

VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY
UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING



OPERATING SYSTEM (CO3094)

Extended assignment

“Remote File Access Methods”

Instructor(s): Hoàng Lê Hải Thanh

Students: Nguyễn Xuân Huy Hoàng - 2311070 (*TN01 - Team hihahaha, **Leader***)
Trần Vĩnh Dũng - 2310574 (*TN01 - Team hihahaha*)
Lê Quang Dũng - 2310548 (*TN01 - Team hihahaha*)
Bùi Trọng Hiên - 2310993 (*TN01 - Team hihahaha*)
Nguyễn Đăng Hiên - 2310936 (*TN01 - Team hihahaha*)



Contents

List of Symbols	2
List of Acronyms	2
List of Figures	4
List of Tables	4
Member list & Workload	4
1 GIỚI THIỆU	5
2 DANH SÁCH CÁC PHƯƠNG PHÁP	5
2.1 Remote Desktop	5
2.2 File Transfer Protocol	6
2.3 Cloud sync	7
2.4 VPN	8
2.5 NAS với giao diện web - Synology	8
3 LỰA CHỌN PHƯƠNG PHÁP PHÙ HỢP NHẤT	10
4 MINH HỌA TRIỂN KHAI	11
5 KẾT LUẬN	11



List of Symbols

\mathbb{N} Set of natural numbers

\mathbb{R} Set of real numbers

\mathbb{R}^+ Set of positive real numbers

List of Acronyms

ODE (First-Order) Ordinary Differential Equation

IVP Initial-Value Problem

LTE Local Truncation Error

DS Dynamical System

Fig. Figure

Tab. Table

Sys. System of Equations

Eq. Equation

e.g. For Example

i.e. That Is



List of Figures

1	Caption	10
2	Hình ảnh từ máy chủ (Host) – máy tại nhà, đang bật Chrome Remote Desktop.	11
3	Hình ảnh từ máy client – kết nối thành công với máy chủ thông qua Chrome Remote Desktop. Người dùng có thể truy cập và thao tác trực tiếp các tệp tin trên máy chủ như đang ngồi trước máy đó.	11

List of Tables

1	Member list & workload	4
---	----------------------------------	---



Member list & Workload

No.	Fullname	Student ID	Problems	% done
1	Nguyễn Xuân Huy Hoàng	2311070	-	100%
2	Trần Vĩnh Dũng	2310574	-	100%
3	Lê Quang Dũng	2310548	-	100%
4	Bùi Trọng Hiến	2310993	-	100%
5	Nguyễn Đăng Hiên	2310936	-	100%

Table 1: Member list & workload

1 GIỚI THIỆU

Trong bối cảnh công nghệ thông tin phát triển mạnh mẽ, nhu cầu truy cập dữ liệu từ xa ngày càng trở nên phổ biến. Người dùng mong muốn có thể truy cập, quản lý hoặc chia sẻ tệp tin trên máy tính cá nhân ở nhà dù đang ở nơi khác, thông qua kết nối Internet.

Bài tập này nhằm mục đích giúp sinh viên tìm hiểu và so sánh các phương pháp truy cập tệp tin từ xa hiện nay, đánh giá ưu nhược điểm, yêu cầu cài đặt, và lựa chọn phương án phù hợp nhất cho người dùng phổ thông.

Việc hiểu và triển khai truy cập từ xa không chỉ giúp tiết kiệm thời gian, mà còn hỗ trợ công việc linh hoạt, đặc biệt trong các tình huống làm việc từ xa, học trực tuyến, hoặc quản lý hệ thống tại nhà.

2 DANH SÁCH CÁC PHƯƠNG PHÁP

2.1 Remote Desktop

1. Cách hoạt động:

- Remote Desktop Protocol (RDP) là giao thức do Microsoft phát triển, cho phép người dùng điều khiển giao diện đồ họa của một máy tính từ xa qua mạng.
- Khi kết nối, toàn bộ hình ảnh màn hình, chuột, bàn phím của máy đích được truyền tới máy truy cập.
- Người dùng thao tác như đang ngồi trực tiếp tại máy đích, trong khi toàn bộ quá trình xử lý vẫn diễn ra trên máy đích.

