

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC BÁCH KHOA  
KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH



BÁO CÁO

---

MẠNG MÁY TÍNH  
CHAT APPLICATION & NETWORK DESIGN

---

GVHD: **Bùi Xuân Giang**

Lớp: **L10**  
Nhóm: **L10**

Sinh viên thực hiện: **Nguyễn Minh Mỹ** 2013811  
**Hồ Đức Hưng** 2013381  
**Ngô Gia Phong** 2014121  
**Lưu Vũ Hà** 2013039

**Giáo viên hướng dẫn:** Bùi Xuân Giang

**Sinh viên thực hiện:**

Hồ Đức Hưng - 2013381 - hung.hoduccse@hcmut.edu.vn

Ngô Gia Phong - 2014121 - ngogiaphong123@hcmut.edu.vn

Nguyễn Minh Mỹ - 2013811 - my.nguyen060902@hcmut.edu.vn

Lưu Vũ Hà - 2013039 - ha.luuhaluu7202@hcmut.edu.vn

**Trường Đại Học Bách Khoa - ĐHQG HCM**  
**Khoa khoa học và kỹ thuật máy tính**  
**Báo cáo bài tập lớn Mạng máy tính**

# Mục lục

<b>1 Chat application</b>	<b>4</b>
1.1 Giới thiệu . . . . .	4
1.2 Sơ đồ Use-Case . . . . .	5
1.3 Entity–relationship model . . . . .	6
1.4 Communication Protocols . . . . .	6
1.4.1 WebSocket . . . . .	6
1.4.1.1 Định nghĩa . . . . .	6
1.4.1.2 Hoạt động . . . . .	6
1.4.1.3 Thư viện Socket.io . . . . .	6
1.4.2 WebRTC . . . . .	8
1.5 Các chức năng đã hiện thực . . . . .	10
1.5.1 Đăng ký . . . . .	10
1.5.2 Đăng nhập . . . . .	10
1.5.3 Tìm bạn bè . . . . .	11
1.5.4 Gửi lời mời kết bạn . . . . .	11
1.5.5 Chấp nhận/ từ chối lời mời kết bạn . . . . .	12
1.5.6 Xoá bạn bè . . . . .	12
1.5.7 Trò chuyện thời gian thực . . . . .	13
1.5.8 Call Video . . . . .	13
1.5.9 Gửi tệp (file Transfer) . . . . .	14
<b>2 Network design</b>	<b>15</b>
2.1 Phân tích yêu cầu . . . . .	15
2.2 Danh sách các thiết bị . . . . .	16
2.2.1 Server . . . . .	16
2.2.2 Switch 2 layer . . . . .	16
2.2.3 Access Point . . . . .	17
2.2.4 Switch Layer 3 . . . . .	17
2.2.5 Router . . . . .	18
2.2.6 Firewall . . . . .	19
2.3 Các thuật ngữ được sử dụng . . . . .	20
2.3.1 VLAN . . . . .	20
2.3.2 Sub-interface . . . . .	20
2.3.3 Access list . . . . .	20
2.3.4 Subnet mask . . . . .	20
2.3.5 Static NAT . . . . .	21
2.3.6 Dynamic NAT . . . . .	21
2.3.7 DMZ Network . . . . .	21
2.4 Thiết kế hệ thống mạng . . . . .	21
2.4.1 Cấu trúc mạng . . . . .	21
2.4.2 Thiết kế chi tiết mạng cho H6 . . . . .	23
2.4.3 IP diagram . . . . .	23
2.4.4 Hiện thực cấu hình firewall (tường lửa) . . . . .	23
2.4.5 Hiện thực trên Cisco Packet Tracer . . . . .	24
2.5 Kiểm tra hệ thống . . . . .	26



---

2.6	Tính toán băng thông, dung lượng lưu trữ và lưu lượng mạng . . . . .	26
2.6.1	Stotage capacity (dung lượng lưu trữ) . . . . .	26
2.6.2	Tính toán về bandwidth (băng thông) và Throughput (thông lượng) . . . . .	27
2.7	Dánh giá hệ thống . . . . .	27
2.7.1	Bảo mật . . . . .	27
2.7.1.1	Phân tích yêu cầu . . . . .	27
2.7.1.2	Hướng giải quyết được đề xuất . . . . .	28
2.7.2	Những vấn đề chưa giải quyết . . . . .	28
2.7.3	Các bước tiếp theo . . . . .	28



# Chương 1

## Chat application

### 1.1 Giới thiệu

Ứng dụng trò chuyện trực tuyến trong thời gian thực như telegram, zalo, messenger ... là một phần không thể thiếu, chúng len lỏi tới tất cả các khía cạnh của đời sống, từ nhu cầu công việc, học tập cho tới giải trí. Nhu cầu trao đổi thông tin ngày càng nhiều đòi hỏi ứng dụng phát triển phải đạt hiệu quả tối đa.

Các mô hình kỹ thuật được ứng dụng trong ứng dụng này bao gồm client - server, giao thức TCP/IP cũng được ứng dụng rộng rãi

#### Yêu cầu chức năng cơ bản

Yêu cầu cơ bản của ứng dụng trò chuyện bao gồm:

- Trò chuyện thời gian thực
- Gửi tệp
- Gọi video

Ngoài ra còn ứng dụng còn có các chức năng mở rộng như

- Gửi yêu cầu kết bạn
- Chấp nhận và từ chối yêu cầu kết bạn
- Xóa bạn bè ra khỏi danh sách
- Tìm bạn bè

#### Yêu cầu phi chức năng

- Phát triển trên môi trường web app
- Thời gian phản hồi theo thời gian thực

## 1.2 Sơ đồ Use-Case



Hình 1.1: Sơ đồ use-case cho chat application

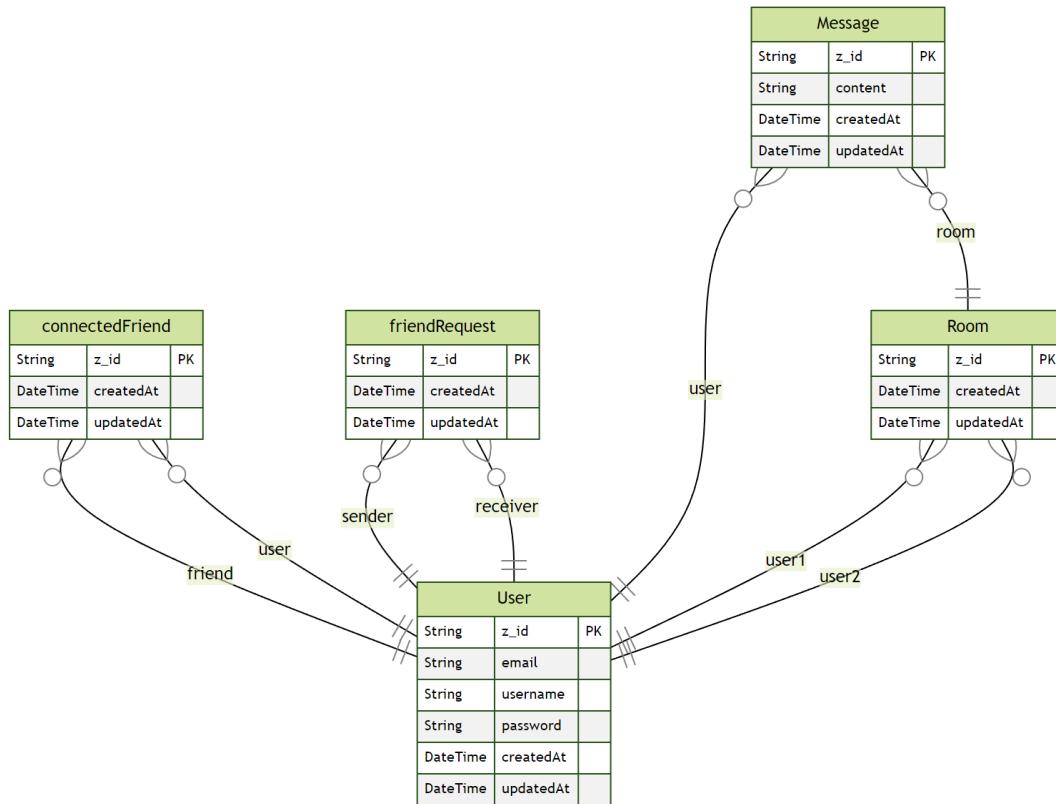
Các Actor gồm có:

- User
- Peer Server

Use-case gồm:

- Tìm bạn bè
- Chấp nhận / Từ chối lời mời kết bạn
- Gửi tệp
- Gửi lời mời kết bạn
- Gọi video
- Xóa bạn
- Trò chuyện
- Kết nối Peer

