng dụng cũng tăng lên thì tài nguyên băng thông mạng trở nên thiếu hụt, điều này sẽ dẫn tới việc mất gói đáng kể khi truyền qua mạng. Để khắc phục điều này thì QoS ra đời với nhiệm vụ ưu tiên cho các ứng dụng thời gian thực bằng cách cấp phát thêm băng thông và đặt chúng ở mức ưu tiên cao hơn các ứng dụng khác.

Chất lượng dịch vụ chỉ có thể được xác định bởi người sử dụng, vì chỉ người sử dụng mới có thể biết được chính xác ứng dụng của mình cần gì để hoạt động tốt. Tuy nhiên, không phải người sử dụng tự động biết được mạng cần phải cung cấp những gì cần thiết cho ứng dụng, họ phải tìm hiểu các thông tin cung cấp từ người quản trị mạng và chắc chắn rằng, mạng không thể tự động đặt ra QoS cần thiết cho một ứng dụng của người sử dụng. Để giải quyết vấn đề đó nhà cung cấp và khách hàng họ lập ra một bản cam kết, trong đó nhà cung cấp phải thực hiện đầy đủ cung cấp các thông số thoả mãn chi tiết bản cam kết đặt ra. Còn phía đối tác cũng phải thực hiện đầy đủ điều khoản của mình.

Nếu một mạng không áp dụng QoS thì sẽ xảy ra các trường hợp như sau:

Bảng 2.3. Các dấu hiệu của mạng khi không có QoS

|  |  |
| --- | --- |
| **Kiểu lưu lượng** | **Các vấn đề khi không có QoS** |
| Voice | - Voice nghe khó hiểu.  - Voice không liên tục, tiếng nói bị méo.  - Người gọi không biết người nhận kết thúc cuộc gọi khi nào hay kết thúc chưa.  - Cuộc gọi không kết nối được. |
| Video | - Hình ảnh hiển thị chập chờn.  - Âm thanh không đồng bộ với video.  - Sự di chuyển của hình ảnh chậm lại. |
| Data | - Dữ liệu được chuyển đến khi nó không còn giá trị nữa.  - Dữ liệu phản hồi không đúng so với ban đầu.  - Thời gian truyền bị gián đoạn làm cho người dùng thất vọng và từ bỏ hoặc thực hiện lại dịch vụ. |

Nếu một mạng được tối ưu hoàn toàn cho một loại dịch vụ, thì người sử dụng ít phải xác định chi tiết các thông số QoS. Ứng dụng Voice IP đòi hỏi việc truyền dữ liệu phải liên tục, độ trễ thấp (thời gian thực). Ứng dụng FTP không yêu cầu cao về độ trễ, miễn là truyền đủ và chính xác nội dung dữ liệu. Ứng dụng Video Conferencing cũng cần việc truyền dữ liệu phải liên tục, độ trễ thấp ngoài ra nó còn đòi hỏi dữ liệu chuyển tiếp phải có tính tương tác, thống nhất cao để hình ảnh và âm thanh có thể truyền đến người nhận đồng thời mà không bị mất hay lệch gói.

Với mạng IP này, chúng ta cần phải áp dụng các kỹ thuật xử lý lưu lượng nhằm phân loại lưu lượng và áp dụng các chính sách ưu tiên khác nhau nhằm đảm bảo lưu lượng IP telephony phải có độ ưu tiên đường truyền cao hơn, thậm chí thông suốt kể cả khi mạng bị nghẽn so với dịch vụ truyền file FTP, hệ thống mạng như vậy được gọi là có cam kết chất lượng dịch vụ mà sau đây gọi tắt là QoS.

### **2.4.2. Các yêu cầu chất lượng dịch vụ trong mạng IP**

Mỗi ứng dụng đều có đặc tính riêng của nó, do đó để xác định được yêu cầu chất lượng dịch vụ, hệ thống thường nhận biết dựa trên các lớp dịch vụ. Theo quan điểm của ITU-T, các lớp dịch vụ được chia như sau:

Bảng 2.4. Phân chia các lớp dịch vụ

|  |  |
| --- | --- |
| **Lớp QoS** | **Các đặc tính QoS** |
| 0 | Thời gian thực, nhạy cảm với jitter, tương tác cao |
| 1 | Thời gian thực, nhạy cảm với jitter, tương tác cao |
| 2 | Dữ liệu chuyển tiếp, tương tác cao |
| 3 | Dữ liệu chuyển tiếp, tương tác |
| 4 | Tổn hao thấp |
| 5 | Các ứng dụng nguyên thủy của mạng IP ngầm định |

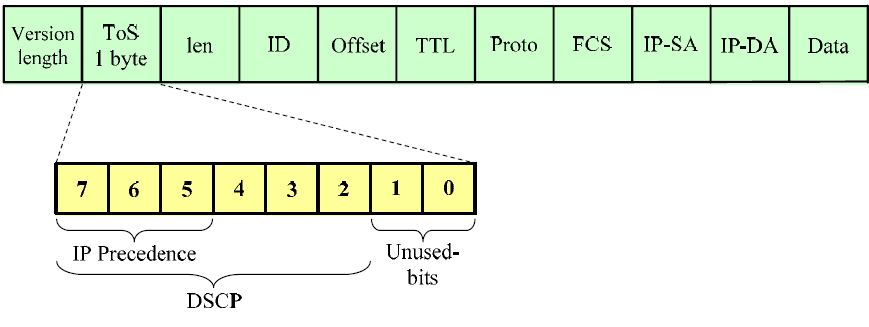
Như vậy, theo quan điểm của ITU thì các ứng dụng thời gian thực và các ứng dụng có tính tương tác cao được đặt lên hàng đầu đối với mạng IP, phần lớn các ứng dụng này được triển khai trong các mạng chuyển mạch hướng kết nối (chuyển mạch kênh và ATM). Trong khi đó, mạng IP nguyên thủy không hỗ trợ QoS cho các dịch vụ thời gian thực.

### **2.4.3. Phân lớp lưu lượng trong mạng IP**

Dựa trên các đặc tính của lưu lượng được truyền tải, thực hiện phân loại các gói tin thành các nhóm riêng biệt mà có thể áp dụng các kỹ thuật QoS. Bằng việc phân loại gói, ta có thể phân chia lưu lượng truyền tải thành nhiều mức ưu tiên khác nhau hay nhiều lớp dịch vụ khác nhau.

Các phương thức phân loại gói trước đây bị giới hạn bởi số bít trong trường tiêu đề (Header). Trong các phương thức gần đây đánh dấu gói kết hợp với phân loại gói cho phép ta có thể thiết lập giá trị trên các tiêu đề tại các lớp 2, 3 hoặc có thể thiết lập trên tải trọng của gói.

Các router tại biên của mạng sử dụng chức năng phân loại gói để nhận dạng các gói thuộc về lớp lưu lượng nào trên mạng tuỳ theo một hoặc nhiều trường trong tiêu đề gói IP. Sau đó chức năng đánh dấu được sử dụng để đánh dấu gói đó bằng cách thiết lập các bit trong trường IP Precedence hoặc trường DSCP (Differentiated Service Code Point). Trong mạng IP các gói được lưu chuyển từ nguồn đến đích với mức ưu tiên khác nhau. Để xác định IP Prececdence cho các gói tin người ta sử dụng 3 bits ToS.



Hình 2.6. Mô tả trường ToS trong gói IP

Trên cơ sở đó thiết lập các lớp dịch vụ khác nhau cho các gói tin. Với các lớp dịch vụ tùy theo các yêu cầu cụ thể mà thực hiện các phương pháp cấu hình tính năng QoS khác nhau để quản lý tắc nghẽn hay phân phối băng thông.

Việc gán thứ tự ưu tiên cho các gói thông qua tổ hợp 3 bits ToS trong địa chỉ mào đầu IP để tạo ra các lớp dịch vụ khác nhau. Về lý thuyết với 3 bits ToS có thể phân chia thành 8 loại CoS khác nhau. Tuy nhiên chỉ phân 6 lớp dịch vụ tương ứng với 6 giá trị ToS, 2 giá trị còn lại được dành cho sử dụng trong thông tin nội bộ mạng.

Trong chế độ mặc định các phần mềm thường không thiết lập các gía trị của IP Precedence. Như vậy để có thể sử dụng các phần tử mạng cần thực hiện gán giá trị IP Precedence trong trường tiêu đề (header). Chú ý rằng các gói đến từ các mạng khác có thể đã được gán giá trị ưu tiên do đó nên thực hiện thiết lập lại giá trị ưu tiên cho tất cả các gói được gửi tới. Bằng cách điều khiển giá trị IP Precedence chúng ta có thể ngăn chặn các người dùng không mong muốn hay lựa chọn các dịch vụ thích hợp hơn.

## **2.5. QoS trong một mô hình mạng**

**❖ Quản lý tắc nghẽn**

Do sự bùng nổ tự nhiên của lưu lượng thoại/video/dữ liệu, nên vài luồng lưu lượng sẽ vượt quá tốc độ của một liên kết. Tại điểm này, các router sẽ làm gì? Sẽ tạo một bộ đệm trong hàng đợi và cho phép gói đầu tiên vào sẽ ra đầu tiên? Hay là sẽ đặt các gói vào các hàng đợi khác nhau. Công cụ quản lý tắc nghẽn bao gồm hàng đợi ưu tiên PQ (Priority Queuing), hàng đợi khách CQ (Custom Queuing), hàng đợi hợp lý theo trọng số WFQ (Weighted Fair Queuing) và hàng đợi hợp lý theo trọng số dựa trên cơ sở lớp CBWFQ (Class-Base Weighted Fair Queuing).

**❖ Quản lý hàng đợi**

Do các hàng đợi không có kích thước vô hạn nên chúng có thể bị đầy và tràn. Khi hàng đợi đầy, các gói thêm vào không được đặt trong hàng đợi và sẽ bị đẩy ra ngoài. Đó là hiện tượng “tail drop” - rơi đuôi (tức là các gói cuối sẽ bị đẩy ra từng gói một). Vấn đề xảy ra với hiện tượng “tail drop” là các router không thể ngăn chặn các gói rơi ra ngoài (kể cả các gói có độ ưu tiên cao). Vì thế cần giải quyết hai vấn đề sau:

* Thử tạo một hàng đợi và đảm bảo là nó không bị đầy, ở hàng đợi đó chứa các gói có độ ưu tiên cao.
* Thiết lập tiêu chuẩn đối với các gói bị rơi ra ngoài: các gói có độ ưu tiên thấp sẽ bị đẩy ra ngoài trước các gói có độ ưu tiên cao.

Thuật toán WRED (Weighted Early Random Detect)-phát hiện sớm ngẫu nhiên theo trọng số có thể thực hiện được cả hai điều trên.

**❖** **Lập lịch gói tin**

Lập lịch gói tin là thực hiện thiết lập thứ tự đi ra khỏi hàng đợi cho từng gói, dựa trên đặc tính của cổng đầu ra bộ định tuyến mà các gói tin sẽ được phân bổ và đưa tới cổng đầu ra theo luật. Kỹ thuật lập lịch gói tin chính là mấu chốt của chất lượng dịch vụ và là thước đo công nghệ giữa các nhà cung cấp dịch vụ.

Một vài kỹ thuật lập lịch gói tin thường được sử dụng: Vào trước ra trước FIFO (First in – First out), hàng đợi ưu tiên PQ (Priority Queuing), hàng đợi cân bằng FQ (Fair Queuing), hàng đợi quay vòng theo trọng số WRR (Weighted Round Robin), hàng đợi cân bằng theo trọng số WFQ (Weighted Fair Queuing) và hàng đợi cân bằng trọng số dựa theo lớp (Class Based WFQ).

**❖ Chính sách và định hình lưu lượng**

Phương pháp này khiến cho tốc độ luồng lưu lượng đến bị thay đổi để giúp điều hoà luồng lưu lượng đến với đầu ra. Khi luồng lưu lượng đến có độ bùng nổ cao, nó cần phải đệm để giảm sự bùng nổ và mềm hơn. Việc điều chỉnh tốc độ lưu lượng được ví như quá trình “dừng và đi”. Thời gian trễ tại bộ đệm sẽ khiến các gói tin ở đầu ra bộ định tuyến được điều chỉnh theo yêu cầu. Có hai dạng định hướng lưu lượng thường được sử dụng là định hướng lưu lượng thuần và định hướng lưu lượng gáo rò.

## **2.6. Kết luận chương 2**

Việc vận chuyển một dữ liệu trong hệ thống đường truyền mạng đòi hỏi quá trình xử lý qua nhiều giai đoạn, từ xử lý tại mạng cục bộ cho đến xử lý từ điểm gửi đến điểm nhận. Chương 2 đã trình bày chi tiết các phương thức vận chuyển dữ liệu, bao gồm các quy trình và vấn đề mà gói dữ liệu gặp phải trong quá trình truyền dẫn. Điều này đặt ra câu hỏi về cách tiếp cận và áp dụng các phương pháp và phương thức để giải quyết các vấn đề xuất phát trên đường truyền và làm thế nào để đảm bảo việc truyền dữ liệu hiệu quả từ nguồn đến đích.