2. Yêu cầu hệ thống:

- **Máy đích (server):**
 - Hệ điều hành hỗ trợ RDP Server như Windows Pro/Enterprise/Server hoặc xRDP trên Linux.
 - Cần bật tính năng Remote Desktop và mở cổng TCP 3389 (hoặc cổng khác nếu thay đổi cấu hình).
- **Máy truy cập (client):**
 - Sử dụng phần mềm Microsoft Remote Desktop (Windows, macOS, iOS, Android) hoặc công cụ tương tự trên Linux.
 - Cung cấp địa chỉ IP/hostname của máy đích và thông tin đăng nhập hợp lệ.

3. Ưu điểm:

- Cho phép truy cập và điều khiển trực tiếp hệ điều hành từ xa.
- Tích hợp sẵn trên Windows, dễ sử dụng, hiệu năng cao.
- Hỗ trợ chia sẻ clipboard, ổ đĩa, âm thanh và máy in giữa hai máy.

4. Nhược điểm:

- Truyền giao diện đồ họa, không tối ưu nếu chỉ cần truyền file.
- Cổng 3389 dễ bị tấn công quét hoặc brute force nếu mở trực tiếp ra Internet.
- Hiệu năng phụ thuộc chất lượng mạng; độ trễ cao khi băng thông yếu.

5. Cấu hình an toàn:

- Ưu tiên sử dụng RDP qua VPN (OpenVPN, WireGuard) hoặc SSH tunnel.
- Đổi cổng mặc định 3389 sang cổng khác, giới hạn IP được phép truy cập.
- Bật Network Level Authentication (NLA) để xác thực trước khi thiết lập phiên làm việc.
- Cập nhật hệ thống thường xuyên để tránh lỗ hổng bảo mật.

2.2 File Transfer Protocol

1. **Cách hoạt động:** File Transfer Protocols là nhóm giao thức tiêu chuẩn cho việc truyền tải dữ liệu giữa máy chủ (server) và máy khách (client) qua Internet. Với phương pháp này, máy tính tại nhà được cấu hình như một *FTP/SFTP/FTPS server*, trong khi thiết bị ở xa đóng vai trò là *client*. Sau khi quá trình xác thực hoàn tất (username, password), người dùng có thể duyệt thư mục, tải lên hoặc tải xuống tệp tin trực tiếp.

- **FTP (File Transfer Protocol):** hoạt động dựa trên cơ chế client-server nhưng dữ liệu truyền tải không được mã hóa.
- **SFTP (SSH File Transfer Protocol):** sử dụng kết nối bảo mật thông qua giao thức SSH, đảm bảo toàn bộ dữ liệu và thông tin đăng nhập được mã hóa.
- **FTPS (FTP Secure):** bổ sung thêm lớp bảo mật bằng SSL/TLS trên nền tảng FTP truyền thống.

2. Yêu cầu:

- *Phần mềm:*
 - Máy chủ: FileZilla Server (Windows), vsftpd/proftpd (Linux).
 - Máy khách: FileZilla Client, WinSCP hoặc Cyberduck.
- *Phần cứng:*
 - Máy tính tại nhà (server) cần bật thường xuyên và có kết nối Internet ổn định.
 - Router hỗ trợ cấu hình port forwarding.
- *Cấu hình mạng:*
 - Cổng dịch vụ: 21 (FTP), 22 (SFTP), 990 (FTPS).
 - Địa chỉ IP công cộng: có thể là **tĩnh** hoặc **động**. Với IP động, cần sử dụng dịch vụ Dynamic DNS (DDNS) để ánh xạ thành tên miền cố định.

3. Ưu điểm:

- Cho phép truy cập trực tiếp vào tệp tin với tốc độ truyền tải nhanh.
- SFTP và FTPS hỗ trợ mã hóa, nâng cao tính bảo mật.
- Hỗ trợ đa nền tảng, nhiều công cụ miễn phí, dễ dàng triển khai trên Windows, Linux, macOS.

4. Nhược điểm:

- FTP thường không có mã hóa, dễ bị tấn công hoặc nghe lén trên đường truyền.
- Yêu cầu kiến thức kỹ thuật để cài đặt và cấu hình (đặc biệt là port forwarding và firewall).

- Máy chủ phải hoạt động liên tục, tiêu tốn điện năng và phụ thuộc vào chất lượng đường truyền Internet.