### 1.3 Entity–relationship model



Hình 1.2: Sơ đồ ERD cho chat application

### 1.4 Communication Protocols

#### 1.4.1 WebSocket

##### 1.4.1.1 Định nghĩa

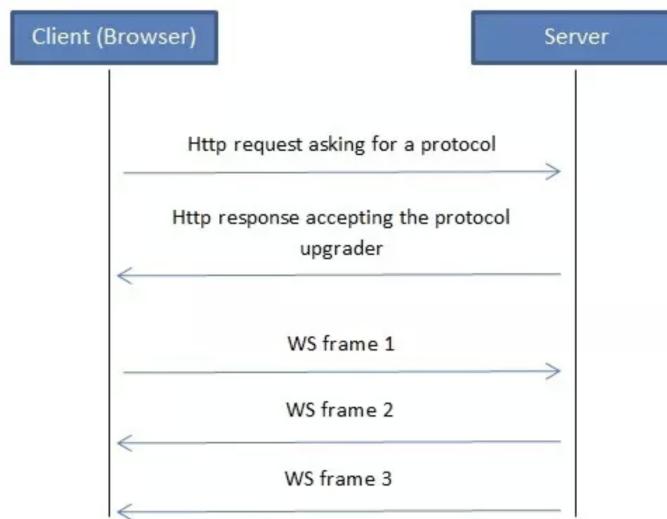
WebSocket là một communication protocol giúp truyền dữ liệu hai chiều giữa client-server thông qua một kết nối TCP duy nhất. Hơn nữa, WebSocket là một giao thức được thiết kế để truyền dữ liệu bằng cách sử dụng cổng 80 và cổng 443 và nó là một phần của HTML5. Vì vậy, webSockets có thể hoạt động trên các cổng web tiêu chuẩn, nên không gặp rắc rối về việc mở cổng cho các ứng dụng, lo lắng về việc bị chặn bởi tường lửa hoặc máy chủ proxy.

##### 1.4.1.2 Hoạt động

Giao thức có hai phần: Bắt tay và truyền dữ liệu. Ban đầu client sẽ gửi yêu cầu khởi tạo kết nối websocket đến server, server kiểm tra và gửi trả kết quả chấp nhận kết nối, sau đó kết nối được tạo và quá trình gửi dữ liệu có thể được thực hiện, dữ liệu chính là các Ws frame.

##### 1.4.1.3 Thư viện Socket.io

Socket.io là một thư viện cho phép giao tiếp dựa trên sự kiện, hai chiều và có độ trễ thấp giữa client và server.



**Hình 1.3:** Cách thực hiện hoạt động của *WebSocketProtocol*

Nó được xây dựng dựa trên giao thức WebSocket và cung cấp các đảm bảo bổ sung như dự phòng cho HTTP long-polling hoặc kết nối lại tự động. Ưu điểm của thư viện socket.io :

1. HTTP long-polling fallback
2. Automatic reconnection
3. Packet buffering
4. Acknowledgements
5. Broadcasting
6. Multiplexing

Chi tiết xem tại : <https://socket.io/docs/v4/>

Sử dụng thư viện socket.io trong assignment :

```
// Client : Sidebar.js file
  socket.emit("join-room", friend.roomId);
// Client : RoomPage.js file
useEffect(() => {
  socket.on('receive-message', ({data}) => {
    setMessages([...messages, data]);
  })
}, [socket, messages])
const handleSendMessage = (e) => {
  e.preventDefault();
  e.stopPropagation();
  socket.emit("send-message", {message, sender, roomId, friend});
  setMessage("");
}
```

```
// Server : index.ts file
const app = express();
const httpServer = http.createServer(app);
const io = new Server(httpServer, {
```



```
cors: {
    origin: '*',
    methods: ['GET', 'POST'],
    credentials: true,
},
})
io.on('connection', (socket: Socket) => {
    logger.info(`Client connected: ${socket.id}`);
    socket.on('join-room', (roomId) => {
        // leave previous room
        const iterator = socket.rooms[Symbol.iterator]();
        iterator.next();
        const socketRoomId = iterator.next().value;
        socket.leave(socketRoomId);
        socket.join(roomId);
    });
    socket.on('send-message', async (data) => {
        const iterator = socket.rooms[Symbol.iterator]();
        iterator.next();
        const socketRoomId = iterator.next().value;
        const {roomId, sender, message} = data;
        const result = await addMessageService(roomId, sender.id, message);
        const response = {
            ...result,
            roomId,
        }
        if(result) {
            io.to(socketRoomId).emit('receive-message', response);
        }
    });
    socket.on('disconnect', () => {
        logger.info('user disconnected');
    });
});
```

#### 1.4.2 WebRTC

WebRTC (Web Real-Time Communication) là một dự án mã nguồn mở và miễn phí cung cấp cho các trình duyệt web và ứng dụng di động khả năng giao tiếp thời gian thực (RTC) thông qua các giao diện lập trình ứng dụng (API). Nó cho phép giao tiếp âm thanh và video hoạt động bên trong các trang web bằng cách cho phép giao tiếp ngang hàng trực tiếp, loại bỏ nhu cầu cài đặt plugin hoặc tải xuống ứng dụng gốc. Được Apple, Google, Microsoft, Mozilla và Opera hỗ trợ, các thông số kỹ thuật của WebRTC đã được xuất bản bởi World Wide Web Consortium (W3C) và Lực lượng đặc nhiệm kỹ thuật Internet (IETF).

#### Thư viện Peerjs

PeerJS triển khai WebRTC của trình duyệt để cung cấp API kết nối peer-to-peer hoàn chỉnh, có thể cấu hình và dễ sử dụng. Không cần gì ngoài peerID, peer có thể tạo kết nối luồng dữ liệu hoặc phương tiện P2P với một remote peer.

Chi tiết xem tại : <https://peerjs.com>

Sử dụng thư viện peerjs trong assignment :

```
// Client : VideoCall.js
useEffect(() => {
```



```
const peer = new Peer(user?.id);
peer.on('open', (id) => {
    setPeerId(id)
});
setRemotePeerIdValue(friendId);
// Await a call from a remote peer
peer.on('call', (call) => {
    var getUserMedia = navigator.getUserMedia || navigator.webkit GetUserMedia
    || navigator.mozGetUserMedia;
    getUserMedia({ video: true, audio: true }, (mediaStream) => {
        currentUserVideoRef.current.srcObject = mediaStream;
        currentUserVideoRef.current.play();
        call.answer(mediaStream)
        call.on('stream', function (remoteStream) {
            remoteVideoRef.current.srcObject = remoteStream
            remoteVideoRef.current.play();
        });
    });
})
peerInstance.current = peer;
}, [user, friendId])
```

```
// Client : FileTransfer.js
useEffect(() => {
    const peer = new Peer(user?.id);
    peer.on('open', (id) => {
        setPeerId(id)
    });
    // Await file from a remote peer
    peer.on('connection', (conn) => {
        conn.on('data', async ({sentFile, contentType, fileName}) => {
            const base64String = arrayBufferToBase64(sentFile);
            const blob = await b64toBlob(base64String, contentType);
            // create url for download
            const url = URL.createObjectURL(blob);
            setReceiveFile({url, fileName, contentType});
        });
    })
    peerInstance.current = peer;
}, [user])
const handleSendFile = (e) => {
    const conn = peerInstance.current.connect(remotePeerIdValue);
    conn.on('open', () => {
        const contentType = sentFile.type;
        const fileName = sentFile.name;
        conn.send({sentFile, contentType, fileName});
    });
}
```



## 1.5 Các chức năng đã hiện thực

### 1.5.1 Đăng ký

Name	Dăng ký
Protocol	HTTP
Description	Cho phép người dùng tạo account để truy cập vào hệ thống.

Hình 1.4: Đăng ký

### 1.5.2 Đăng nhập

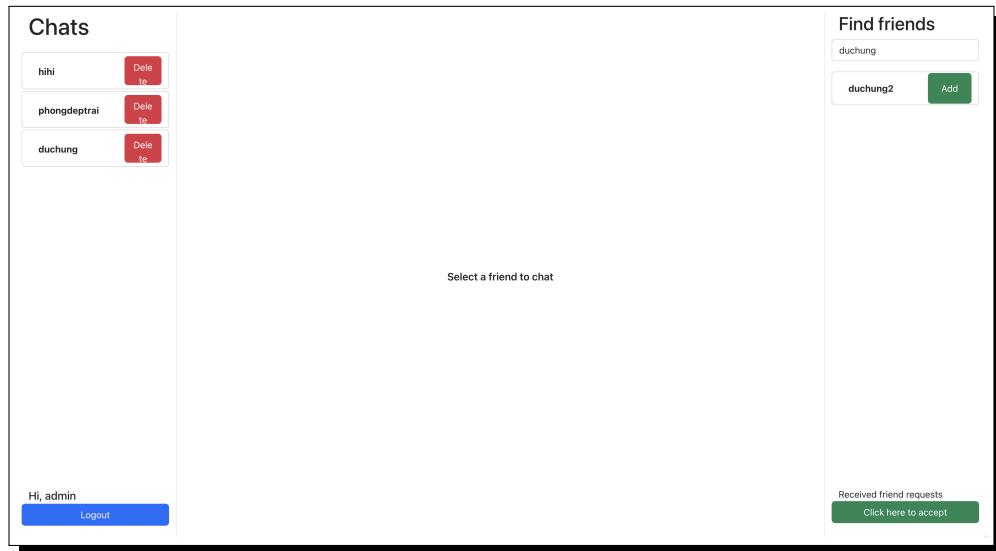
Name	Dăng nhập
Protocol	HTTP
Description	Cho phép người dùng đăng nhập bằng email password đã đăng ký để truy cập vào hệ thống.