Cách mà các vấn đề này được xử lý sẽ ảnh hưởng đến chất lượng truyền dẫn, bao gồm chất lượng dịch vụ truyền dẫn, và các thông số quan trọng như độ trễ, độ nghẽn mạng, biến động thời gian truyền, và nhiều yếu tố khác. Nhìn từ góc độ này, chúng ta cần đánh giá và áp dụng những phương pháp giải quyết thích hợp vào mạng và người dùng để đảm bảo truyền dẫn dữ liệu với chất lượng tối ưu, không chỉ cho mạng mà còn cho tất cả người dùng của nó.

# CHƯƠNG 3. MỘT SỐ GIẢI PHÁP ĐÁNH GIÁ TRUYỀN DẪN LƯU LƯỢNG TRONG MẠNG IP

## **3.1. Cải thiện thông số QoS**

### **3.1.1. Kỹ thuật quản lý tắc nghẽn dữ liệu**

Điều khiển luồng phía đầu cuối: đây không phải lược đồ điều khiển tắc nghẽn nhưng cũng là cách để tránh trường hợp phía phát gửi quá nhiều lưu lượng vượt quá cả không gian bộ đệm phía thu.

Điều khiển tắc nghẽn mạng: trong lược đồ này, các hệ thống đầu cuối giảm tốc độ của luồng lưu lượng để tránh tắc nghẽn trong mạng, cơ chế này tương tự như điều khiển luồng đầu cuối, nhưng mục đích chính là để giảm tắc nghẽn trong mạng chứ không phải phía thu.

Tránh tắc nghẽn trên cơ sở mạng: trong lược đồ này, router sẽ cố gắng dò tìm ra tắc nghẽn khi nó có khả năng xảy ra, và cố gắng giảm tốc độ của luồng đầu vào trước khi hàng đợi hàng đợi đầy.

Phân phối tài nguyên: kỹ thuật bao gồm tiến trình lập lịch có sử dụng các mạch vật lý hoặc các nguồn tài nguyên khác. Một mạch ảo được xây dựng qua nhiều chuyển mạch cùng với băng thông đảm bảo cũng là một loại phân phối tài nguyên. Kỹ thuật này rất khó nhưng nó có khả năng loại trừ tắc nghẽn trong mạng bằng việc khoá các lưu lượng vượt quá khả năng của mạng.

Một giải pháp quan trọng nhất trong điều khiển tắc nghẽn đó là sử dụng hàng đợi. Các bộ đệm trong các thiết bị mạng được quản lý bởi rất nhiều kỹ thuật hàng đợi. Nói đúng ra quản lý hàng đợi có thể tối thiểu hoá việc mất gói trong mạng và tắc nghẽn xảy ra cũng như là cải thiện được hiệu năng của mạng. Một kỹ thuật hàng đợi cơ bản nhất là FIFO, các gói được xử lý theo trật tự mà chúng đến hàng đợi, còn hàng đợi ưu tiên sử dụng cấu trúc đa hàng đợi với các mức ưu tiên khác nhau sẽ ưu tiên xử lý các gói quan trọng nhất và truyền tới các node kế tiếp.

Một kỹ thuật hàng đợi quan trọng nữa là tự ấn định các luồng cho chính bản thân các hàng đợi. Với các luồng khác nhau thì độ ưu tiên cũng được khác nhau, và mỗi luồng đều được xử lý để chắc chắn rằng chúng không làm tràn hàng đợi. Việc tách rời các hàng đợi theo cách này đảm bảo rằng các hàng đợi sẽ chỉ chứa các gói từ một nguồn đơn lẻ.

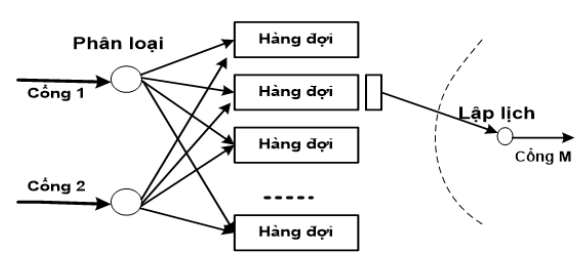
### **3.1.2. Tối ưu tốc độ truyền dẫn và tốc độ gói**

Việc đảm bảo tốc độ truyền dẫn phụ thuộc vào việc quy ước phân loại tin đảm bảo tính chất lượng truyền trong hệ thống truyền dẫn của mạng. Việc đó được hình thành những quy tắc phân loại:

Một sơ đồ phân loại chung lựa chọn một số mẫu N bit trong phần tiêu đề của gói tin để phân biệt tới 27 loại hoặc gói. Mẫu này được gọi là khóa phân loại.

Một khóa phân loại không thể dài tùy ý – bộ nhớ của một router bắt buộc phải giới hạn số lượng thông tin trạng thái mà nó có thể lưu giữu để nhận biết lớp. Thời gian xử lí mỗi gói kết hợp trong từng bước phân loại cũng tăng lên theo chiều dài khóa. Điều đó có thể cản trở hiệu suất truyền dẫn của router.

Nhân tố hạn chế thực hiện của hầu hết các router là số tiêu đề gói có thể được xử lý trên một giây, một hạn chế có thể thấy lưu lượng bao gồm nhiều gói nhỏ hơn là một lượng ít các gói lớn hơn. Khi phân loại gói MF (phân loại đa đường) thêm vào tìm kiếm VIB, tầng phân loại gói tự nó trở thành một điểm nghẽn trong Router. Nếu bộ xử lý phân đại không thể giữ gói tự nó trở thành một điểm nghẽn trong router. Nếu bộ xử lý phân loại không thể giữ các gói như giao diện bên trong chúng yêu cầu, một bộ đệm được yêu cầu trước tăng phân loại. Các gói vào có thể được sắp xếp trong hàng đợi FIFO ở đây không quan tâm tới những loại nào, chúng có thể là một vùng nhớ hoặc được loại bỏ từ giai đoạn phân loại.



Hình 3.1 Phân loại hàng đợi và lặp lịch từng chặng

Bộ đếm trước phân loại là một điều bất thường cho các router nỗ lực tối đa, nhưng rất quan trọng khi cân nhắc đến vai trò của một router trong mạng có chất lượng dịch vụ truyền dẫn cho phép. Bộ đêm này thậm chí chỉ có thể chấp nhận nếu hoạt động phân loại ở một tỉ lệ thỏa đáng của tốc độ đầu vào. Phụ thuộc vào sự bùng nổ mong đợi của gói tin IP nhỏ đến bộ đệm.

### **3.1.3. Bổ sung QoS**

Nếu một mạng thiếu QoS thì người sử dụng phải tự thêm vào các phương pháp của mình để có QoS cần thiết. Trong tất cả các tham số QoS, tham số mà người sử dụng khó tự thêm vào nhất là trễ. Thực tế sẽ đơn giản hơn nhiều nếu khắc phục được nhược điểm của QoS bằng cách thêm băng thông hơn là bất cứ cách nào khác. Thêm vào đủ băng thông thì ít nhất trễ và jitter sẽ được cải thiện. Nếu băng thông được thêm vào đúng đắn thì thậm chí cả lỗi, tính sẵn sàng và bảo mật cũng sẽ được cải thiện. Kết quả của việc thêm băng thông là có thể dự đoán được. Đầu tư vào băng thông để nhận được các kết quả biết trước thì tốt hơn là đầu tư vào một cách mới nào đó để vận chuyển lỗi đi vòng quanh và sau đó nhận ra là không có gì tốt hơn trước đó.

Như vậy là có hai lựa chọn để nhận được QoS cho người sử dụng và cho ứng dụng đó là tích hợp QoS hay là thêm QoS lên trên mạng. Điều này thực sự là không có gì khác hơn là việc cân nhắc giữa việc có sẵn QoS trong mạng và việc thêm QoS ở cấp ứng dụng bên ngoài mạng.

Bảng 3.1 Một số phương pháp thực tiễn cải thiện QoS

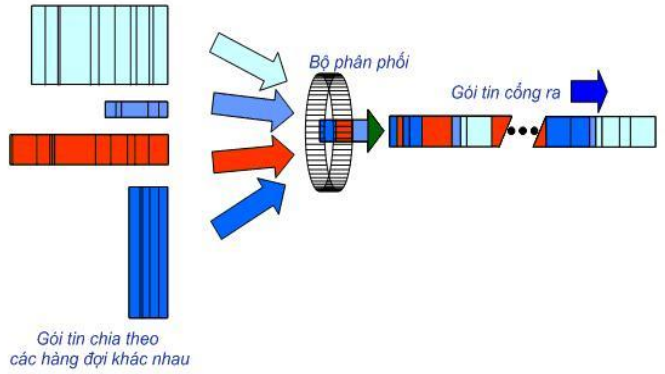
|  |  |
| --- | --- |
| **Cải thiện thông số QoS** | **Thực tiễn áp dụng** |
| Băng thông | Dồn kênh theo hướng ngược để tăng khả năng cao cho nhiều cuộc gọi |
| Trễ | Không làm gì nhiều trừ cố gắng tối thiểu các bước nhảy giữa các bộ định tuyến |
| Jitter | Thêm các bộ đếm Jitter |
| Mất thông tin | Thêm phần tiền sửa lỗi vào gói thoại |
| Tính sẵn sàng | Sử dụng nhiều liên kết đến ISP, thậm chí sử dụng nhiều ISP |
| Bảo mật | Thêm các phương pháp nhận thực và mã hóa chính họ |

Dồn kênh ngược có thể cần để cung cấp nhiều luồng lưu lượng VoIP thay vì kết nối VoIP riêng lẻ. Các bộ đệm jitter được sử dụng rộng rãi với bất kì hình thức VoIP nào không cần biết có bao gồm Internet hay không, bởi vì chỉ có PSTN trên cơ sở kênh mới có giới hạn đủ chặt chẽ về jitter để thoả mãn thoại. Ảnh hưởng của lỗi có thể được tối thiểu một phần bằng cách sử dụng mã FEC (Forward Error-Correcting Code), nhưng điều này hiếm khi được thực hiện. FEC yêu cầu tính tương thích nên nó giới hạn sự lựa chọn của người sử dụng, và FEC cũng không giúp được gì khi toàn bộ gói bị mất trên Internet.

Tính sẵn sàng được tăng cường bằng cách sử dụng nhiều liên kết tới một ISP hoặc thậm chí sử dụng nhiều ISP. Cuối cùng, bảo mật theo truyền thống là một vấn đề cần sự quan tâm về QoS của người sử dụng và VoIP hay điện thoại Internet có thể sử dụng một trong nhiều cách để đảm bảo tính riêng tư và nhận thực, mặc dù khả năng hoạt động cùng với nhau vẫn còn là vấn đề cần giải quyết.

## **3.2. Các cơ chế phân phối lưu lượng ra**

Nói đến các kỹ thuật QoS người ta người nhắc nhiều đến cơ chế hàng đợi. Ở trạng thái bình thường khi không có tắc nghẽn xảy ra các gói tin sẽ được gửi đi ngay khi chúng được chuyển tới. Trong trường hợp xảy ra tắc nghẽn trên một giao diện nào đó, nếu như không áp dụng các kỹ thuật điều khiển tắc nghẽn, các gói tin đến nhanh hơn có thể được gửi đi trước kết hợp với thời gian tắc nghẽn kéo dài có thể phát sinh rớt gói, ảnh hưởng đến chất lượng dịch vụ. Trong một số trường hợp hiện tượng tắc nghẽn kéo dài, khả năng xử lý của CPU bị quá tải rất dễ dẫn đến hiện tượng “treo” mạng, hoặc các gói bị loại bỏ nhiều gây ảnh hưởng đến chất lượng dịch vụ, do đó ngoài các cơ chế phân loại lưu lượng, các cơ chế tránh tắc nghẽn cũng cần được áp dụng trong các mạng IP.



Hình 3.2. Mô hình phân phối lưu lượng ra

Việc điều khiển tắc nghẽn đòi hỏi xây dựng các cơ chế hàng đợi, các gói tin sẽ được “tích tụ” tại giao diện tạo thành hàng đợi và được gửi đi ngay khi có thể. Thứ tự các gói tin được gửi đi tùy theo giá trị ưu tiên của chúng và phương thức xử lý hàng đợi được cấu hình trên cổng giao diện. Nói cách khác hàng đợi trên router là cần thiết để điều chỉnh sự bùng nổ khi tốc độ gói đến lớn hơn tốc độ gói xuất phát vì một trong 2 lý do là giao diện đầu vào nhanh hơn giao diện đầu ra và giao diện đầu ra thu nhận các gói đến từ nhiều giao diện khác nhau.