5. Cấu hình cụ thể:

- *Port forwarding*: cấu hình router cho phép truy cập từ ngoài Internet đến cổng dịch vụ (21/22/990).
- *Địa chỉ IP*:
 - Với IP tĩnh: có thể sử dụng trực tiếp để kết nối.
 - Với IP động: cần dịch vụ Dynamic DNS để cung cấp hostname cố định.
- *Firewall*: mở quyền cho phép kết nối đến các cổng dịch vụ FTP/SFTP/FTPS.
- *Khuyến nghị bảo mật*: ưu tiên sử dụng SFTP hoặc FTPS thay vì FTP thông thường để tránh rủi ro về an toàn dữ liệu.

2.3 Cloud sync

1. Cách hoạt động:

- Dịch vụ Cloud Sync (Google Drive, Dropbox, OneDrive, iCloud, v.v.) hoạt động bằng cách đồng bộ nội dung của một hoặc nhiều thư mục trên máy tính với không gian lưu trữ trực tuyến (cloud).
- Khi file được thêm, chỉnh sửa hoặc xóa trên máy tính, thay đổi này được tự động cập nhật lên cloud và ngược lại.
- Người dùng có thể truy cập hoặc chia sẻ file từ bất kỳ thiết bị nào thông qua ứng dụng hoặc trình duyệt web.

2. Yêu cầu:

- Có tài khoản của nhà cung cấp dịch vụ (Google, Microsoft, Apple, Dropbox, v.v.).
- Cài đặt ứng dụng đồng bộ (sync client) trên máy tính hoặc thiết bị di động để tự động cập nhật dữ liệu giữa máy và cloud.

3. Ưu điểm:

- Dễ sử dụng, thao tác đơn giản, phù hợp cho người dùng phổ thông.
- Truy cập file ở mọi nơi, trên nhiều thiết bị khác nhau.
- Một số dịch vụ hỗ trợ tính năng *versioning* — có thể khôi phục các phiên bản file trước đó.
- Dữ liệu được bảo mật bởi hạ tầng của nhà cung cấp (mã hóa, sao lưu).

4. Nhược điểm:

- Dữ liệu được lưu trên máy chủ của bên thứ ba, người dùng không hoàn toàn kiểm soát (không “tự chủ”).
- Dung lượng miễn phí có giới hạn; cần trả phí nếu muốn mở rộng.
- Tốc độ đồng bộ phụ thuộc vào kết nối mạng; có thể gặp độ trễ khi upload/-download file lớn.

5. Cấu hình khuyến nghị:

- Chỉ bật đồng bộ cho các thư mục thực sự cần thiết để tránh lãng phí dung lượng và băng thông.
- Bật xác thực hai yếu tố (2FA) để tăng cường bảo mật tài khoản.
- Định kỳ kiểm tra quyền chia sẻ file và thư mục để tránh rò rỉ dữ liệu ngoài ý muốn.

2.4 VPN

1. Cách hoạt động:

- VPN tạo kết nối mạng riêng ảo giữa thiết bị ở xa và mạng gia đình.
- Khi kết nối thành công, thiết bị từ xa được coi như nằm trong cùng mạng LAN.
- Người dùng có thể truy cập an toàn các dịch vụ như SMB, SFTP, RDP, ...

2. Yêu cầu:

- **Phần mềm:** Cài đặt VPN Server (OpenVPN, WireGuard, L2TP/IPsec) trên router, NAS, hoặc PC.
- **Mạng:** Router cần cấu hình port forwarding; có thể dùng Dynamic DNS nếu không có IP tĩnh.
- **Client:** Ứng dụng VPN Client trên thiết bị truy cập (Windows, macOS, Linux, iOS, Android).

3. Ưu điểm:

- **Bảo mật cao:** Toàn bộ lưu lượng được mã hóa.
- **Truy cập toàn diện:** Có thể dùng mọi dịch vụ mạng nội bộ như khi ở nhà.
- **Đa nền tảng:** Hỗ trợ nhiều hệ điều hành với client miễn phí.

4. Nhược điểm:

- **Khó cấu hình:** Yêu cầu thiết lập server, chứng chỉ, và port.
- **Yêu cầu mạng:** Phải mở port, đôi khi có thể bị ISP chặn.
- **Không tiện lợi:** Không *plug-and-play* như các dịch vụ cloud.