Hình 1.5: Đăng nhập



### 1.5.3 Tìm bạn bè

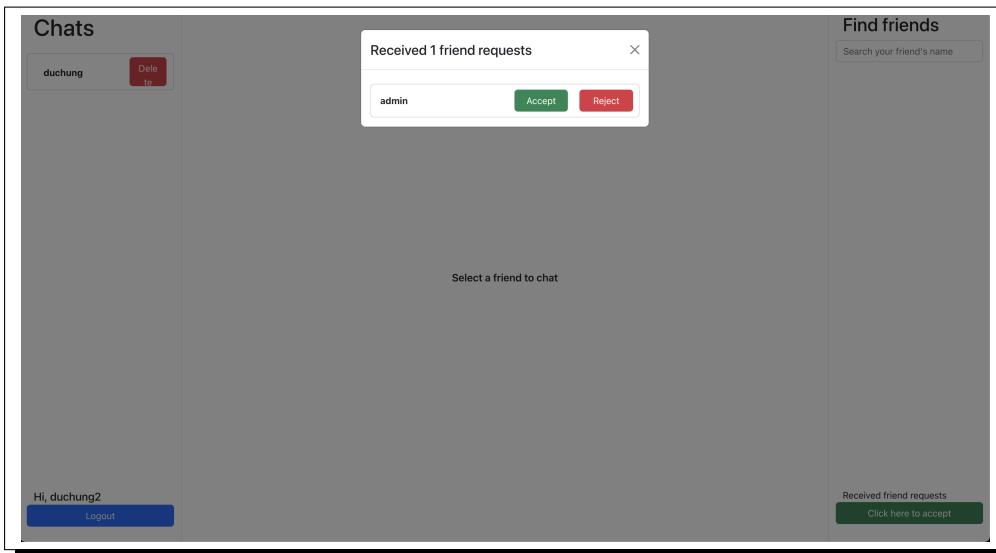
Name	Tìm bạn bè
Protocol	HTTP
Description	Người dùng đã truy cập hệ thống có thể tìm bạn bè của mình thông qua username ở thanh sidebar bên phải màn hình.



Hình 1.6: Tìm bạn bè

### 1.5.4 Gửi lời mời kết bạn

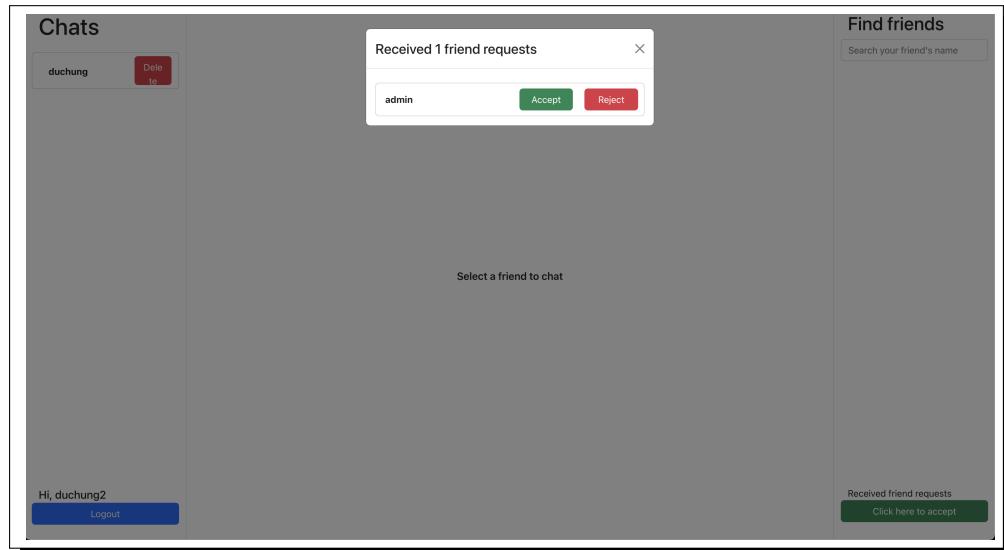
Name	Gửi lời mời kết bạn
Protocol	HTTP
Description	Sau khi tìm kiếm, hệ thống sẽ hiện thị một danh sách các user . Người dùng có thể nhấn nút add để gửi lời mời kết bạn đến 1 user cụ thể trong list các user mà hệ thống tìm được.



Hình 1.7: Gửi lời mời kết bạn

### 1.5.5 Chấp nhận/ từ chối lời mời kết bạn

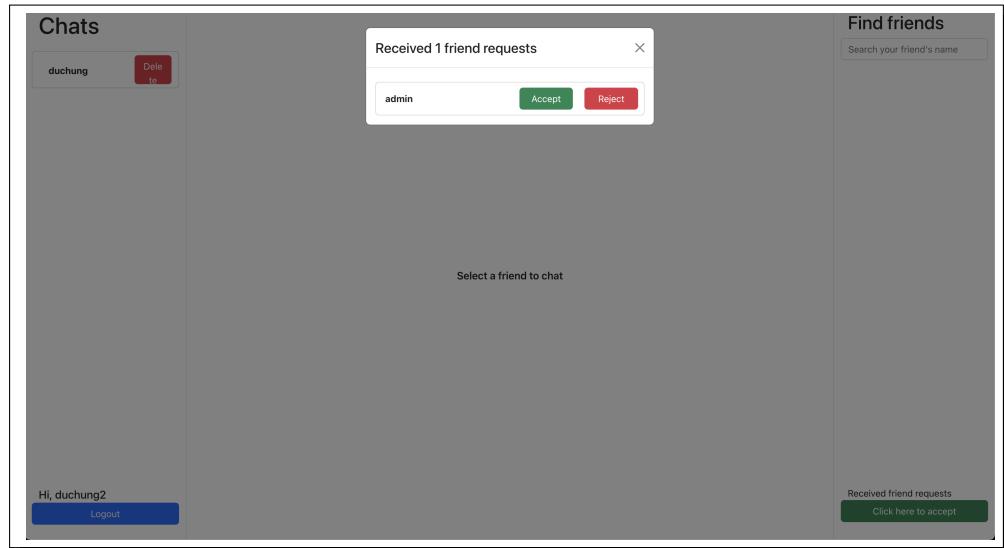
<b>Name</b>	Chấp nhận/ từ chối lời mời kết bạn
<b>Protocol</b>	HTTP
<b>Description</b>	Khi người dùng ấn vào nút "Click here to accept". Hệ thống sẽ hiện thi danh sách các lời mời kết bạn đã được gửi đến người dùng. Người dùng có thể accept hoặc reject lời mời kết bạn. Sau khi accept, user được accept sẽ được đưa vào danh sách bạn bè của người dùng.



Hình 1.8: Chấp nhận/ từ chối lời mời kết bạn

### 1.5.6 Xoá bạn bè

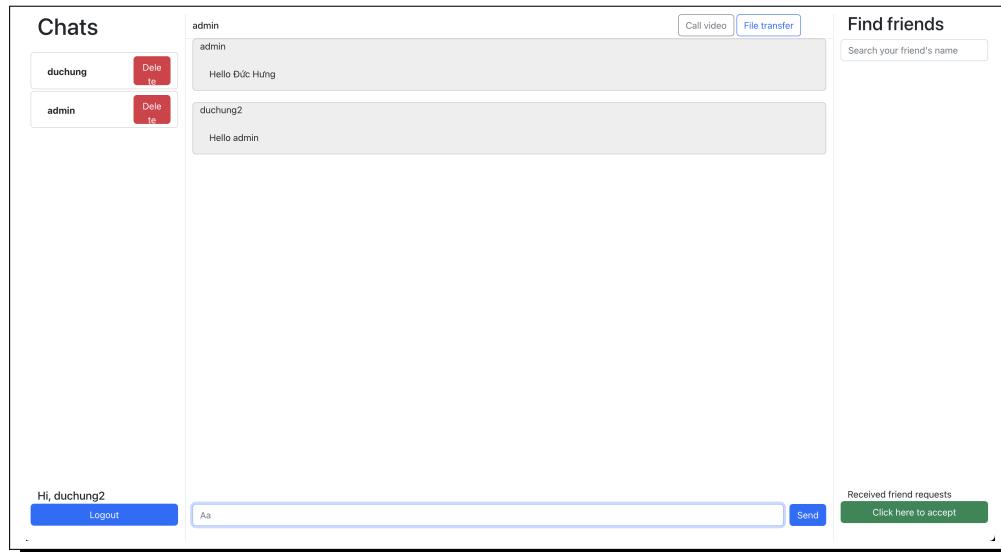
<b>Name</b>	Xoá bạn bè
<b>Protocol</b>	HTTP
<b>Description</b>	Khi người dùng ấn vào nút "Click here to accept". Hệ thống sẽ hiện thi danh sách các lời mời kết bạn đã được gửi đến người dùng. Người dùng có thể accept hoặc reject lời mời kết bạn. Sau khi accept, user được accept sẽ được đưa vào danh sách bạn bè của người dùng.