Trong kỹ thuật QoS có bốn loại cơ chế hàng đợi được sử dụng, mỗi một cơ chế có các nguyên tắc sắp xếp hàng đợi và xử lý tắc nghẽn khác nhau:

- FIFO (First In First Out).

- CQ (Custom Queuing).

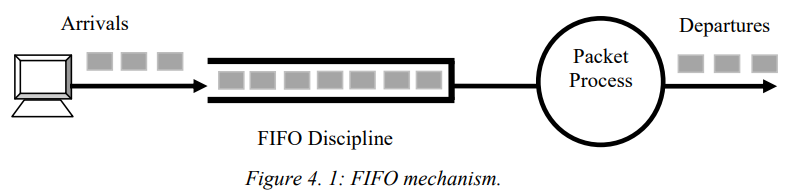
- PQ (Priority Queuing).

- WFQ (Weighted Fair Queuing).

Cơ chế phân phối lưu lượng ra là một thành phần quan trọng của các dịch vụ tích hợp kiến trúc tại các bộ định tuyến. Tồn tại nhiều cơ chế lập lịch để đạt được chất lượng dịch vụ. Tất cả những điều này đều có một số ưu điểm và nhược điểm. Mặc định cơ chế được thực hiện trong internet ngày nay là FIFO hoặc mô hình đến trước phục vụ trước.

### **3.2.1. Nhập trước xuất trước (FIFO)**

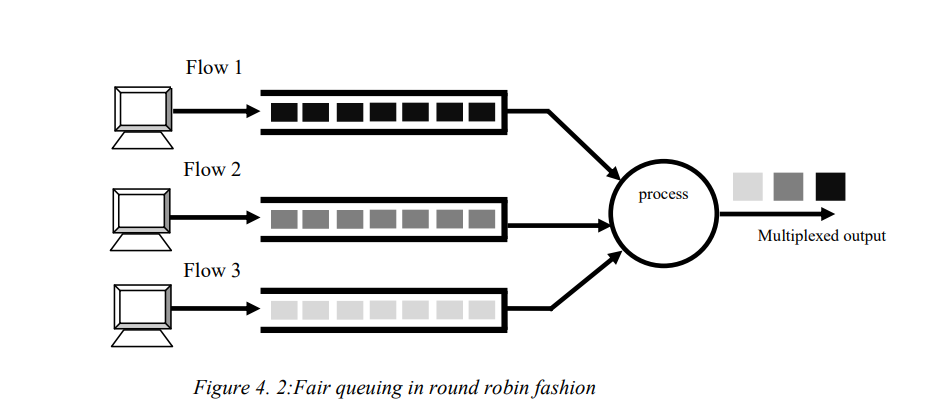
Trong mạng Internet truyền thống, bộ định tuyến sử dụng phương pháp xếp hàng đầu tiên - còn gọi là "ai đến trước, phục vụ trước" tại mỗi cổng đầu ra. Tại hàng đợi đầu ra, các gói tin phải chờ đợi để được truyền nếu liên kết hiện đang bận truyền gói tin khác, và nếu không còn chỗ để chứa gói tin đến, thì gói tin mới sẽ bị loại bỏ một cách đơn giản. Các chính sách loại bỏ gói tin của cơ chế xếp hàng này thực hiện công việc loại bỏ các gói tin không thể xử lý. Hệ thống xếp hàng FIFO chọn các gói tin cho hàng đợi đầu ra và truyền chúng theo thứ tự chính xác mà chúng đến hàng đợi đầu ra.



Hình 3.3. Cơ chế FIFO

### **3.2.2. Xếp hàng công bằng (FQ)**

Để khắc phục những hạn chế của cơ chế FIFO, cơ chế xếp hàng công bằng đã được đề xuất. Trong cơ chế FIFO truyền thống, chỉ có một hàng đợi duy nhất được sử dụng cho toàn bộ lưu lượng truy cập từ tất cả các nguồn khác nhau. Điều này có nghĩa là nếu có ba nguồn lưu lượng truy cập khác nhau muốn truy cập vào mạng thông qua một cổng duy nhất, tất cả các lưu lượng truy cập này phải chia sẻ một hàng đợi chung. Ngược lại, trong cơ chế xếp hàng công bằng, mỗi nguồn lưu lượng truy cập riêng biệt được gán một hàng đợi riêng. Trong cơ chế này, các gói tin từ mỗi nguồn lưu lượng truy cập được xếp vào một hàng đợi cụ thể, và sau đó tất cả các hàng đợi này được phục vụ theo kiểu vòng tròn, nghĩa là mỗi lần lấy một gói tin từ mỗi hàng đợi lần lượt theo chu kỳ cố định. Cơ chế này còn được gọi là cơ chế cân bằng tải, vì nó giúp cân bằng tải lưu lượng truy cập giữa các nguồn lưu lượng truy cập khác nhau.



Hình 3.4. Xếp hàng công bằng theo kiểu vòng tròn

### **3.2.3. Xếp hàng công bằng vòng tròn bit (BRFQ)**

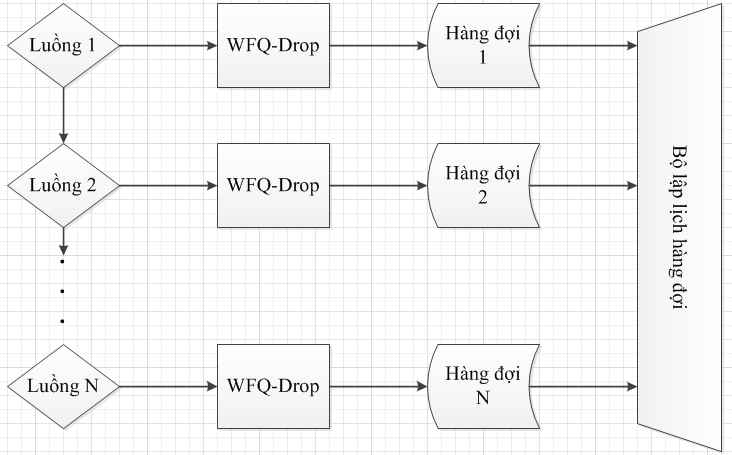
Vấn đề phân phối băng thông không đồng đều trong xếp hàng công bằng được giải quyết trong bit xếp hàng công bằng vòng tròn. Trong cơ chế này, thay vì truyền một gói mỗi vòng, một bit từ mỗi gói được thông qua ở mỗi vòng. Bằng cách này, vấn đề không bằng phân phối băng thông được giải quyết và do đó, các gói dài hơn sẽ không có lợi thế dung lượng băng thông trên các gói nhỏ hơn. Trong cơ chế này, nếu giả sử có N tổng số băng thông, sau đó mỗi hàng đợi trong trường hợp này sẽ nhận được 1 / N trong tổng số băng thông. Cách tiếp cận này còn được gọi là chia sẻ bộ xử lý.

Bảng 3.2. Nhược điểm trong có chế lập kế hoạch

|  |  |
| --- | --- |
| Cơ chế | Nhược điểm |
| FIFO | - Hạn chế chính trong cơ chế này là loại bỏ gói.  - Bình đẳng với các gói thông thường mà không có ưu tiên.  - Nhạy cảm với thời gian.  - Đỗ trễ (các gói lớn hơn nhận được dịch vụ tốt hơn các gói nhỏ hơn). |
| FQ | - Không thể phân biệt giữa các gói có mức độ ưu tiên cao hơn và ưu tiên thấp hơn. Tất cả các gói được phục vụ như nhau trong một thời gian vòng tròn.  - Một nhược điểm nghiêm trọng khác trong việc xếp hàng công bằng là không bình đẳng phân phối tài nguyên băng thông.  - Sự cố rớt gói giống như FIFO. |
| BRFQ | - Vấn đề phân phối băng thông không đồng đều nhưng vấn đề làm thế nào để đạt được chất lượng dịch vụ theo mức độ ưu tiên không được giải quyết trong cơ chế này.  - Sư cố rơi gói giống như trong FIFO. |

### **3.2.4. Xếp hàng công bằng có trọng số (WFQ)**

Cơ chế này giới thiệu cơ chế chia sẻ bộ xử lý tổng quát (GPS) qua chia sẻ bộ xử lý (PS) như trong xếp hàng công bằng vòng bit. Trong cơ chế này, cá nhân các gói được truyền thay vì các bit riêng lẻ từ mỗi hàng đợi ở mỗi vòng như trong xếp hàng công bằng nhưng trong cơ chế này; mỗi loại lưu lượng nhận được một lượng khác nhau của dịch vụ trong bất kỳ khoảng thời gian nào. Đặc biệt hơn để phân phối băng thông đồng đều dung lượng trong số tất cả các hàng đợi, mỗi lớp được ấn định một trọng số cụ thể. Dưới xếp hàng công bằng có trọng số, giả sử một lớp tôi sẽ được cấp Wi có trọng lượng sẽ bằng sang Wi / ΣWj. trong đó ΣWj là tổng trọng lượng của tất cả các hàng đợi trong kịch bản đó.



Hình 3.5. Cơ chế hoạt động của hàng đợi WFQ

WFQ tự động phân loại các gói tin dựa trên thông tin về dòng lưu lượng, trong đó từng dòng sẽ được đặt trong một hàng đợi riêng lẽ. Một dòng lưu lượng được định nghĩa bao gồm tất cả các gói tin có cùng thông số.

### **3.2.5. Chất lượng dịch vụ hỗ trợ trong WFQ**

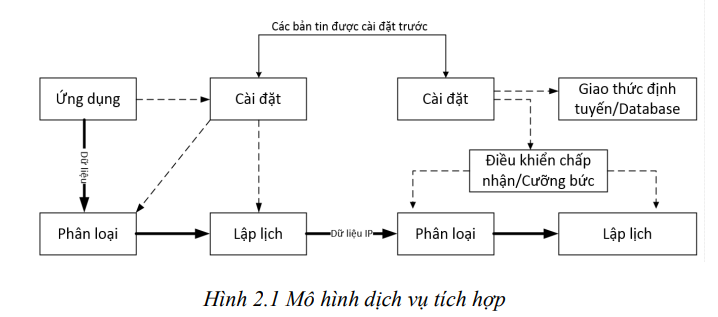
Xếp hàng hợp lý có trọng số cung cấp chất lượng dịch vụ đồng nhất và phù hợp để lưu lượng mạng. Giả sử có một liên kết với tốc độ 1 và tốc độ đảm bảo cho truyền trên liên kết 1 là 0,5 và giả sử tỷ lệ đảm bảo cho 9 liên kết khác là 0,05. Nó là cho rằng luồng 1 trên liên kết 1 gửi 10 gói và tất cả 9 luồng khác gửi một gói tại thời điểm 0. Theo cơ chế FIFO, mỗi gói sẽ được truyền từ mỗi luồng nhưng trong xếp hàng công bằng có trọng số, tất cả 10 gói của luồng 1 sẽ được truyền tại thời điểm 0 và sau đó tất cả 9 luồng khác sẽ truyền một gói tại thời điểm 0. Điều này là do phân bố trọng lượng bằng nhau giữa tất cả các dòng chảy. Xếp hàng có trọng lượng đóng vai trò trung tâm vai trò trong việc đạt được chất lượng dịch vụ có sẵn trong các sản phẩm bộ định tuyến ngày nay.

## **3.3. Mô hình đảm bảo chất lượng dịch vụ**

Để đảm bảo QoS cho mạng IP, IETF đã thống nhất đưa ra hai mô hình chính: Mô hình dịch vụ tích hợp IntServ và mô hình dịch vụ phân biệt DiffServ. IntServ hướng theo mô hình báo hiệu QoS (signaled-QoS), theo đó thiết bị đầu cuối cần truyền phát tín hiệu yêu cầu QoS đến thiết bị nhận, tín hiệu này sẽ đi qua các thiết bị trung gian đến thiết bị nhận. Mô hình DiffServ làm việc theo kiểu cung cấp các mức độ QoS dự kiến có được (provisionedQoS), theo mô hình này những nhân tố mạng được thiết lập để cho lưu lượng thuộc nhiều lớp dịch vụ khác nhau đi qua và có thể đạt được QoS dự kiến, trong điều kiện thuận lợi.

### **3.3.1. Mô hình IntServ (Intergrated Services)**

Ý tưởng ban đầu của mô hình dịch vụ tích hợp là hỗ trợ việc dành trước tài nguyên cho các luồng lưu lượng. Để thực hiện được cần thiết lập một tuyến dành trước tài nguyên, trước khi gửi dữ liệu, các bộ định tuyến và thiết bị mạng phải được cài đặt chức năng ưu tiên dành tài nguyên và bộ định tuyến cần phải điều khiển được các luồng lưu lượng.



Hình 3.6. Mô hình dịch vụ tích hợp

Mô hình tích hợp dịch vụ IntServ mô tả ứng dụng QoS trong mạng IP theo phương pháp nhận dạng luồng lưu lượng với năm tham số cơ bản sau:

* Địa chỉ IP nguồn
* Cổng nguồn
* Địa chỉ IP đích
* Cổng đích
* Giao thức truyền.