5. Cấu hình cần thiết:

- Thiết lập VPN Server (OpenVPN hoặc WireGuard).
- Tạo chứng chỉ bảo mật (CA, server key, client key).
- Cấu hình port forwarding (ví dụ UDP 1194 cho OpenVPN).
- Xuất file cấu hình (.ovpn hoặc tương tự) và import vào VPN Client.

2.5 NAS với giao diện web - Synology

1. Cách hoạt động:

- NAS (Network Attached Storage) có giao diện web và dịch vụ DDNS/relay (ví dụ: Synology QuickConnect, myQNAPcloud).
- Người dùng có thể truy cập file từ xa qua Internet mà không cần cấu hình phức tạp.

- Ngoài giao diện web, NAS còn hỗ trợ WebDAV, FTP/SFTP, SMB để tích hợp với nhiều ứng dụng khác.

2. Yêu cầu:

- **Phần cứng:** NAS (ví dụ Synology hoặc QNAP).
- **Phần mềm/dịch vụ:** Cấu hình QuickConnect hoặc myQNAPcloud, tài khoản nhà sản xuất.
- **Mạng:** Kết nối Internet ổn định, router hỗ trợ UPnP hoặc NAT.
- **Bảo mật:** Bật HTTPS (TLS/SSL).

3. Ưu điểm:

- Thiết kế chuyên cho chia sẻ file, có giao diện web GUI dễ sử dụng.
- Hỗ trợ đa nền tảng: web, PC, ứng dụng di động.
- Tích hợp thêm các chức năng *backup, sync, multimedia*.
- Có các giải pháp *relay/secure*, không cần port forwarding thủ công.

4. Nhược điểm:

- Chi phí đầu tư NAS khá cao so với các giải pháp cloud.
- Nếu mở trực tiếp SMB/FTP ra Internet thì rất rủi ro về bảo mật.
- Tốc độ phụ thuộc vào relay hoặc server trung gian khi dùng QuickConnect.

5. Cấu hình cần thiết:

- Đăng ký và bật QuickConnect (Synology) hoặc myQNAPcloud (QNAP).
- Bật HTTPS (TLS/SSL) để bảo mật kết nối.
- Kích hoạt 2FA cho tài khoản quản trị.
- Tránh mở trực tiếp SMB/FTP ra Internet, thay vào đó dùng relay hoặc VPN.

3 LỰA CHỌN PHƯƠNG PHÁP PHÙ HỢP NHẤT

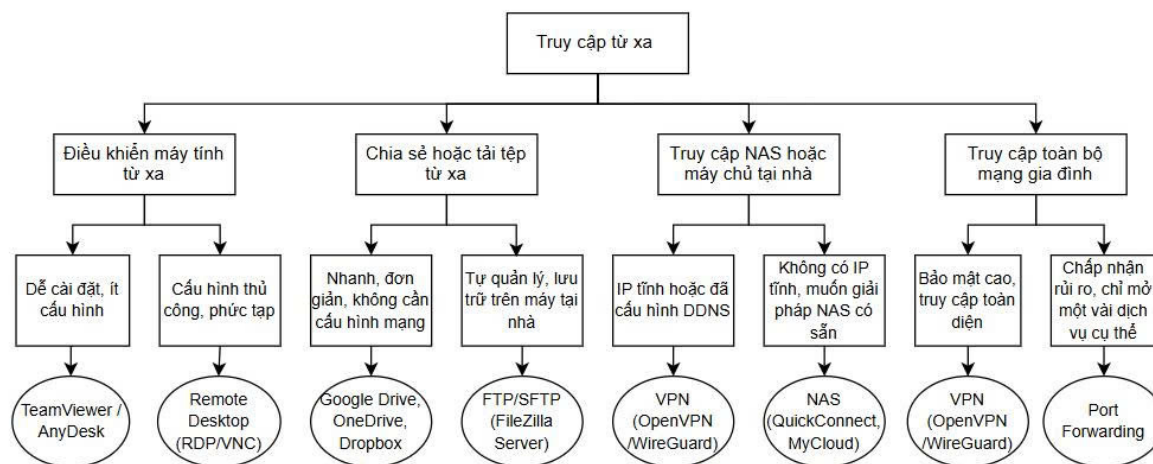


Figure 1: Caption

4 MINH HỌA TRIỂN KHAI

Trong phần này, chúng tôi minh họa việc triển khai **Chrome Remote Desktop** để truy cập máy tính tại nhà từ xa. Hai hình dưới đây thể hiện kết nối giữa máy chủ (host) và máy client.