Hình 1.9: Xoá bạn bè

### 1.5.7 Trò chuyện thời gian thực

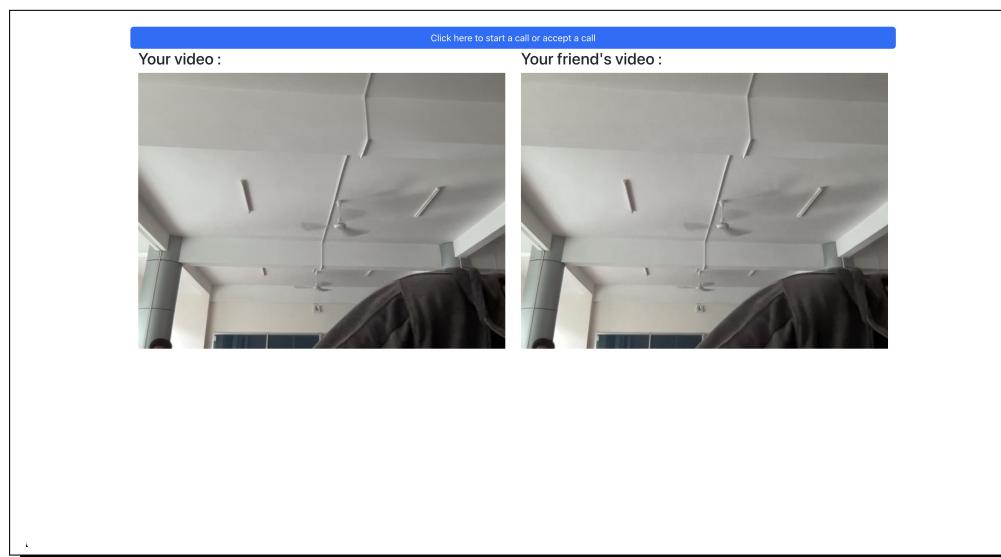
<b>Name</b>	Trò chuyện thời gian thực
<b>Protocol</b>	HTTP, WebSocket Protocol (based on TCP/IP)
<b>Description</b>	Cho phép 2 user đã kết nối với nhau (kết bạn) cùng truy cập vào hệ thống có thể trò chuyện thời gian thực bằng giao thức websocket (sử dụng thư viện Socket.IO).



Hình 1.10: Realtime chat

### 1.5.8 Call Video

<b>Name</b>	Call Video
<b>Protocol</b>	HTTP, WebRTC được sử dụng để thực hiện kết nối peer-to-peer
<b>Description</b>	Cho phép 2 user đã kết nối với nhau (kết bạn) cùng truy cập vào hệ thống có thể trò chuyện video thông qua giao thức Peer-to-Peer (sử dụng thư viện peerjs trong javascript).

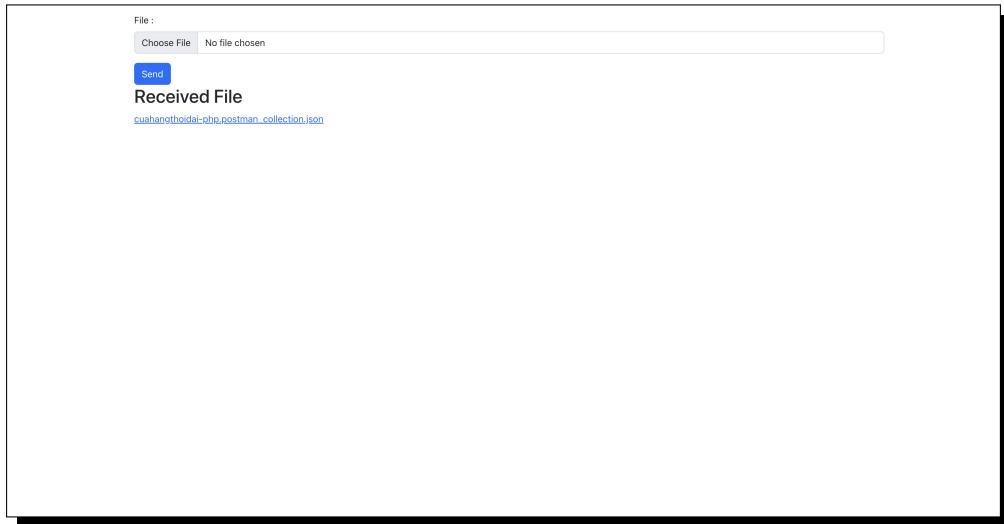


Hình 1.11: Video call



### 1.5.9 Gửi tệp (file Transfer)

<b>Name</b>	Gửi tệp (file Transfer)
<b>Protocol</b>	HTTP, WebRTC được sử dụng để thực hiện kết nối peer-to-peer
<b>Description</b>	Cho phép 2 user đã kết nối với nhau (kết bạn) cùng truy cập vào hệ thống có thể gửi tập tin thông qua giao thức Peer-to-Peer (sử dụng thư viện peerjs trong javascript).



Hình 1.12: Gửi file



## Chương 2

# Network design

### 2.1 Phân tích yêu cầu

Các yêu cầu mô tả của dự án về hệ thống máy tính tại tòa H6:

- Tòa H6 có hệ thống camera giám sát tại một số thời điểm và dữ liệu của camera sẽ được lưu trữ tập trung tại phòng máy chủ 106 H6. Ngoài ra còn có các phòng máy tính ở tầng 6 và 7.
- Ở các phòng lớn gồm có các thiết bị: 6 cảm biến nhiệt độ, 6 cảm biến ánh sáng và các thiết bị điều khiển ánh sáng
- Ở các phòng nhỏ gồm có các thiết bị: 3 cảm biến nhiệt độ, 3 cảm biến ánh sáng và các thiết bị điều khiển ánh sáng
- Các phòng học sẽ được trang bị máy tính để bàn. Ngoài ra, tòa H6 còn có văn phòng hành chính (administrative) gồm 10 máy tính.

Các mô tả dữ liệu được yêu cầu trong dự án:

- Một cảm biến sẽ đo một chỉ số khác nhưng kích thước định dạng dữ liệu của chúng là 32 Kb.
- Các thiết bị đo sẽ thu thập dữ liệu liên tục 1 phút 1 lần theo thời gian thực và gửi về máy chủ xử lý 5 phút 1 lần.
- Hệ thống camera giám sát hoạt động 24/7 sẽ lưu trữ dữ liệu trực tiếp về máy chủ trung tâm với tốc độ truyền dữ liệu 100 Mbps. Máy tính tại các phòng học mỗi ngày tải khoảng 200MB (giờ cao điểm từ 7h đến 17h30). Mỗi thiết bị khi kết nối với mạng WIFI được sử dụng với tốc độ tối đa 256 Kbps trong khoảng thời gian từ 7h30 đến 17h30.
- Tại tòa H6 thì các máy tính mỗi ngày tải khoảng 200 MB (giờ cao điểm là 8h-11h40, 13h-16h30) và gửi 10 email mỗi ngày, dung lượng tối đa 10 MB/email.
- Mỗi tầng là VLAN config và hệ thống có thể kết nối với H6.

Chi tiết về hệ thống tòa H6:

- Tầng 1:
  - Máy chủ sẽ được đặt tại 106-H6.
  - Phòng bình thường gồm: 6 phòng nhỏ và 3 phòng lớn.
  - Văn phòng hành chính (administrative office) gồm 10 máy vi tính.
  - Hệ thống gồm 4 camera giám sát.
- Tầng 2->5:
  - Phòng bình thường gồm: 6 phòng nhỏ và 3 phòng lớn.

- Hệ thống gồm 4 camera giám sát.
- Tầng 6-7:
  - Phòng bình thường gồm: 4 phòng nhỏ và 2 phòng lớn.
  - Có 3 phòng máy tính, mỗi phòng có 32 máy tính.
  - Hệ thống gồm 4 camera giám sát.

Các yêu cầu chi tiết cụ thể của các thiết bị:

- Hệ thống camera: phải kết nối mạng bằng dây vì tốc độ truyền dữ liệu của nó rất lớn và sẽ truyền dữ liệu về máy chủ với tốc độ 100 Mbps.
- Cảm biến nhiệt độ, cảm biến ánh sáng: Thu thập dữ liệu liên tục mỗi phút. Gửi dữ liệu đến máy chủ xử lý cứ sau 5 phút.
- Thiết bị cảm biến ánh sáng: Có nhiệm vụ gửi nhận dữ liệu để kiểm soát độ sáng của căn phòng.
- Điều khiển thiết bị điều hòa không khí: Có nhiệm vụ gửi nhận dữ liệu để kiểm soát nhiệt độ của căn phòng.