Để dự trữ tài nguyên cho một luồng lưu lượng, ứng dụng luồng cần phải cung cấp các đặc tính luồng. Đặc tính luồng gồm các đặc tính lưu lượng và yêu cầu chất lượng dịch vụ cho luồng đó.

Đặc tính lưu lượng bao gồm tốc độ đỉnh, tốc độ trung bình, kích thước lưu lượng bùng nổ và một số tham số khác. Yêu cầu chất lượng dịch vụ bao gồm băng thông tối thiểu, độ lớn lưu lượng bùng nổ cho phép truyền được và các yêu cầu hiệu năng như trễ, biến thiên trễ và tỷ lệ mất gói.

Mạng theo mô hình IntServ cung cấp cho dịch vụ truyền sự đảm bảo nghiêm ngặt về độ trễ giữa các đầu cuối và bảo đảm băng thông phù hợp với các thông số đặc biệt. Để làm được điều này, IntServ thực hiện cơ chế dành trước tài nguyên. Ứng dụng phải đặc tính hóa luồng lưu lượng và tổng hợp trong chỉ tiêu luồng lưu lượng. Sau đó, ứng dụng gửi yêu cầu thiết lập dự trữ tài nguyên đến mạng và các nút mạng dọc theo tuyến đường từ nút mạng có ứng dụng gửi đến nút mạng có ứng dụng nhận phải đưa vào bảng dự phòng tài nguyên nếu mạng có cam kết dự phòng. Tài nguyên dành trước cần phải qua tất cả các nút trên đường đi và thiết lập các dự phòng. Mỗi nút cần quyết định có chấp nhận việc dành trước hay không, nhận dạng luồng ra sao và lập lịch gói tin như thế nào. Khi gói tin đến, hệ thống nhận dạng gói tin thuộc về luồng đặt trước và đặt gói tin đó vào hàng đợi ưu tiên.

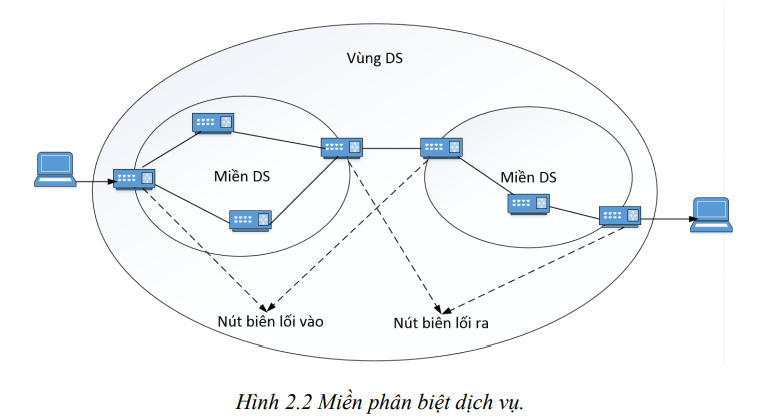
* Điều kiện chấp nhận: Việc dành trước tài nguyên cho yêu cầu mới sẽ bị từ chối nếu nút không có sẵn tài nguyên. Ưu điểm của việc dựa theo đo đạc là tối ưu hóa việc sử dụng tài nguyên mạng, mặc dù không đảm bảo chặt chẽ các cam kết tài nguyên.
* Nhận dạng luồng: Giao thức dành trước tài nguyên RSVP (Resource Reservation Protocol) sử dụng năm tham số trong gói tin để nhận dạng gói tin thuộc về các luồng dành trước tài nguyên trong nút.
* Lập lịch gói tin: Đây là bước cuối cùng trong RSVP. Bộ lập lịch thực hiện việc cấp phát tài nguyên. Nó quyết định gói tin nào gửi tiếp khi đường đi đã sẵn sàng.

### **3.3.2. Mô hình và kiến trúc DiffServ (Differentiated Services)**

Nhóm IETF đã đề xuất mô hình DiffServ như một giải pháp đảm bảo chất lượng có tính khả thi và ứng dụng cao. Mô hình DiffServ thừa nhận một khía cạnh trái ngược với IntServ. Vấn đề tồn tại của IntServ là các nguồn tài nguyên cần phải được duy trì trạng thái thông tin theo từng luồng, điều này trở nên khó triển khai với mạng có số lượng dịch vụ và số lượng thiết bị mạng lớn vì bộ định tuyến cần phải xử lý lưu lượng rất lớn trong mạng. Còn giải pháp DiffServ không xử lý theo từng luồng riêng biệt mà ghép các luồng lại với nhau thành từng nhóm luồng có độ ưu tiên khác nhau. Mô hình DiffServ hướng tới xử lý trong từng dịch vụ phân biệt thay vì việc xử lý các luồng từ nguồn tới đích như mô hình IntServ. Trong mô hình DiffServ, các bộ định tuyến được chia làm hai thành phần chính là:

Thứ nhất, thành phần mạng biên: Nhiệm vụ chính là phân loại gói tin và điều khiển lưu lượng truyền. Tại vị trí biên được đánh dấu, cụ thể là trường DS trong tiêu đề gói tin được thiết lập một giá trị nào đó gọi là CP.

Thứ hai là hành phần mạng lõi: đóng vai trò chuyển tiếp. Khi một gói tin được đánh dấu giá trị CP ở một router có hỗ trợ DiffServ, gói tin chuyển tới chặng tiếp thông qua chính sách của từng chặng. Hành vi chuyển tiếp theo từng chặng – PHB (Per-hop Behavior) thực hiện tại các bộ định tuyến lõi bởi cách xếp hàng và quản lý điểm tắc nghẽn. Vì thế, bằng cách ánh xạ lưu lượng đến PHB khác nhau, bộ định tuyến có thể đảm bảo chất lượng dịch vụ mạng.

**

Hình 3.7. Miền phân biệt dịch vụ

Một miền DS gồm các bộ định tuyến hỗ trợ cơ chế phân biệt dịch vụ. Vùng DS là tập hợp một hay vài miền DS kế tiếp nhau. Vùng này có khả năng hỗ trợ các miền DS, các miền trong vùng có thể hỗ trợ nội bộ cho các nhóm PHB khác nhau và các điểm mã khác nhau để sắp xếp PHB.

### **3.3.3. Các phương pháp xử lý gói trong DiffServ**

Nhóm làm việc về DiffServ của IETF định nghĩa hai loại PHB trong RFC 2598, RFC 3246 và RFC 2596: Thứ nhất là chuyển tiếp nhanh EF (Expedited Forwarding) và thứ hai là chuyển tiếp đảm bảo AF (Assured Forwarding).

* Chuyển tiếp nhanh EF PHB: đảm bảo tính năng về tốc độ hơn là độ tin cậy. Nó được ứng dụng cho các dịch vụ yêu cầu độ trễ, biến động trễ thấp đảm bảo băng thông. Biến động trễ và trễ chủ yếu gây nên bởi thời gian mà gói phải nằm chờ trong bộ nhớ đệm (hàng đợi).
* Chuyển tiếp đảm bảo AF PHB: Chuyển tiếp các gói dữ liệu với sự đảm bảo tỷ lệ mất gói thấp. AF PHB gồm 4 lớp chuyển tiếp và mỗi lớp có ba mức ưu tiên loại bỏ gói tin, mỗi lớp được gán một băng thông và vùng nhớ đệm nhỏ. Nếu bộ nhớ đệm đầy thì quá trình loại bỏ gói sẽ bắt đầu theo trật tự ưu tiên loại bỏ. Chi tiết phân loại AF và việc gán mã DSCP được thể hiện trong bảng dưới đây:
* PHB và thỏa thuận lớp lưu lượng PHB được xác định theo giới hạn tài nguyên của các router lõi, có quan hệ ưu tiên với các PHB khác. PHB được coi như khối sẵn có để cấp phát tài nguyên, chúng chia sẻ chính sách áp dụng cho nhau trong phạm vi nhóm như lập lịch, quản lý bộ đệm.

Bảng 3.3. Chi tiết phân lớp chuyển tiếp đảm bảo AF PH

|  |  |  |  |
| --- | --- | --- | --- |
| **Lớp PBHB** | **Phân lớp** | **Dự đoán mất gói** | **DSCP** |
| AF4 | AF41 | Thấp | 100010 |
| AF42 | Trung bình | 100100 |
| AF43 | Cao | 100110 |
| AF3 | AF31 | Thấp | 011010 |
| AF32 | Trung bình | 011100 |
| AF33 | Cao | 100010 |
| AF2 | AF21 | Thấp | 010010 |
| AF22 | Trung bình | 010100 |
| AF23 | Cao | 010110 |
| AF1 | AF11 | Thấp | 001010 |
| AF12 | Trung bình | 001100 |
| AF13 | Cao | 001110 |

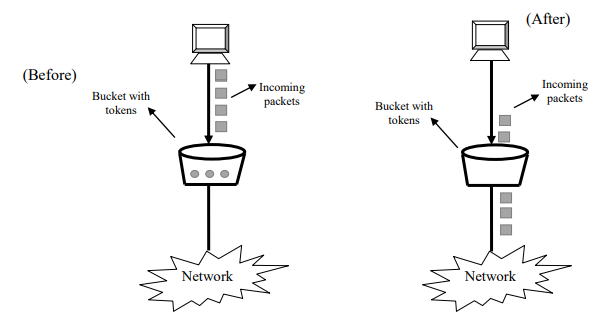
## **3.4. Giải pháp tối ưu lưu lượng trong mạng**

### **3.4.1. Bắt giữ và đánh dấu gói tin**

Mỗi lớp lưu lượng đều có các hạn chế về cách xử lý trước khi nhập vào mạng, bao gồm việc giới hạn tốc độ truyền của các gói tin và quy định số lượng gói tin tối đa được phép vào trong khoảng thời gian nhất định (thường được gọi là Profile). Quá trình bắt giữ và đánh dấu tương tự như những hoạt động diễn ra trong bộ định tuyến khi quyết định xem một gói tin vượt qua giới hạn cụ thể đã định cho mỗi luồng lưu lượng (còn gọi là out profile) sẽ bị loại bỏ hay không. Trong trường hợp bắt giữ, các gói tin vượt quá giới hạn sẽ bị loại bỏ khỏi lưu lượng. Còn trong trường hợp đánh dấu, một hoặc một vài bit trong phần header của các gói tin bị chỉnh sửa và sau đó chúng sẽ được đánh dấu và chuyển đến hàng đợi đầu ra của bộ định tuyến, sau đó đến tầng lập lịch. Các chức năng tương tự này còn được gọi là chức năng định dạng lưu lượng, và chúng sẽ sửa đổi một số đặc điểm tạm thời của lưu lượng bằng cách lựa chọn và chuyển tiếp các gói tin nội bộ với độ trễ cụ thể.

### **3.4.2. Hoạt động của chức năng bắt giữ và đánh dấu**

Bắt giữ và đánh dấu chia sẻ thành phần chung đó là bộ đo. Chức năng đo đạc để quyết định xem gói nằm trong profile (in profile) hay nằm ngoài profile (out profile). Một ví dụ là sử dụng bộ đo thẻ token packet cho phép một mức độ nhỏ các bó bên trong một lớp lưu lượng điển hình. Các thẻ được đưa vào gáo tại tốc độ cố định X (số thẻ /s) và sẽ bị loại bỏ ra khỏi gói khi gói đến. Kích thước của gáo là giới hạn, gáo có kích thước là Y thẻ.



Hình 3.8. Chức năng đo đơn giản của Token Packet

Khi một gói đến trong một gáo, và trong gáo có ít nhất một thẻ tồn tại thì thẻ đó được gán cho gói (thẻ được gỡ bỏ) và gói được xem như in profile. Nếu không có thẻ nào trong gói thì gói được coi là out profile. Thẻ sẽ được bổ sung với tốc độ X thể hiện tốc độ trung bình dài hạn nếu các gói được duy trì trong profile. Tuy nhiên các gói có thể đến dưới dạng các bó ngắn và vẫn được xem như ở trong profile cho tới khi gáo đạt được Y thẻ. Nếu gói đến với tốc độ R nhỏ hơn X thì gáo sẽ điền thêm (X - R) thẻ trên một giây, và sẽ dừng lại khi nó đạt được Y thẻ. Nếu gói đến với tốc độ R= X thì số thẻ trong gáo không đổi. Khi tốc độ R > X thì thẻ ra khỏi gáo với tốc độ R- X. Chỉ cần trong gáo còn ít nhất một thẻ thì gói vẫn được xem như trong Profile. Nếu R quá lớn hơn so với X, gáo rỗng thì các gói đến lần lượt sẽ được xem như nằm ngoài profile. Trạng thái out profile sẽ tiếp diễn cho tới khi R giảm xuống nhỏ hơn X (tại điểm này gáo lại bắt đầu được điền đầy và thoát khỏi trạng thái rỗng). Một token packet có thể được xem như điều luật bắt buộc để điều khiển tốc độ của các gói đến: số lượng các gói đến một điểm đo tại chu kì T phải nhỏ hơn (T X Y).