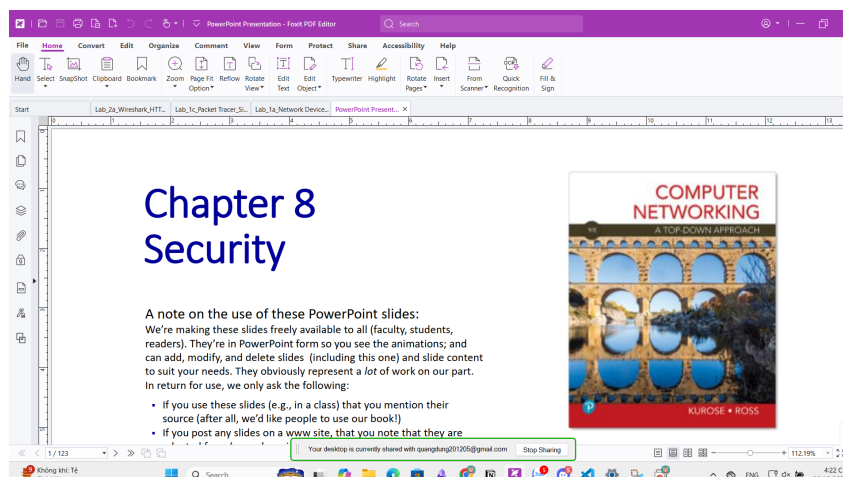


Figure 2: Hình ảnh từ máy chủ (Host) – máy tại nhà, đang bật Chrome Remote Desktop.

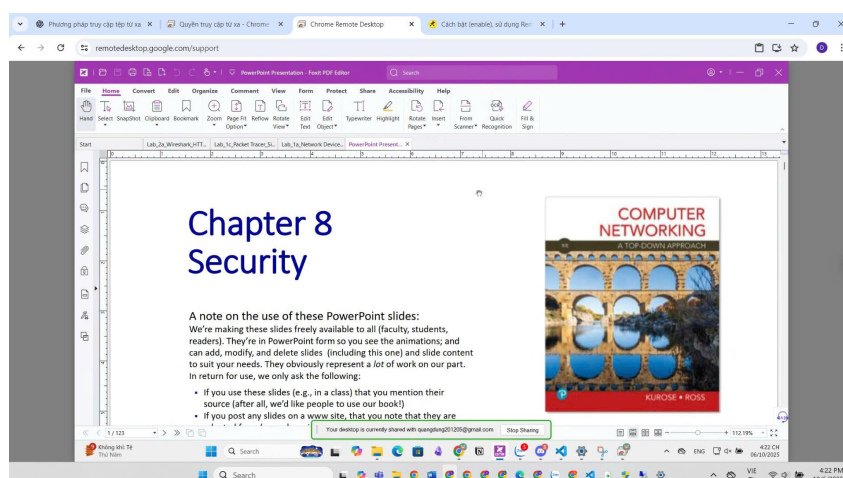


Figure 3: Hình ảnh từ máy client – kết nối thành công với máy chủ thông qua Chrome Remote Desktop. Người dùng có thể truy cập và thao tác trực tiếp các tệp tin trên máy chủ như đang ngồi trước máy đó.

Như minh họa trên, máy client có thể duyệt, mở, sao chép và quản lý các tệp tin trên máy server, chứng minh việc truy cập từ xa hoạt động thành công thông qua Internet mà không cần IP tĩnh hay cấu hình port phức tạp.

5 KẾT LUẬN

Qua quá trình nghiên cứu và thực hành, nhóm đã tìm hiểu được nhiều phương pháp truy cập tệp tin từ xa, bao gồm RDP/VNC, FTP/SFTP, VPN, và các dịch vụ đám mây. Mỗi phương pháp đều có ưu nhược điểm riêng, phù hợp với từng nhu cầu và trình độ kỹ thuật khác nhau.



Đối với người dùng phổ thông, sử dụng dịch vụ đồng bộ đám mây (Google Drive) là lựa chọn tối ưu nhờ sự đơn giản, bảo mật và miễn phí.

Đối với người cso nền tảng công nghệ, có thể kết hợp các phương pháp (ví dụ: VPN + NAS) để đạt được sự linh hoạt, an toàn và hiệu quả cao hơn trong việc truy cập dữ liệu từ xa.