## 2.2 Danh sách các thiết bị

### 2.2.1 Server

Trong thiết kế server bao gồm các chức năng:

- Database server: Để lưu trữ thông tin.
- DHCP server: Để cấp ip cho các thiết bị.

### 2.2.2 Switch 2 layer

#### 2960-24TT

Switch chia cổng 24 port WS-C2960-24TT-L Catalyst 2960 24 10/100 + 2 1000BT LAN Base Image là thiết bị chia cổng chuyên dụng được sử dụng hầu hết tại các phòng sever mạng của ca nhân hay doanh nghiệp vừa và lớn.

Thiết bị chuyển mạch Switch Cisco WS-C2960-24TT-L là dòng Switch Layer 2 cung cấp kết nối mạng hiệu quả và hiệu quả cho các văn phòng chi nhánh hoặc các doanh nghiệp vừa và nhỏ. Những thiết bị chuyển mạch Fast Ethernet cấp doanh nghiệp cấp thiết nhập thiết bị hỗ trợ các dịch vụ cơ bản của Cisco Borderless Networks. Thông số kỹ thuật



**Hình 2.1: WS-C2960-24TT-L Cisco 2960 Switch**

- Loại phụ Fast Ethernet: Cổng 24 x 10/100 + 2 x 10/100/1000
- Hiệu suất: Dung lượng chuyển mạch: 32 Gbps

- Hiệu suất chuyển tiếp (kích thước gói 64 byte): 6,5 Mpps
- Phương pháp xác thực: RADIUS, Võ bảo mật (SSH), TACACS +
- RAM: 64 MB
- Bộ nhớ flash: 32 MB flash
- Kích thước bảng địa chỉ MAC: 8K mục nhập
- Phương pháp xác thực: Võ bảo mật (SSH), RADIUS, TACACS + Chỉ báo trạng thái: Tốc độ truyền cổng, chế độ song công cổng, nguồn, liên kết OK, hệ thống, liên kết / hoạt động
- Kích thước: 17,5 in x 9,3 in x 1,7 in
- Cân nặng: 8 lbs

### 2.2.3 Access Point

Bộ phát wifi Cisco Catalyst C9120AXI-S có thể được kết nối với Kiến trúc mạng kỹ thuật số của Cisco (Cisco DNA), là các sản phẩm cấp doanh nghiệp giúp tận dụng tốt hơn tất cả các tính năng và lợi ích mà Wi-Fi 6 cung cấp. Các bản phát hành IOS XE giúp người dùng có thể triển khai các bộ điều khiển controller 9800 series qua các thiết bị switch catalyst 9000 series, từ đó dễ dàng thêm các access point 9120 vào hệ thống mạng.

Cisco Catalyst C9120AXI-S cung cấp các công nghệ hàng đầu như MU-MIMO, OFDMA, cung cấp khả năng bảo mật tích hợp, khả năng phục hồi và tính linh hoạt trong các chế độ hoạt động. Sản phẩm cũng có thể cài đặt dễ dàng thành các điểm truy cập từ xa cho các công ty tổ chức có nhân viên làm việc tại nhà.



Hình 2.2: Access Point C9120AXI-S

### 2.2.4 Switch Layer 3

Cisco Catalyst 3560 Series là một loạt các thiết bị chuyển mạch có cấu hình cố định, cấp doanh nghiệp bao gồm các chức năng PoE (IEEE 802.3af) và Cisco prestandard Power over Ethernet (PoE) trong các cấu hình Fast Ethernet và Gigabit Ethernet. Cisco Catalyst 3560 là một bộ chuyển đổi lớp truy cập lý tưởng cho doanh nghiệp nhỏ truy cập mạng LAN hoặc môi trường văn phòng chi nhánh, kết hợp cả 10/100/1000 và PoE cấu hình cho năng suất tối đa và bảo vệ đầu tư trong khi cho phép triển khai các ứng dụng mới như điện thoại IP, truy cập, giám sát bằng video, hệ thống quản lý tòa nhà và video từ xa. Trong assignment lần này, nhóm sẽ sử dụng WS-C3560-24PS-S Cisco 3560 Switch

Thông số kỹ thuật :



Hình 2.3: WS-C3560-24PS-S Cisco 3560 Switch

Name	WS-C3560-24PS-S Cisco 3560 Switch
Device Type	Switch - 24 ports - L3 - Managed
Interfaces	Fast Ethernet
Ports	24 x 10/100 (PoE) + 2 x SFP
Power Over Ethernet (PoE)	PoE
MAC Address Table Size	12K entries
Routing Protocol	RIP-1, RIP-2, static IP routing
Remote Management Protocol	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, SSH-2
Compliant Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Power	AC 120/230 V ( 50/60 Hz )
Dimensions (WxDxH)	44.5 cm x 30 cm x 4.4 cm
Weight	5.1 kg

## 2.2.5 Router

Cisco 2800 Series cung cấp giá trị bổ sung đáng kể so với các thế hệ trước của bộ định tuyến Cisco ở mức giá tương tự bằng cách cung cấp cải thiện hiệu suất gấp năm lần, tăng gấp mươi lần hiệu suất bảo mật và thoại, các tùy chọn dịch vụ nhúng mới và tăng đáng kể hiệu suất khe cắm và mật độ trong khi duy trì hỗ trợ cho hầu hết trong số hơn 90 mô-đun hiện có cho Cisco 1700, Cisco 2600 và Cisco 3700 Series. Cisco 2800 Series có khả năng cung cấp nhiều dịch vụ đồng thời chất lượng cao ở tốc độ dây lên tới nhiều kết nối T1/E1/xDSL. Các bộ định tuyến cung cấp khả năng tăng tốc mã hóa nhúng và trên các khe cắm bộ xử lý tín hiệu kỹ thuật số giọng nói (DSP) của bo mạch chủ; hệ thống ngăn chặn xâm nhập (IPS) và chức năng tường lửa; tùy chọn tích hợp xử lý cuộc gọi và hỗ trợ hộp thư thoại; giao diện mật độ cao cho nhiều yêu cầu kết nối; và đủ hiệu suất và mật độ khe cắm cho các yêu cầu mở rộng mạng trong tương lai và các ứng dụng nâng cao.

Trong assignment lần này, nhóm sẽ sử dụng CISCO2811 Router

Thông số kỹ thuật :



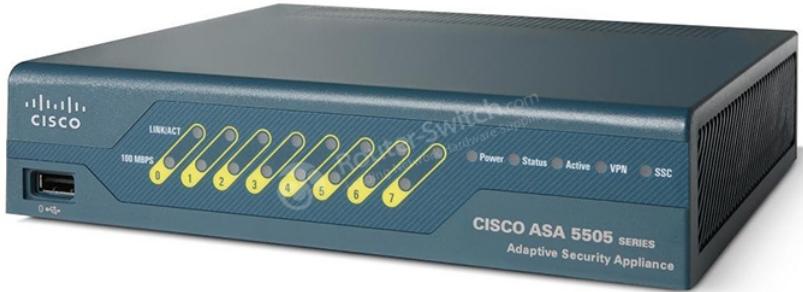
Hình 2.4: CISCO2811 Router

Name	CISCO2811 Router
Device Type	Cisco 2811 Router
DRAM Memory	512 MB (installed) / 768 MB (max) - DDR SDRAM
Flash Memory	128 MB (installed) / 256 MB (max)
Data Link Protocol	Ethernet, Fast Ethernet
Network / Transport Protocol	IPSec
Features	Cisco IOS IP Base , modular design, firewall protection, hardware encryption, VPN support, MPLS support, wall mountable, Quality of Service (QoS)
Remote Management Protocol	SNMP 3
Compliant Standards	IEEE 802.3af, IEEE 802.1x
Power	AC 120/230 V ( 50/60 Hz )
Dimensions (WxDxH)	43.8 cm x 41.7 cm x 4.5 cm
Weight	6.4 kg

## 2.2.6 Firewall

Thiết bị bảo mật thích ứng Cisco ASA 5505 ASA5505-BUN-K9 là thiết bị bảo mật thế hệ tiếp theo, có đầy đủ tính năng dành cho doanh nghiệp nhỏ, văn phòng chi nhánh và môi trường làm việc từ xa của doanh nghiệp. Cisco ASA 5505 cung cấp tường lửa hiệu suất cao, SSL và IPsec VPN cũng như các dịch vụ mạng phong phú trong một thiết bị "plug-and-play" theo mô-đun. Sử dụng Cisco ASDM tích hợp, Cisco ASA 5505 có thể được triển khai nhanh chóng và quản lý dễ dàng, cho phép các doanh nghiệp giảm thiểu chi phí vận hành. Cisco ASA 5505 có bộ chuyển mạch Fast Ethernet 8 cổng 10/100 linh hoạt, có các cổng có thể được nhóm động để tạo tối đa Vlan riêng biệt cho lưu lượng truy cập Internet tại nhà, doanh nghiệp và Internet để cải thiện phân đoạn và bảo mật mạng. Cisco ASA 5505 cung cấp hai cổng Cáp nguồn qua Ethernet (PoE), cho phép triển khai đơn giản các điện thoại IP của Cisco với khả năng thoại an toàn không cần chạm qua IP (VoIP) và triển khai các điểm truy cập không dây bên ngoài để tăng tính di động của mạng. Dịch vụ ngăn chặn xâm nhập và giảm thiểu sâu hiệu suất cao có sẵn với việc bổ sung AIP SSC. Có thể sử dụng nhiều cổng USB để kích hoạt các dịch vụ và chức năng bổ sung trong tương lai.