Có thể có nhiều token packet cùng hoạt động đồng thời để đo các gói đến. Lúc này ta phải sử dụng profile xếp lớp cho các gói đến. Các trường hợp có thể xảy ra khi các gói đến:

* Nếu trong các gáo có tồn tại các thẻ thì tất cả các gói đến đều là in profile tại mỗi gói thẻ sẽ được rút ra và gói được truyền bình thường.
* Nếu một gáo không có thẻ, nhưng các gáo khác vẫn có thẻ thì gói đi vào gáo không thẻ có thể bị bắt giữ, còn các gói đến các gáo có thẻ thì chỉ bị đánh dấu trước khi truyền gói thông thường.
* Nếu tất cả các gáo đều rỗng thì các gói bị loại bỏ (bắt giữ).

Tuy nhiên các router sẽ đối xử các gói bị đánh dấu như các gói loại hai khi có tắc nghẽn xảy ra trong mạng. Có hai cách đối xử với các gói bị đánh dấu này: cách thứ nhất đánh giá thấp độ ưu tiên của gói bằng cách ấn định chúng vào các hàng đợi khác nhau trên quá trình đánh dấu. Cách thứ 2 hoán vị thuật toán quản lý hàng đợi để giữ cho độ chiếm giữ hàng đợi thấp. Cách thứ nhất thường gây ra hiện tượng sắp xếp lại trong hàng đợi của cùng một lớp lưu lượng, hầu hết các giao thức đầu cuối trong mạng TCP không xử lý hiệu quả được hiện tượng này nên cách tốt nhất là sử dụng quản lý hàng đợi tích cực để quản lý các gói đi vào trong hàng đợi. RED là một thuật toán quản lý hàng đợi tích cực cho phép quản lý hiệu quả quá trình các gói đi vào trong hàng đợi.

### **3.4.3. Giảm chiếm giữ hàng đợi**

Hiện tượng chiếm giữ hàng đợi xảy ra khi các gói tin dài hạn trong hàng đợi chưa được xử lý. Việc này làm thu hẹp không gian trong hàng đợi, và khi nhiều gói tin khác đến, chúng có thể không được đưa vào hàng đợi và có thể bị loại bỏ trong trường hợp có tắc nghẽn. Mức độ chiếm giữ hàng đợi tăng lên khi tải cung cấp (tốc độ lưu lượng đến) vượt quá tốc độ xử lý gói tin ra khỏi hàng đợi bởi bộ lập lịch. Tốc độ xử lý hàng đợi ra ngoài phụ thuộc nhiều vào cách bộ lập lịch tương tác với luồng lưu lượng, đặc biệt là từ các hàng đợi khác để truy nhập đầu ra. Mức độ chiếm giữ có thể xem như tác động của các tình huống tắc nghẽn hiện tại lên giao diện đầu ra của hàng đợi.

Để giảm tắc nghẽn, chúng ta áp dụng một số phương pháp trong các giao thức truyền tải, được kích hoạt khi luồng lưu lượng đi qua hàng đợi. Bởi vì tắc nghẽn xảy ra trước khi bất kỳ giao thức truyền tải nào có cơ hội tác động lên router, quản lý hàng đợi xem xét hai khái niệm cơ bản về tắc nghẽn:

Tắc nghẽn trong suốt: xảy ra với chu kì ngắn hơn là thời gian xử lý của các giao thức điều khiển tắc nghẽn. Tắc nghẽn này xảy ra ngắn, liên quan tới các lưu lượng dạng bó từ một hoặc nhiều luồng. Nhìn chung router không muốn loại bỏ các gói từ một bó lưu lượng do đó phải thiết kế được hàng đợi có kích thước sao cho nó có thể bao trùm được kích thước của các bó lưu lượng. Điều này rất khó thực hiện được do kích thước bó lưu lượng thay đổi theo từng luồng lưu lượng đến do đó chỉ có cách là quản lý động kích thước hàng đợi phù hợp với kích thước của bó lưu lượng. Khi kích thước bó lưu lượng lớn thì kích thước hàng đợi trung bình tăng, còn khi lưu lượng đến dưới dạng bó nhỏ thì kích thước hàng đợi trung bình giảm.

Tắc nghẽn dài hạn: là kết quả từ tốc độ trạng thái không đổi của tất cả các luồng khi chuyển qua hàng đợi. Khi có tắc nghẽn trong mạng thì quản lý hàng đợi sẽ sử dụng cơ chế phản hồi cho các giao thức truyền tải để giữ cho trễ dài hạn giảm. Về nguyên lý có thể gửi phản hồi theo hai cách: đánh dấu các gói trong nhóm và loại bỏ các gói.

Mặc dù loại bỏ các gói là cách phù hợp với cơ chế phản hồi, nhưng cách này không tích cực do việc loại bỏ các gói sẽ gây ra lãng phí tài nguyên mạng sử dụng để truyền được gói đến router trước khi nhận thấy có tắc nghẽn. Do đó sử dụng chỉ thị tắc nghẽn để tránh lãng phí tài nguyên. Một cách thức được sử dụng là thông báo tắc nghẽn rõ ràng (ECN). Hai bit không được sử dụng CU trong trường DS được chỉ thị như các bít truyền tải theo ECN (ECT) và bit thể hiện tắc nghẽn (CE). Phía gửi giao thức truyền tải sẽ thiết lập bit ECT tại biên giới ngoài của các gói tin khi đó phần kết thúc một luồng hiểu được 39 bit CE. Khi không có yêu cầu phản hồi điều khiển tắc nghẽn, bit CE bị từ chối. Khi một router dọc theo tuyến muốn gửi phản hồi điều khiển tắc nghẽn thì có hai tuỳ chọn sau:

* Nếu bit ECT được thiết lập, thì thiết lập bit CE.
* Nếu bit ECT được thiết lập lại thì loại bỏ các gói.

Trước khi quyết định loại gói phải đặt ra câu hỏi nên loại bỏ gói để đơn giản việc quản lý và không ảnh hưởng nhiều đến các gói khác trong hàng đợi. Từ vấn đề trên thấy đơn giản nhất là loại bỏ gói ngay trước khi đi vào hàng đợi (gọi là loại bỏ đuôi). Có một cách tương tự trên là loại bỏ trước (DFF), loại bỏ ngay tại đầu hàng đợi. Đôi khi loại bỏ trước được thông báo sớm hơn loại bỏ đuôi tuy nhiên nó mất thời gian và công đoạn xử lý hơn do các gói đã được đưa vào hàng đợi rồi mới bị loại bỏ.

## **3.5. Khả năng liên kết và bảo mật truyền dẫn trong mạng**

❖ Khả năng liên kết

Dung lượng kênh hoặc khả năng liên kết kênh là số lượng tin nhắn trên mỗi đơn vị thời gian được xử lý bởi liên kết. Nó thường được đo bằng mỗi bật trên giây. Một trong những kết quả nổi tiếng nhất trong tất cả lý thuyết thông tin là định lý mã hóa kênh Shannon. Đối với một kênh nhất định ở đó tồn tại một mã sẽ cho phép truyền không có lỗi trên kênh ở tốc độ R, cung cấp , tại đó C là dung lượng kênh. Đẳng thức đạt được chỉ khi tỷ lệ tín hiệu trên tạp âm (SNR) đang ở mức thấp.

❖ Bảo mật chất lượng truyền dẫn trong mạng cục bộ

Trong ngành thiết kế mạng, sự quan tâm đặc biệt thường được dành cho các khung dữ liệu lớn, bởi vì chúng có khả năng làm tăng áp lực lên bộ đệm và gây ra tắc nghẽn nhanh hơn so với các khung nhỏ hơn. Điều này có thể dẫn đến việc mất mát khung dữ liệu và cần phải truyền lại dữ liệu (data retransmission). Mặc dù độ trễ trong việc xử lý các khung dữ liệu lớn có thể tương tự như trong trường hợp của các khung nhỏ hơn, điều quan trọng là các gói tin lớn thường hiệu quả hơn, vì các thiết bị định tuyến và chuyển mạch có thể xử lý chúng nhanh chóng trong các hàng đợi liên quan.

Khung dữ liệu lớn cũng có thể trở thành mục tiêu cho việc phân mảnh, trong đó chúng được chia thành các đơn vị nhỏ hơn để phù hợp với Maximum Transmission Unit (MTU). MTU là một tham số quy định kích thước tối đa của datagram có thể được truyền qua một giao diện IP. Mặt khác, việc sử dụng các khung dữ liệu nhỏ hơn có thể dẫn đến nhiều xung đột hơn trong mạng Ethernet hoặc giảm hiệu suất trên các liên kết WAN.

❖ An toàn thông tin bao gồm các nội dung

* Tính bí mật: tính kín đáo riêng tư của thông tin
* Tính xác thực của thông tin, bao gồm xác thực đối tác (bài toán nhận danh), xác thực thông tin trao đổi.
* Tính trách nhiệm đảm bảo người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình đã gửi.

Để đảm bảo an toàn thông tin dữ liệu trên đường truyền tin và trên mạng máy tính có hiệu quả thì điều trước tiên là phải lường trước hoặc dự đoán trước các khả năng 40 không an toàn, khả năng xâm phạm, các sự cố rủi ro có thể xảy ra đối với thông tin dữ liệu được lưu trữ và trao đổi trên đường truyền tin.

❖ Bảo mật truyền dữ liệu

Về cơ bản dựa trên kỹ thuật bảo mật ta có thể quy chiếu công tác bảo mật thông tin thành hai nhóm: bảo mật thông tin dữ liệu bằng các biện pháp kỹ thuật phần cứng và phần mềm thông qua các thuật toán bảo mật. Tuy nhiên để đảm bảo an toàn dữ liệu trên đường truyền mạng máy tính có hiệu quả nhằm chống các khả năng xâm phạm và các rui ro hay sự cố có thể xảy ra trong quá trình truyền tin thì việc phòng chống và xác định chính xác các nguy cơ có thể làm ảnh hưởng đến dữ liệu là vô cùng quan trọng. Trên thực tế có hai hình thức gây hại chính cho dữ liệu truyền tin là hình thức chủ động (active) và thụ động (passive). Hai hình thức này hướng đến:

***Đánh cắp thông tin:*** Lắng nghe thông tin trên đường truyền, biết được thông tin về người gửi và nhận nhờ vào thông tin được chứa trong gói tin truyền trên hệ thống mạng. Hình thức này, kẻ xâm nhập có thể kiểm tra được tần số trao đổi, số lượng gói tin truyền đi và độ dài của gói tin này.

Tuy nhiên, với hành động trên, thông thường với mục đích xem thông tin, Sao chép, đánh cắp nội dung thông tin (ví dụ như mật khẩu, thông tin về ngân hàng...) chứ không làm ảnh hưởng nguy hại về mật vật lý đối với dữ liệu hay làm sai lệch nội dung dữ liệu.

***Phá hoại thông tin*:** Thay đổi nội dung dữ liệu, chèn thêm thông tin dữ liệu, phá hủy làm hỏng các gói tin, làm trễ thời gian truyền tin, Sao chép lặp đi lặp lại dữ liệu... với mục đích phá hỏng hay làm sai lệch nội dung thông tin. Để bảo vệ thông tin dữ liệu trên đường truyền, ở bài báo này tôi trình bày hướng đến hai thình thức bảo mật:

Bảo mật hướng theo đường truyền (Link Oriented Security): Thông tin được mã hóa để bảo vệ dựa trên đường truyền giữa hai nút và không quan tâm đến nguồn và đích của thông tin đó. Các cặp thiết bị mật mã được đặt ở hai đầu của đường truyền. Do đó tất cả luồng thông tin trên tất cả các đường truyền sẽ được an toàn.

Bảo mật dựa trên hai điểm đầu và cuối (End to End Security): Mã hóa đường truyền từ máy tính nguồn đến máy tính đích. Thông tin được mã hóa ngay khi mới được tạo ra tại máy nguồn và chỉ được giải mã khi tới máy đích.

## **3.6. Kết luận chương 3**

Để đánh giá được chất lượng truyền dẫn đường truyền mạng thì cần dựa vào yếu tố xuất hiện và ảnh hưởng đến hoạt động của nó. Chất lượng truyền dẫn hoạt động sẽ có sự tác động của các yếu tố như độ trễ, băng thông, an toàn bảo mật thông tin. Mỗi một yếu tố ảnh hưởng đến chất lượng truyền dẫn khi xuất hiện giá trị của nó sẽ phần nào đánh giá được chất lượng lưu lượng truyền dẫn trong mạng.

Mỗi một giải pháp đánh giá truyền dẫn sẽ chỉ ra một mặt ảnh hưởng trực tiếp đến đường truyền mạng. Trên đường truyền dẫn có những yếu tố điển hình như băng thông hay độ đụng gói tin sẽ làm đường truyền bị tức bị trễ gói phía nhận, khiến cho việc truyền dẫn gặp nhiều khó khăn. Vậy để có cái nhìn rõ ràng hơn về các yếu tố đánh giá chất lượng truyền dẫn của mạng ta sẽ đi vào mô phỏng ở chương tiếp theo để mọi người thấy được phương thức hoạt động của lưu lượng mạng, cách thiết lập mô hình và những yếu tố như trên ảnh hưởng như thế nào đến chất lượng truyền dẫn đường truyền mạng.

# CHƯƠNG 4. XÂY DỰNG BÀI TOÁN MÔ PHỎNG QOS TRÊN MẠNG IP

## **4.1. Xây dựng kịch bản mô phỏng**

**❖ Xây dựng kịch bản mô phỏng:**

Mô phỏng mạng kết hợp (hybrid) các cấu trúc liên kết này có thể bao gồm hỗn hợp cấu trúc liên kết bus, cấu trúc liên kết lưới, cấu trúc liên kết vòng, cấu trúc liên kết hình sao và cấu trúc liên kết hình cây. Cấu trúc liên kết lai vòng sao là sự kết hợp của cấu trúc liên kết hình sao và cấu trúc liên kết vòng. Hai hoặc nhiều cấu trúc liên kết hình sao được kết nối với nhau thông qua cấu trúc liên kết vòng. Mô phỏng với quy mô trong một công ty vừa và nhỏ với cơ chế sử dụng các dịch vụ dữ liệu thoại, video, và FTP cụ thể như sau:

**Voice IP:** là phương thức thực hiện và nhận cuộc gọi điện thoại qua Internet. VoIP chuyển đổi tín hiệu thoại được sử dụng trong công nghệ điện thoại truyền thống thành tín hiệu kỹ thuật số truyền qua Internet thay vì qua đường dây điện thoại tương tự.

**Video Conferencing:** Video conferencing, hay còn gọi là hội nghị truyền hình là một hình thức trao đổi thông tin trực tiếp giữa các thành viên ở xa nhau (có thể là từ phòng này đến phòng khác trong một tòa nhà, hay là từ quốc gia này đến quốc gia khác). Bạn chỉ cần ngồi tại văn phòng mà vẫn có thể đối thoại trực tiếp với các đối tác hoặc chi nhánh ở xa.

**FTP:** Viết tắt từ File Transfer Protocol, là một giao thức truyền tải tập tin từ máy tính này đến máy tính khác thông qua một mạng TCP hoặc qua mạng Internet. Nhờ vào giao thức này nên người sử dụng có thể tải dữ liệu như hình ảnh, văn bản, các tập tin nhạc, video... từ máy tính của mình lên máy chủ đang đặt ở một nơi khác hoặc tải các tập tin đã có trên máy chủ về máy tính cá nhân của mình một cách dễ dàng. FTP cũng là giao thức dùng để truyền tải dữ liệu web lên máy chủ web cho dù máy chủ đặt rất xa.

**❖ Phần mềm mô phỏng**

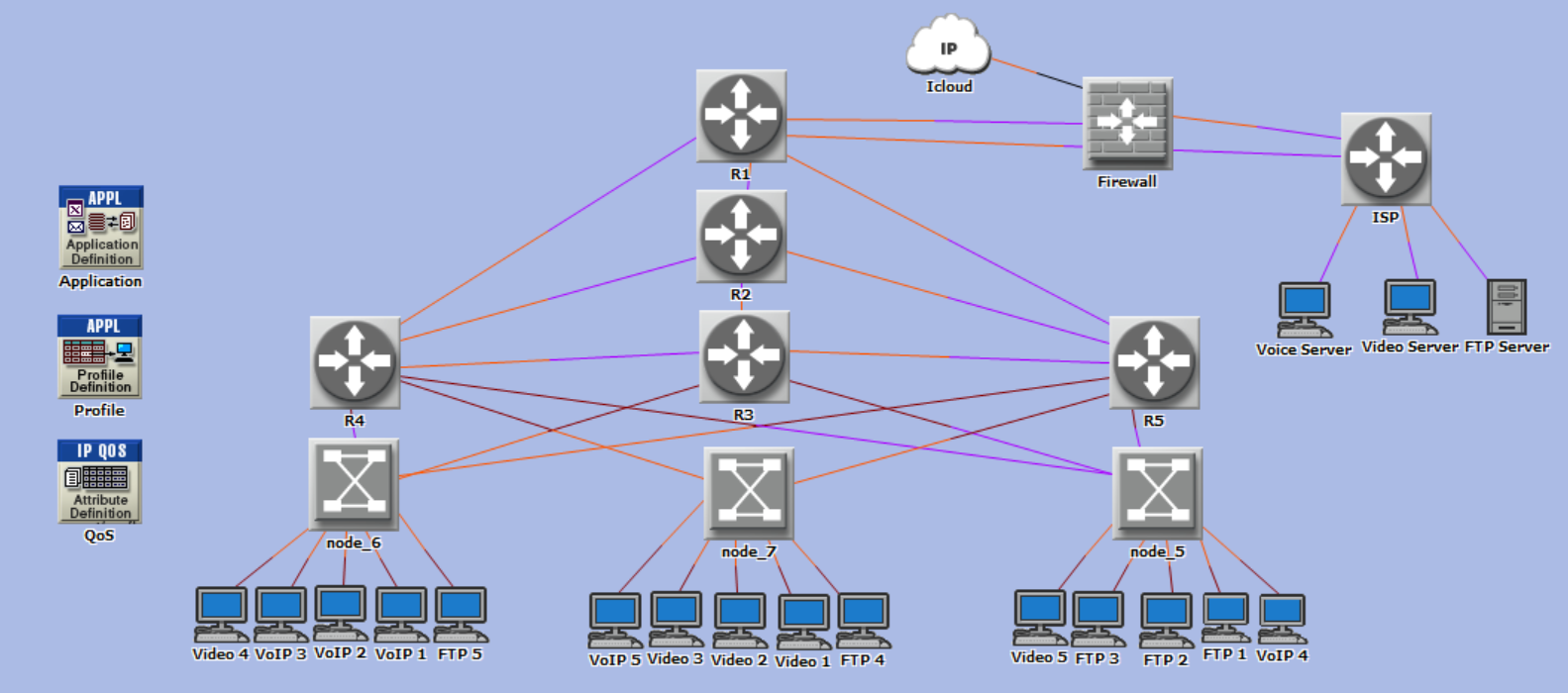
Sử dụng phần mềm mô phỏng: để mô phỏng lưu lượng truyền dẫn trong mạng, để đánh giá theo các tiêu chí trên: độ trễ, lưu lượng truy cập giảm, thời gian phản hồi, lưu lượng gửi đi, lưu lượng truy cập, thông lượng… Để đánh giá chi tiết hơn về chất lượng dịch vụ QoS và mức độ hoạt động của các dịch vụ trong mạng và đưa ra đánh giá về các lưu lượng ưu tiên của các dịch vụ FTP, Video Conferencing, Voice khi sử dụng trong mô hình mạng.

## **4.2. Thực hiện mô phỏng cho mô hình mạng**

### **4.2.1. Xây dựng mô phỏng**

Mô phỏng mô hình mạng với quy mô vừa và nhỏ với cơ chế sử dụng các công cụ có sẵn để mô phỏng. Trong đó, hệ thống được chia thành 2 bộ phận chính gồm các phòng máy chủ quản lý và còn lại là phòng ban khác nhau có thể truyền gửi gói tin giữa các PC với nhau và có thể gọi điện thoại Voice IP nội bộ trong mạng. Mỗi bộ phận sẽ bao gồm các router, switch và PC kết nối với nhau.

* Các Node trung tâm là Các Router: R1, R2, R3, R4 và R5.
* Đường dây cơ sở sử dụng Ethernet 1000BaseT (1000Mbps)
* Sử dụng mô hình nút ngoại vi để Ethernet WorkStation (trạm). Sử dụng tất cả 21 máy và 4 Server để mô phỏng cho hệ thống mạng LAN
* Sử dụng Ethernet Application, Profile, IP QoS để thêm các dịch vụ mạng: FTP, Video, VoIP.
* Sử dụng kỹ thuật hàng đợi cho các dịch vụ: Video Conferencing, Voice IP, FTP.



Hình 4.1. Mô hình thiết kế trên phần mềm Riverbed Opnet

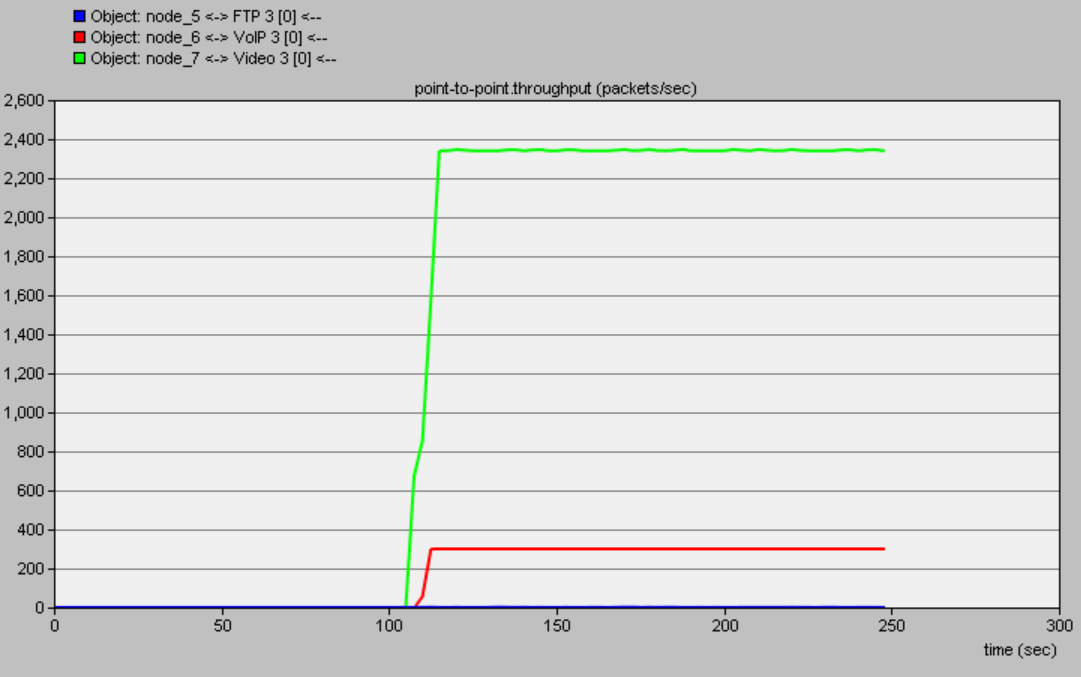
Cài đặt cấu hình cho từng ứng dụng FTP, Video Conferencing, Voice theo bảng dưới đây Trong tất cả các tình huống, nguồn và đích sẽ được bắt đầu ở 108 giây vì thời gian bắt đầu cấu hình được đặt là 40 giây và thời gian để tạo ra lưu lượng cho ứng dụng là 68 giây.

*Bảng 4.1. Cấu hình dịch vụ*

|  |  |
| --- | --- |
| **Dịch vụ** | **Cấu hình cho dịch vụ** |
| FTP | High load  Bandwidth Type: Best-effort  Mail, FTP, Web, Text |
| Video Conferencing | High Resolution Video  Frame size information (Byte), HD, Full HD, 4K-UHD, 8K-UHD |
| Voice | PCM Quality Speech  FLAC, MP3, MP4 |

### **4.2.2. Đánh giá kết quả thu được khi thực hiện mô phỏng**

**❖ Thông lượng**

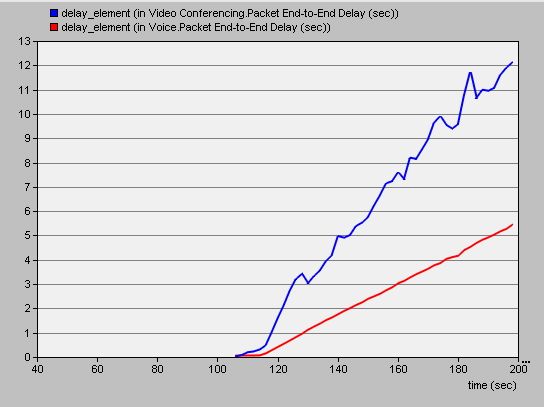
*****Hình 4.2. Thông lượng truyền tải trung bình của Router*

Thông lượng độ rộng băng thông của Video là cao nhất, độ rộng truyền tải của hai dịch vụ FTP và Voice thì thấp hơn Video, đều ổn định sau 100 giây mô phỏng.