Thông số kỹ thuật :



Hình 2.5: Cisco ASA 5505

Name	ASA5505 Firewall
Description	ASA 5505 Security Appliance with SW, 10 Users, 8 ports, 3DES/AES, Cisco ASA 5500 Series Firewall Edition Bundles
Users/Nodes	10
Firewall Throughput	Up to 150 Mbps
Maximum Firewall and IPS Throughput	Up to 150 Mbps with AIP-SSC-5
Memory	256 MB
Minimum System Flash	64 MB
Dimensions (WxDxH)	1.75 x 7.89 x 6.87 in. (4.45 x 20.04 x 17.45 cm)
Weight	4.0 lb (1.8 kg)

## 2.3 Các thuật ngữ được sử dụng

### 2.3.1 VLAN

Üng với tầng lầu hoặc phòng ban, nhóm sẽ thiết kế một mạng VLAN. Việc này sẽ giúp hoàn thiện yêu cầu về chia sẻ riêng tư giữa các VLAN và tăng được hiệu năng cho hệ thống nhờ vào giảm chi phí truyền tải.

### 2.3.2 Sub-interface

Được sử dụng để routing giữa các VLAN nhờ vào lợi ích có thể lưu lại cỗng vật lý của router.

### 2.3.3 Access list

Được sử dụng để điều khiển truy cập giữa VLAN để tăng khả năng bảo mật. Chỉ có máy tính trong VLAN của server được quyền ping lẫn nhau, các VLAN khác thì không

### 2.3.4 Subnet mask

Nhóm sử dụng Subnet mask cho các IP ẩn danh bắt đầu từ 192.168.0.0. Mỗi VLANs sẽ có một khoảng IP riêng. Bằng cách này, ta sẽ có các lợi ích:

- Lưu trữ và có thể tối ưu hóa sự phân bố IP address
- Broadcast domain, tối ưu hiệu năng hệ thống do có thể nâng cao lưu lượng truy cập

### 2.3.5 Static NAT

Static NAT được dùng để chuyển đổi một địa chỉ IP này sang một địa chỉ khác một cách cố định, thông thường là từ một địa chỉ cục bộ sang một địa chỉ công cộng và quá trình này được cài đặt thủ công, nghĩa là địa chỉ ánh xạ và địa chỉ ánh xạ chỉ định rõ ràng tương ứng duy nhất.

Static NAT rất hữu ích trong trường hợp những thiết bị cần phải có địa chỉ cố định để có thể truy cập từ bên ngoài Internet. Những thiết bị này phổ biến là những Server như Web, Mail,...

### 2.3.6 Dynamic NAT

Dynamic NAT được dùng để ánh xạ một địa chỉ IP này sang một địa chỉ khác một cách tự động, thông thường là ánh xạ từ một địa chỉ cục bộ sang một địa chỉ được đăng ký. Bất kỳ một địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán một thiết bị bên trong mạng. Khác với static NAT, khi một thiết bị được dynamic NAT, thì ta không thể chủ động để thực hiện một kết nối đến thiết bị đó do hầu như ta không biết được tại thời điểm đó máy được dynamic NAT ra thành địa chỉ IP nào.

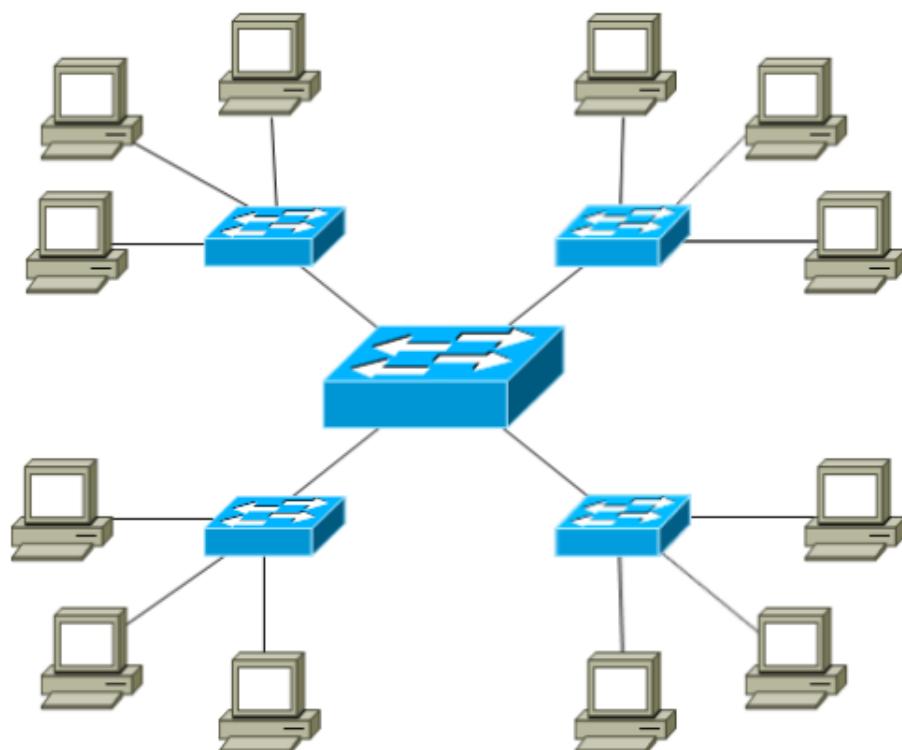
### 2.3.7 DMZ Network

DMZ Network giúp bảo vệ các máy chủ trong mạng nội bộ. Nếu các máy chủ công cộng bị tấn công, tin tức vẫn không thể dựa vào chúng để tấn công các máy chủ đặt bên trong có chứa thông tin quan trọng. Máy chủ trong DMZ bao gồm: Web, Mail, FTP, VoIP, ...

## 2.4 Thiết kế hệ thống mạng

### 2.4.1 Cấu trúc mạng

Dựa trên yêu cầu, thiết kế mạng theo dạng hình sao mở rộng (extend star topology) cho mỗi tầng Ưu



diểm:



- Giá thành không cao
- Dễ cho bảo trì và phát triển, đặc biệt khi cần phải thêm thiết bị vào hệ thống
- Nếu một workstation hoặc một thiết bị nào đó gặp trục trặc sẽ không làm trục trặc hệ thống



### 2.4.2 Thiết kế chi tiết mạng cho H6

1. Chia cấu trúc mạng thành các vlan (virtual local area network) để dễ quản lý:
  - VLAN 10: dành cho các thiết bị trong các phòng bình thường ở tầng 1 (phòng lớn và nhỏ)
  - VLAN 20: dành cho các thiết bị trong các phòng bình thường ở tầng 2 (phòng lớn và nhỏ)
  - VLAN 30: dành cho các thiết bị trong các phòng bình thường ở tầng 3 (phòng lớn và nhỏ)
  - VLAN 40: dành cho các thiết bị trong các phòng bình thường ở tầng 4 (phòng lớn và nhỏ)
  - VLAN 50: dành cho các thiết bị trong các phòng bình thường ở tầng 5 (phòng lớn và nhỏ)
  - VLAN 60: dành cho các thiết bị trong các phòng bình thường ở tầng 6 (phòng lớn và nhỏ)
  - VLAN 70: dành cho các thiết bị trong các phòng bình thường ở tầng 7 (phòng lớn và nhỏ)
  - VLAN 80: dành cho tất cả các camera giám sát
  - VLAN 90: dành cho các thiết bị máy chủ trong phòng server
  - VLAN 100: dành cho 10 PC trong văn phòng administrator
  - VLAN 110: dành cho các PC trong các phòng computer ở tầng 6 và 7
  - VLAN 120: dành cho các thiết bị điều hòa ở trong các phòng computer
2. Tạo các vlan tương ứng trên switch ở mỗi tầng và cả main switch.
3. Các switch ở các tầng sẽ được nối với main switch được đặt ở tầng 1 (Sử dụng switch layer 3 với mục đích có thể routing được cho các kết nối vào nó, giúp các vlan và các cổng được cấu hình ip có thể giao tiếp được với nhau)
4. Sử dụng dịch vụ DHCP của thiết bị server ở phòng server để cấp địa chỉ ip động cho các vlan yêu cầu (chi tiết dãy ip của mỗi vlan được thể hiện ở mục IP Diagram)
5. Áp dụng các ACLs trên main switch (access control lists) để có thể lọc các gói tin đi vào các vlan
  - ACLs cho camera: chỉ cho phép truy cập từ phòng server, phòng máy tính, phòng administrator. Ngoài ra từ chối tất cả các gói tin khác.
  - ACLs cho thiết bị điều hòa: chỉ cho phép truy cập từ phòng server và administrator, còn lại từ chối tất cả các gói tin khác.
  - ACLs cho phòng máy chủ: chỉ cho phép các camera, máy điều hòa gửi dữ liệu về, các máy ở phòng administrator có thể truy cập được, còn lại từ chối tất cả các gói tin khác.
  - ACLs cho phòng administrator: chỉ cho phép truy cập từ phòng server, còn lại từ chối các gói tin khác.