Bảng 4.2. Thống kê thông lượng truyền tải trung bình

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **FTP** | **Video Conferencing** | **Voice** |
| 107.5 (Sec) | 0 (Packets/Sec) | 676.4 (Packets/Sec) | 0 (Packets/Sec) |
| 110 (Sec) | 0.4 (Packets/Sec) | 859.73 (Packets/Sec) | 60.4 (Packets/Sec) |
| 112.5 (Sec) | 1.2 (Packets/Sec) | 1574.672 (Packets/Sec) | 299.6 (Packets/Sec) |
| 170 (Sec) | 1.6 (Packets/Sec) | 2346.86 (Packets/Sec) | 300 (Packets/Sec) |
| 195 (Sec) | 0 (Packets/Sec) | 2340 (Packets/Sec) | 300 (Packets/Sec) |

**❖ Độ trễ từ đầu đến cuối của Video Conferencing và Voice**



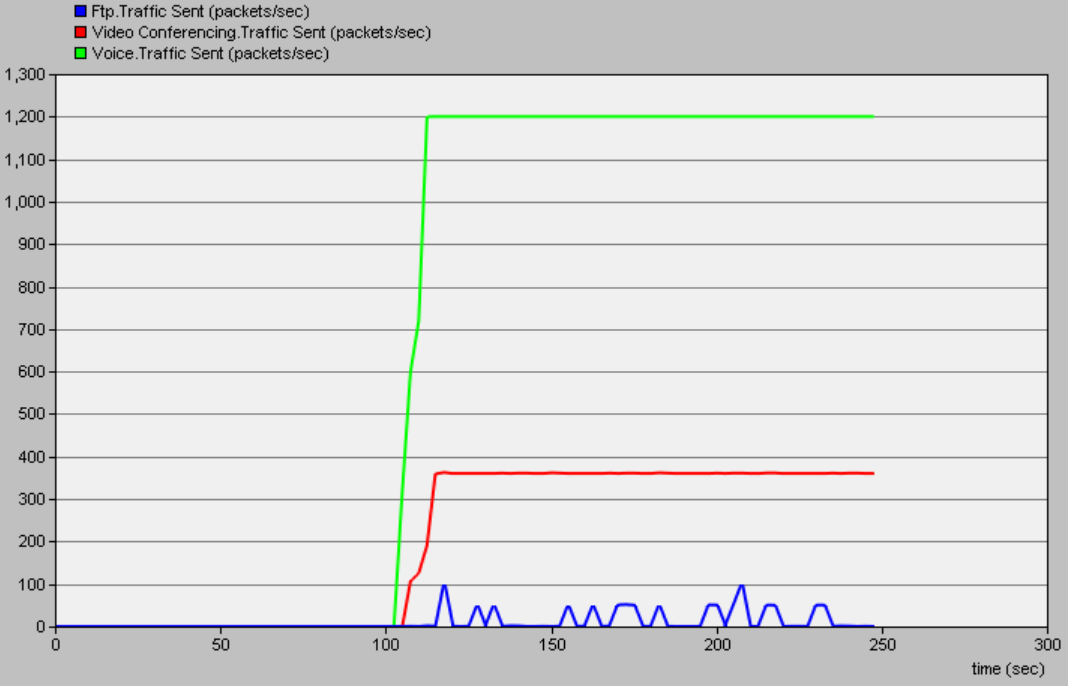
Hình 4.3. Độ trễ trung bình từ đầu đến cuối của Video conferencing và Voice

Trong khoảng thời gian các bytes bị ảnh hưởng bởi trễ hàng đợi thì packet end-to-end delay bằng 0. Sau đó packet end-to-end delay đi vào ổn định.

Bảng 4.3. Thống kê thời gian độ trễ từ đầu đến cuối của dịch vụ

|  |  |  |
| --- | --- | --- |
| **Time** | **Video Conferencing** | **Voice** |
| 112(Sec) | 0.23(Sec) | 0.0611(Sec) |
| 132(Sec) | 3.334(Sec) | 1.251(Sec) |
| 152(Sec) | 6.231(Sec) | 2.498(Sec) |
| 176(Sec) | 9.545(Sec) | 4.033(Sec) |
| 196(Sec) | 11.906(Sec) | 5.272(Sec) |

**❖ Lưu lượng gửi đi**



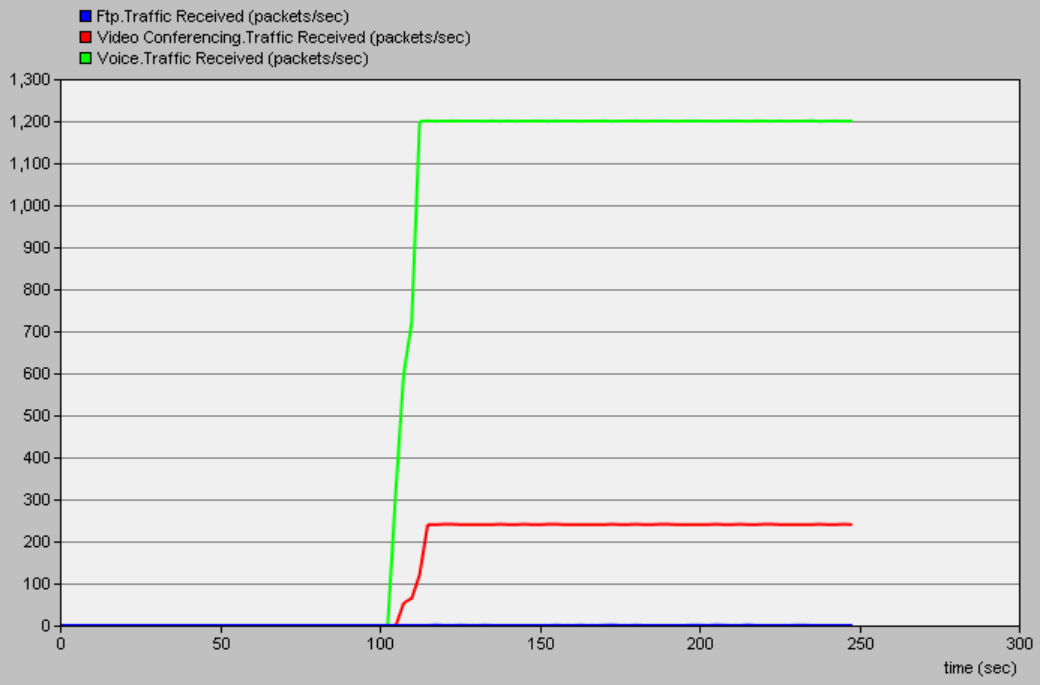
Hình 4.4. Lưu lượng gửi đi khi sử dụng các dịch vụ

Lưu lượng gửi đi khi sử dụng Voice thì lượng gói tin gửi đi cao hơn so với 2 dịch vụ FTP và Video điều đó chứng tỏ dịch vụ Voice có lưu lượng ưu tiên tối ưu hơn hẳn so với các dịch vụ còn lại.

*Bảng 4.4. Thống kê lưu lượng gửi đi*

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **FTP** | **Video Conferencing** | **Voice** |
| 110 (Sec) | 0 (Packets/Sec) | 126.8 (Packets/Sec) | 721.2 (Packets/Sec) |
| 117.5 (Sec) | 100 (Packets/Sec) | 362.4 (Packets/Sec) | 1200 (Packets/sec) |
| 175 (Sec) | 50 (Packets/Sec) | 360.8 (Packets/Sec) | 1200 (Packets/sec) |
| 207.5 (Sec) | 100.4 (Packets/Sec) | 360.8 (Packets/Sec) | 1200 (Packets/sec) |
| 220 (Sec) | 0 (Packets/Sec) | 360 (Packets/Sec) | 1200 (Packets/sec) |

**❖ Lưu lượng truy cập**



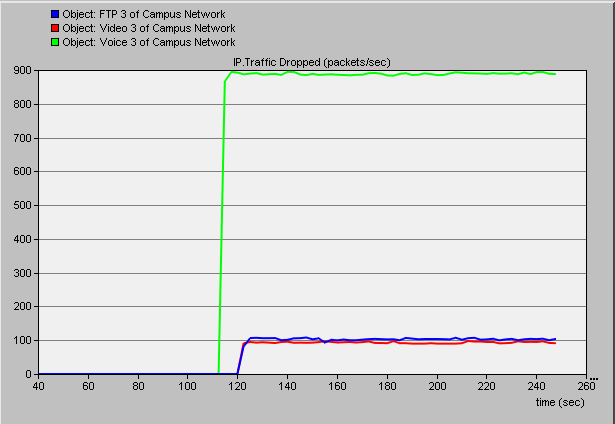
*Hình 4.5. Lưu lượng truy cập khi sử dụng dịch vụ*

Đối với lưu lượng nhận được khi sử dụng Voice thì lưu lượng gói tin nhận được ở mức rất cao so với các dịch vụ cùng mạng.

Bảng 4.5. Thống kê lưu lượng truy cập

|  |  |  |  |
| --- | --- | --- | --- |
| Time | FTP | Video Conferencing | Voice |
| 110 (Sec) | 0 (Packets/Sec) | 65.6 (Packets/Sec) | 721.6 (Packets/Sec) |
| 125 (Sec) | 0.4 (Packets/Sec) | 240 (Packets/Sec) | 1200 (Packets/Sec) |
| 150 (Sec) | 0 (Packets/Sec) | 240 (Packets/Sec) | 1200.4 (Packets/Sec) |
| 205 (Sec) | 0.8 (Packets/Sec) | 240.8 (Packets/Sec) | 1199.6 (Packets/Sec) |
| 210 (Sec) | 0 (Packets/Sec) | 240 (Packets/Sec) | 1200.4 (Packets/Sec) |

**❖ Lưu lượng truy cập giảm**



Hình 4.6. Lưu lượng truy cập giảm khi sử dụng các dịch vụ trong mạng

Các mô phỏng cũng đã được thực hiện như trong hình 4.9 về việc giảm gói tin, trong đó số liệu thống kê về giảm lưu lượng được hiển thị. Có thể quan sát thấy rằng Voice có mức giảm gói tin cao hơn rất nhiều so với FTP và Video.

*Bảng 4.6. Thống kê lưu lượng truy cập giảm của các dịch vụ*

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **FTP** | **Video Conferencing** | **Voice** |
| 127.5(Sec) | 107.2(Packets/Sec) | 92.8(Packets/Sec) | 890.8(Packets/Sec) |
| 145(Sec) | 108(Packets/Sec) | 92.8(Packets/Sec) | 886.8(Packets/Sec) |
| 167.5(Sec) | 100(Packets/Sec) | 93.2(Parket/Sec) | 885.6(Packets/Sec) |
| 182.5(Sec) | 102.8(Packets/Sec) | 97.2(Parket/Sec) | 883.5(Packets/Sec) |
| 197.5(Sec) | 103.6(Packets/Sec) | 91.2(Packets/Sec) | 888(Packets/Sec) |

## **4.3. Tổng quát đánh giá chất lượng truyền dẫn trong mạng**

* **Đánh giá chung**

Với các loại dịch vụ sẽ hoạt động theo các cách khác nhau và chúng có các ưu điểm và nhược điểm riêng thích hợp với từng loại dịch vụ lưu lượng. Có loại dịch vụ sẽ được ưu tiên hơn với loại lưu lượng này và không nên sử dụng với loại lưu lượng khác.

Việc tìm hiểu đặc tính của các loại dịch vụ và hàng đợi cho phép sử dụng hiệu quả kĩ thuật này trong việc điều khiển tắc nghẽn và điều khiển lưu lượng.

Bảng 4.7. Bảng tổng hợp đánh giá dịch vụ mạng theo tiêu chí lưu lượng

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiêu chí** | **FTP** | **Video Conferencing** | **Voice** |
| Thông lượng | 0.64 packets/sec | 1559.532 packets/sec | 192 packets/sec |
| Lưu lượng gửi đi | 50.08 packets/sec | 314.16 packets/sec | 1104.24 packets/sec |
| Lưu lượng truy cập | 0.24 packets/sec | 205.28 packets/sec | 1104.4 packets/sec |
| Lưu lượng truy cập giảm | 104.32 packet/sec | 93.44 packets/sec | 886.94 packets/sec |
| Độ trễ từ đầu đến cuối | 0 sec | 6.249 sec | 2.623 sec |

Thông lượng càng lớn thì quá trình truyền dữ liệu càng nhanh. Dịch vụ Video có độ rộng băng thông khá lớn vì thế các gói tin có gửi và nhận nhiều hơn trong suốt quá trình mô phỏng, đối với các dịch vụ Voice và FTP thì lưu lượng băng thông khá thấp lượng tin qua băng thông có phần nhỏ hơn vì cơ chế băng thông giới hạn cung cấp chỉ cho phép lần lượt các gói tin đi qua mà không có sự phân cấp nên dễ gặp tình trạng lưu lượng gói tin thấp.

Dịch vụ FTP sử dụng ít lưu lượng hơn so với Video và Voice khi được áp dụng cơ chế QoS, đặc biệt là trong các mạng kích thước trung bình được mô phỏng trong đồ án này, do FTP là là một giao thức truyền tải tập tin đơn giản từ máy tính này đến máy tính khác thông qua một mạng. Điểm yếu của FTP là thời gian gửi và nhận gói tin chậm hơn trong các mạng lớn hơn.

Voice hoạt động tốt hơn về khả năng gửi gói tin và độ trễ từ đầu đến cuối của mạng, Voice sử dụng kỹ thuật hàng đợi nên rất tối ưu băng thông. Kỹ thuật hàng đợi này giúp phân chia băng thông một cách tối ưu và có nhiều luồng xử lý gói tin tránh gây ra hiện tượng tắc nghẽn khi sử dụng. Trong một mạng mô phỏng kích thước trung bình, Voice luôn đòi hỏi yêu cầu xử lý và yêu cầu bộ nhớ bổ sung và tiêu thụ băng thông lớn cho việc làm ngập gói trạng thái liên kết ban đầu.

Video hoạt động tốt hơn về thời gian phản hồi trung bình trong mạng, lưu lượng định tuyến và độ trễ Ethernet. Video có các đặc điểm của kỹ thuật hàng đợi khi gói tin nào được vào trước thì sẽ ưu tiên gói đó và tránh để trường hợp thất thoát gói tin, nhưng khi có hiện tượng nhiều gói tin mà vào cùng 1 lúc ta có thể thấy là hiện tượng tắc nghẽn xuất hiện và làm gói tin luôn trong tình trạng gói tin ra ít hơn so với gói tin vào và làm giảm hiệu quả lưu lượng truyền tải gói tin, thời gian độ trễ của nó khá cao và làm giảm việc sử dụng băng thông.

* **Đánh giá các thống kê qua biểu đồ**
  + **Thông lượng**

Hình 4.7 Biểu đồ thông lượng truyền tải trung bình của các dịch vụ

* Thông lượng trung bình của Voice là khoảng 602.12 packets/sec. Điều này là do Voice sử dụng tín hiệu âm thanh tương tự, cần phải được mã hóa và giải mã trước khi truyền qua mạng. Quá trình này tiêu tốn một lượng băng thông đáng kể.
* Thông lượng trung bình của FTP là khoảng 361.326 packets/sec. FTP là một giao thức truyền tệp, được sử dụng để truyền các tệp lớn qua mạng. Giao thức này có thể sử dụng nhiều băng thông, tùy thuộc vào kích thước và tính chất của tệp được truyền.
* Thông lượng trung bình của Video Conferencing là khoảng 1559.532 packets/sec. Video Conferencing sử dụng tín hiệu video tương tự, cần phải được mã hóa và giải mã trước khi truyền qua mạng. Quá trình này tiêu tốn một lượng băng thông lớn đáng kể.
* **Lưu lượng gửi đi**

Hình 4.8. Biểu đồ thể hiện lưu lượng gửi đi khi sử dụng các dịch vụ

* Lưu lượng gửi đi của dịch vụ Voice luôn ổn định ở mức cao, khoảng 1200 packets/sec. Điều này có thể giải thích bởi nhu cầu liên lạc thoại của người dân ngày càng tăng, đặc biệt là trong thời gian dịch bệnh.
* Lưu lượng gửi đi của dịch vụ Video Conferencing tăng đột biến vào khoảng thời gian 117.5s đổ đi. Đây là thời điểm nhiều người sử dụng các ứng dụng video conferencing để làm việc, học tập hoặc giải trí.
* Lưu lượng gửi đi của dịch vụ FTP thấp hơn hai dịch vụ còn lại, dao động trong khoảng 105 - 300 packets/sec. Điều này có thể giải thích bởi nhu cầu sử dụng dịch vụ FTP ngày càng giảm, khi các phương thức lưu trữ và chia sẻ dữ liệu khác trở nên phổ biến hơn.

Dựa trên biểu đồ, có thể thấy nhu cầu sử dụng các dịch vụ mạng Voice và Video Conferencing ngày càng tăng. Điều này đòi hỏi các nhà cung cấp dịch vụ cần nâng cấp cơ sở hạ tầng mạng để đáp ứng nhu cầu của người dùng.

* **Lưu lượng truy cập**

Hình 4.9. Biểu đồ thể hiện lưu lượng truy cập khi sử dụng các dịch vụ

Biểu đồ lưu lượng gửi đi của các dịch vụ mạng Voice, FTP, Video Conferencing cho thấy một số điểm đáng chú ý sau:

* Lượng lưu lượng gửi đi của Voice và Video Conferencing cao hơn nhiều so với FTP. Ở thời điểm cao nhất, lượng lưu lượng gửi đi của Voice lên tới 1200,4 packets/sec, trong đó Video đạt 640,8 gói/giây. Điều này có thể được giải thích bởi đặc điểm của các dịch vụ này. Voice và Video Conferencing đều sử dụng âm thanh và video, vốn là những dữ liệu có dung lượng lớn. FTP, mặt khác, chủ yếu được sử dụng để truyền tải các tệp dữ liệu, có dung lượng nhỏ hơn nhiều so với âm thanh và video.
* Lượng lưu lượng gửi đi của Voice và Video Conferencing có xu hướng biến động mạnh hơn so với FTP. Điều này có thể được giải thích bởi thực tế là Voice và Video Conferencing thường được sử dụng cho các cuộc gọi và hội nghị trực tuyến, trong khi FTP thường được sử dụng để truyền tải các tệp dữ liệu theo kế hoạch. Các cuộc gọi và hội nghị trực tuyến có thể có số lượng người tham gia và thời lượng khác nhau, dẫn đến lượng lưu lượng gửi đi biến động.

**❖ Kết luận chung**

Sau khi mô phỏng mô hình và đánh giá chất lượng truyền dẫn, thông qua các tiêu chí: độ trễ, lưu lượng truy cập, lưu lượng gửi đi, lưu lượng truy cập giảm, thông lượng để nhằm đánh giá chất lượng truyền dẫn trong mạng IP khi sử dụng dịch vụ FTP, Video Conferencing và Voice để đảm bảo được tốc độ mạng khi sử dụng dịch vụ, lưu lượng gói tin gửi đi đến đích sao cho chính xác nhất, không gây rơi rớt gói tin hay làm trễ đường truyền mạng, và cho chúng ta thấy một cái nhìn rõ hơn về việc làm sao để đánh giá rằng một mạng hoạt động tốt trong hoàn cảnh nào, chất lượng truyền dẫn của mạng như thế nào, hoạt động tốt nhất đối với loại hình dịch vụ nào trong mạng và mức độ lưu lượng ưu tiên của mạng.

Biến đổi trễ này được tích lũy trong suốt quá trình gói tin được truyền từ bên gửi tới bên nhận. Tại mỗi node, địa chỉ đích trong gói tín được xem xét và so sánh với một danh sách các địa chỉ đích trong bảng định tuyến. Khi đi qua các node này, gói tin nhận một lượng trễ và biến đổi trễ phụ thuộc vào thời gian tra cứu bảng dữ liệu và số lượng gói phải xử lý trong một khoảng thời gian cho trước.

## **4.4. Kết luận chương 4**

Qua phần mô phỏng, so sánh, và đánh giá dựa trên các tiêu chí đã nêu, có thể nhận thấy rằng mỗi chương trình mô phỏng đều cung cấp khả năng đánh giá chất lượng truyền dẫn của mạng khi sử dụng các dịch vụ như FTP, video conferencing, và voice. Việc đánh giá chất lượng truyền dẫn được thực hiện thông qua việc xem xét các yếu tố ảnh hưởng tồn tại trong từng mô phỏng, từ đó phản ánh chất lượng truyền dẫn trong hệ thống mạng hiện tại.

Khi sử dụng các thiết bị đa dạng và có số lượng khác nhau, khả năng kết nối trong mỗi mạng vẫn tồn tại, tuy nhiên, sự khác biệt nằm ở việc khi áp dụng các thiết bị khác nhau và có số lượng khác nhau, chất lượng truyền dẫn cũng sẽ biến đổi. Điều này tạo ra sự đa dạng trong khả năng truyền dẫn mà không gặp phải vấn đề va chạm và tắc nghẽn mạng, từ đó gia tăng khả năng truyền tải thông tin một cách nhanh chóng và chính xác.

# KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

**❖ Kết luận**

Sau một thời gian tìm hiểu để tài “Mô phỏng đánh giá chất lượng truyền tải dữ liệu trong mạng IP” và thực hiện hoàn thành đồ án, em đã hoàn thành được những nội dung sau đây:

Việc tìm ra các vấn đề cản trở sự phát triển và lưu thông chất lượng truyền dẫn trên đường truyền mạng, cách vận chuyển các gói tin trong đường truyền hệ thống mạng cục bộ cũng như các lỗi thường gặp khi truyền gói tin đi và cách khắc phục lỗi.

Đánh giá được chất lượng truyền dẫn trong mạng thì cần dựa vào những yếu tố nào để đánh giá nó và yếu tố nào ảnh hưởng đến hoạt động của nó. Chất lượng truyền dẫn hoạt động sẽ có sự tác động của những yếu tố như độ trễ, thông lượng, lưu lượng truy cập nhận được, số gói tin va chạm, ...

Chất lượng lưu lượng truyền dẫn trong mạng có sự ảnh hưởng của rất nhiều yếu tố trong đường truyền mạng như tắc nghẽn, độ trễ, biến thiên độ trễ, .... Việc đảm bảo chất lượng dịch vụ truyền dẫn có được là do sự ảnh hưởng của việc xử lí mạng cục bộ trên cở sở tài nguyên mạng hiện có. Chúng có mối quan hệ mật thiết với chất lượng dịch vụ truyền dẫn cung cấp cho mạng.

Mục đích cuối cùng của bài là thiết kế một mô hình mạng giúp truyền tải những dữ liệu băng thông lớn, truyền lượng thông tin lớn mà không bị nhiễu hoặc mất tín hiệu, …

**❖ Hướng phát triển**

Xây dựng những mô hình mạng với điều kiện thực tế hơn, phức tạp hơn, chi tiết hơn và liên kết với nhau chặt chẽ hơn với những mô hình mạng đang được sử dụng phổ biến hiện nay.

Phát triển các mô hình từ mạng có kết nối mở rộng lên cho mạng đô thị, mạng quốc gia. Ứng dụng bằng cách mở rộng các mô hình mạng có sẵn và sử dụng thêm các thiết bị kết nối nhiều mạng lại thành một mạng rộng lớn để kết nối được xa hơn và rộng hơn nhưng vẫn phải đảm bảo được chất lượng truyền dẫn cũng như đường truyền của mạng. Mở rộng liên kết bằng các giao thức thiết bị khác nhau với nhiều hình thức mô hình mạng đa dạng khác nhau.

Mở rộng các điểm cung cấp dịch vụ có thể kéo lên những nơi ít người dùng, đảm bảo chất lượng truyền đi là tốt nhất. Khi lượng người truy cập cùng một lúc tăng lên thì tình trạng tắc nghẽn sẽ được giảm đến mức tối thiểu, các nhà cung cấp mạng sẽ cải tiến đường truyền để phù hợp với kinh tế của từng người, từng nhà. Độ phân dải cao phù hợp với lại tình trạng hiện tại như trong các cuộc họp truyền hình hội nghị hay trong các buổi tọa đàm,…

# TÀI LIỆU THAM KHẢO

**Tiếng Việt**

[1] Phạm Lê Tiệp, Nghiên cứu đánh giá chất lượng dịch vụ mạng IP bằng phần mềm OPNET, 123doc.com, năm 2012

[2] Lê Tuấn Anh, QoS là gì?, quantrimang.com, ngày 29.06.2021

[3] Nguyễn Văn Long, Nguyễn Đức Tiến, Nguyễn Xuân Ngọc, Internet QoS, Học Viện Công nghệ bưu chính viễn thông, 2021

**Tiếng Anh**

[4] Performance Modeling of Queuing Techniques for Enhance QoS Support for Uniform and Exponential VoIP & Video based Traffic B.K Mishra Principal, Thakur College of Engineering and Technology, Thakur Village, Kandivali (East), Mumbai-400101

[5] Managing IP Networks: Challenges and Opportunities (pp.57 – 142) Edition: 1st edition Publisher: John Wiley & Sons, Inc., Hoboken, NJ, USA Editors: Salah Aidarous, T. Plevyak

[6] Computer Science Department University of Crete HY536 - Network Technology Lab II, 2000 - 2001

[7] Pascal Lorenz, QOS in Next Generation Network. 26th International Conference Interfaces ITI 2004, June 7-10.

[8] Balogh, T.; Medvecky, M.; ―Performance evaluation of WFQ, WF2Q+ and WRR queue scheduling algorithms ―, Telecommunications and Signal Processing (TSP), 2011 34th International Conference 2011

[9] Hsieh, W.B., & Leu, J. S. (2018). Implementing a secure VoIP communication over SIP - based networks. Wireless Networks, 24(8), 2915-2926

**Website**

[10] https://www.youtube.com

[11] https://vi.wikipedia.org

[12] https://text.123docz.net

[13] https://doc.edu.vn

[14] https://timtailieu.vn