### 2.4.3 IP diagram

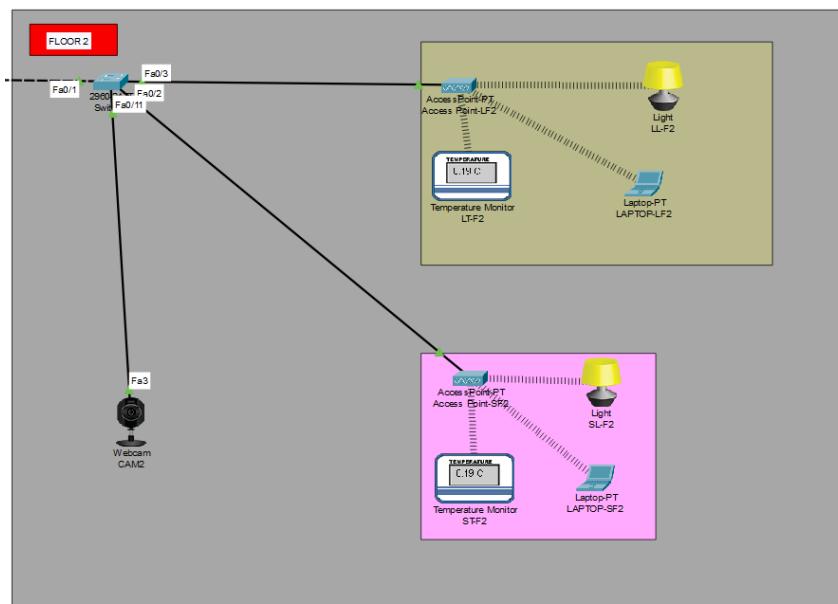
### 2.4.4 Hiện thực cấu hình firewall (tường lửa)

Sử dụng tường lửa để điều khiển truy cập từ bên ngoài internet vào bên trong mạng H6 và ngược lại. (Chi tiết trong file H6\_Network(pkt và được demo vào buổi thuyết trình)

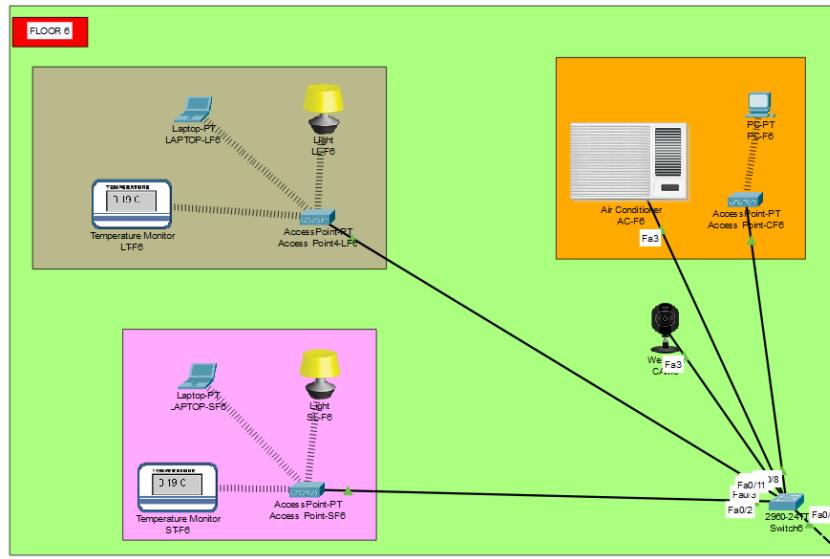
Bảng 2.1: Dãy ip của các VLAN

VLAN	Đối tượng	Network	IP range
10	Normal rooms in floor	192.168.1.0/24	192.168.1.5-254
20	Normal rooms in floor 2	192.168.2.0/24	192.168.2.5-254
30	Normal rooms in floor 3	192.168.3.0/24	192.168.3.5-254
40	Normal rooms in floor 4	192.168.4.0/24	192.168.4.5-254
50	Normal rooms in floor 5	192.168.5.0/24	192.168.5.5-254
60	Normal rooms in floor 6	192.168.6.0/24	192.168.6.5-254
70	Normal rooms in floor 7	192.168.7.0/24	192.168.7.5-254
80	Normal rooms in floor 8	192.168.8.0/24	192.168.8.5-254
90	Normal rooms in floor 9	192.168.9.0/24	192.168.9.5-254
100	Normal rooms in floor 10	192.168.10.0/24	192.168.10.5-254
110	Normal rooms in floor 11	192.168.11.0/24	192.168.11.5-254
120	Normal rooms in floor 12	192.168.12.0/24	192.168.12.5-254

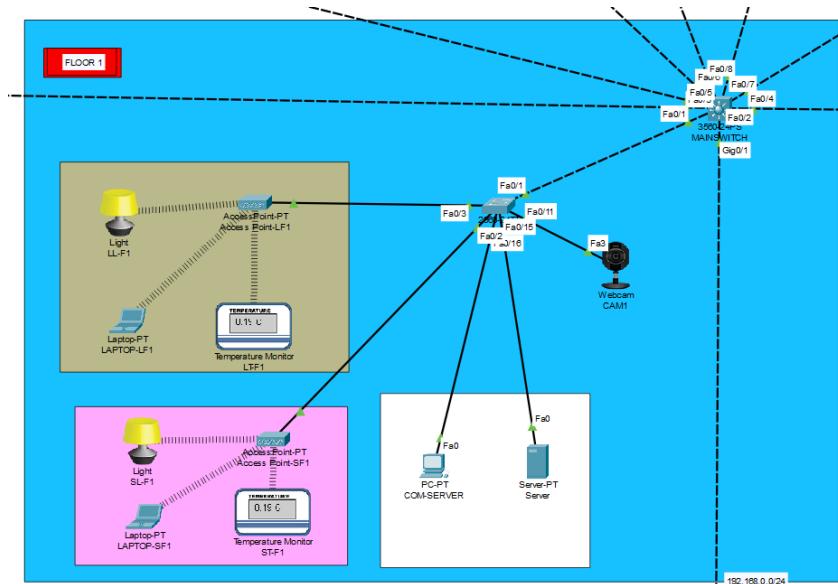
#### 2.4.5 Hiện thực trên Cisco Packet Tracer



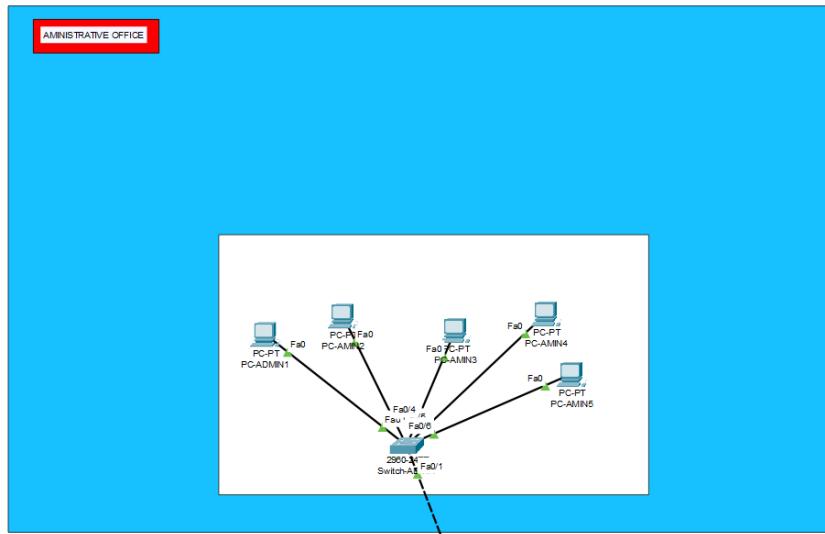
Hình 2.6: Cấu trúc mô phỏng mạng ở các tầng 2-5



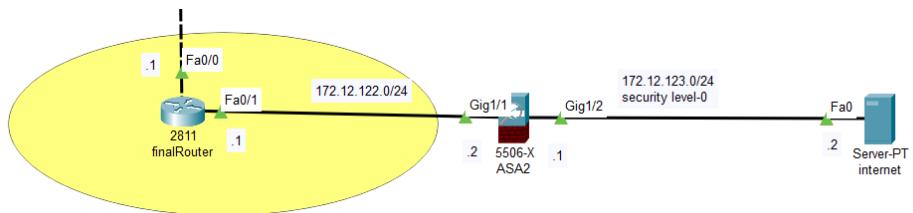
Hình 2.7: Cấu trúc mô phỏng mạng ở các tầng 6-7



Hình 2.8: Cấu trúc mô phỏng mạng ở các tầng 1



Hình 2.9: Cấu trúc mô phỏng mạng ở các tầng admin



Hình 2.10: Cấu trúc mạng mô phỏng quá trình truy cập ra ngoài internet

### Tổng quát

Trong mô hình này

- Vùng màu hồng đại diện cho một phòng nhỏ
- Vùng màu nâu đại diện cho phòng lớn hơn
- Mỗi phòng đều có 1 access point để truy cập mạng
- Một camera được kết nối thẳng tới switch đại diện cho 4 camera được đặt ở hành lang
- Switch sẽ nối thẳng tới main switch được đặt ở tầng 1
- Các máy điều hòa được nối thẳng tới switch ở tầng 6 và 7 để dễ thiết lập vlan cho nó.

## 2.5 Kiểm tra hệ thống

Trong phần này, ta sử dụng các tiêu chuẩn sau để kiểm tra sự kết nối trong thiết kế mạng:

- Thực hiện kết nối được giữa các thiết bị trong cùng một VLAN
- Thực hiện kiểm thử kết nối được giữa các thiết bị ở các VLANs khác nhau
- Các máy tính có thể kết nối Internet được đến một Web server

Chi tiết của phần này sẽ được thể hiện rõ hơn trong phần demo.

## 2.6 Tính toán băng thông, dung lượng lưu trữ và lưu lượng mạng

### 2.6.1 Storage capacity (dung lượng lưu trữ)

Theo mô tả yêu cầu của dự án, chỉ cho chúng ta biết sẽ có hệ thống camera giám sát chứ chưa đi vào chi tiết hoạt động như thế nào và công suất ra sao và dữ liệu từ các cảm biến có thể được xử lý và truyền tải



ngay (thu nhập dữ liệu 1 phút một lần và gửi đi sau 5 phút). Do đó, chỉ cần tập trung vào một chi tiết quan trọng là lưu trữ dữ liệu của các cảnh quay được từ camera giám sát tại các tầng. Dự án yêu cầu tại mỗi tầng sẽ bao gồm 4 camera giám sát, ví vậy toàn bộ tòa nhà sẽ có 28 camera. Giả sử, mỗi camera mỗi ngày sẽ lưu trữ 25GB dữ liệu, nên ta có 28 camera sẽ chiếm 700GB một ngày và khoảng 21000GB một tháng tương đương 20.5TB một tháng và khoảng 246TB một năm. Vì vậy, nếu muốn toàn bộ camera trong tòa nhà lưu trữ dữ liệu trong 1 năm thì cần tối thiểu 246TB để đảm bảo dung lượng bộ nhớ, tính toán vẹn của dữ liệu.

### 2.6.2 Tính toán về bandwidth (băng thông) và Throughput (thông lượng)

- Hệ thống camera giám sát hoạt động 24/7 sẽ lưu trữ dữ liệu trực tiếp về máy chủ trung tâm qua mạng wifi với tốc độ truyền tải 100Mbps.
- Bất kỳ thiết bị điện tử nào có thể kết nối internet bằng wifi như điện thoại thông minh, máy tính bảng,... sẽ có tốc độ tối đa là 256Kbps khi kết nối với kết nối không dây giống như kết nối cảm biến trong khoảng thời gian từ 7h30 đến 17h30.
- Máy tính tại các phòng học mỗi ngày tải khoảng 200MB vào khung giờ cao điểm từ 7h đến 17h30. Tổng thời gian cao điểm là 10.5h. Tầng 6, 7 sẽ có 6 phòng máy tính và mỗi phòng sẽ có 32 máy tính. Vậy có tổng tất cả 192 máy tính. Giả sử thời gian làm việc trong 1 ngày là 12h và giờ cao điểm trao đổi chiếm 80% dữ liệu trong ngày. Ta có:

$$\text{bandwidth} = \frac{200 * 192 * 8 * 0.8}{10.5 * 3600} = 6.5020 \text{ Mbps}$$
$$\text{throughput} = \frac{200 * 192 * 8}{12 * 3600} = 7.111 \text{ Mbps}$$

- Văn phòng hành chính sẽ có 10 máy tính Các máy tính mỗi ngày tải khoảng 200MB vào các khung giờ cao điểm là 8h-11h40 và 13h-16h30. Tổng thời gian cao điểm là 43/6h. Và gửi 10 email mỗi ngày với dung lượng tối đa 10MB/email. Giả sử thời gian làm việc trong 1 ngày là 12h và giờ cao điểm trao đổi chiếm 80% dữ liệu trong ngày. Ta có:

$$\text{bandwidth} = \frac{200 * 10 * 8 * 0.8}{43/6 * 3600} = 0.496 \text{ Mbps}$$
$$\text{throughput} = \frac{200 * 10 * 8}{12 * 3600} = 0.370 \text{ Mbps}$$

Với Email, ta có:

$$\text{throughput} = \frac{10 * 10 * 8}{12 * 3600} = 0.019 \text{ Mbps}$$

- Mỗi phòng lớn có 6 cảm biến nhiệt độ, 6 cảm biến ánh sáng, mỗi phòng nhỏ có 3 cảm biến nhiệt độ, 3 cảm biến ánh sáng. Tầng 2 đến tầng 5 sẽ chỉ có phòng thường với 6 phòng nhỏ, 3 phòng lớn. Tầng 1 ngoài 2 loại phòng trên sẽ có 1 phòng máy chủ, tầng 6 và 7 sẽ có 4 phòng nhỏ, 2 phòng lớn, 3 phòng vi tính. Vậy có tổng tất cả là 456 cảm biến. Một cảm biến sẽ đo một chỉ số khác nhau kích thước định dạng dữ liệu của chúng là 32 Kb. Các cảm biến sẽ thu thập dữ liệu một phút một lần và sau 5 phút, chúng sẽ gửi dữ liệu này đến máy chủ trung tâm qua mạng WIFI. Nên ta có:

$$\text{throughput} = \frac{0.032 * 456 * 8}{300} = 0.389 \text{ Mbps}$$

## 2.7 Đánh giá hệ thống

### 2.7.1 Bảo mật

#### 2.7.1.1 Phân tích yêu cầu

Hoạt động của trường đại học luôn có một lượng lớn thông tin được xử lý theo thời gian thực. Tuy nhiên, không phải ai cũng có quyền truy cập vào các thông tin này. Vì vậy, trường đại học có nhu cầu xây dựng một hệ thống an toàn cho mạng máy tính để phục vụ cho vận hành. Hệ thống bảo mật này phải đảm bảo:



- Không được quyền thay đổi cấu trúc mạng, trừ khi được ủy quyền
- Chống được các truy cập bất hợp pháp từ bên ngoài
- Kiểm soát được lượng truy cập
- Đảm bảo được việc an toàn cho thông tin khi được truyền đi cũng như nhận vào
- Các dữ liệu "nhạy cảm" phải được giữ bảo mật ngay cả khi bị tấn công

#### 2.7.1.2 Hướng giải quyết được đề xuất

- Tăng cường bảo vệ và bảo mật cho các thiết bị mạng như switch và router.
- Backup các thông tin quan trọng
- Bảo vệ tuyệt đối cho database server
- Thiết lập Firewall và cấu hình ACL phù hợp

#### 2.7.2 Những vấn đề chưa giải quyết

- Vì là thiết kế dựa trên lý thuyết là chủ yếu nên chưa đảm bảo tính đúng đắn với thực tế 100%
- Giá cả các thiết bị cao (tuy nhiên đảm bảo được chất lượng tốt do được thiết kế bởi hãng cisco)
- Chưa có dữ liệu về khoảng cách địa lý, kết cấu tòa nhà (tường, tầng,...) nên chưa thể tính toán chi phí cho dây nối.
- Chưa có sự bảo mật dành cho database server nên có thể dễ bị tấn công từ bên ngoài

#### 2.7.3 Các bước tiếp theo

- Phát triển hệ thống bảo mật: có thể thêm lớp DMZ để giảm thiểu tải
- Khảo sát chi tiết về kiến trúc tòa nhà và khoảng cách các tầng để thực hiện lắp dây
- Tìm kiếm định hướng khi hệ thống mạng H6 mở rộng hơn nữa