Pilates by Raina Network Architecture

TAC 357- Final Project

1. Executive Summary

Pilates by Raina is a new small fitness boutique studio planning to open in Los Angeles. This studio plans to expand operations to two new locations by the end of its first year. For the business to expand according to plan, this studio requires a well-budgeted, secure, and scalable network infrastructure. This network must be able to aggregate all staff workstations, sales systems, security equipment, client Wi-Fi, and IoT-enabled reformer machines. Pilates by Raina also plans to use a cloud-based service to let customers book classes online and store files. This network architecture plan outlines the required wireless and routing design, VLAN segmentation, cloud service, and the security plan. This report also proposes the required hardware and software costs. A packet tracer demonstration will also be included to simulate the studio network plan.

2. Business Operations and Technological Requirements

2.1 Business Operations Description

Pilates by Raina is a boutique fitness studio opening its first location in Los Angeles. It plans to open two satellite locations in the Los Angeles area within the first year of opening its central location. The studio will include IoT-enabled reformer Pilates machines, a client reception check-in area, and a staff operations back room. Bookings for classes at this studio will be using a cloud-based booking platform that clients can use to schedule and pay for classes online.

2.2 Operation Logistics

For the business to build a secure network, it requires specific operational requirements to support its infrastructure and meet business operations.

- **Staff Equipment:** This will include office computers, a check-in desk tablet, and laptops for creating schedules, communication, client check-in, and back-office administrative tasks.
- **Point-of-Sale (POS) systems:** It is crucial to have a POS system that supports secure online transactions for clients and complies with the Payment Card Industry Data Security Standards (PCI DSS). This protects the studio and clients from fraud and also tracks sales records.
- **IoT-enabled Reformers:** These reformers come equipped with sensors that track and record physical movement, such as resistance and reps completed on the machine, and require a stable Wi-Fi connection to aggregate all that data to a single device attached to the network.
- **Security cameras (CCTV):** The studio will require two PoE CCTV cameras with cloud-based backup to ensure client safety and network security.
- **Client Wi-Fi:** The client Wi-Fi network must be a separate, high-traffic wireless network used only for client needs and not for operational purposes.
- **Cloud booking platform:** the interface for clients to book classes, which must be connected to the database backend system for class schedules, client information, accounts, and payment methods.
- **Staff VPN access:** Remote access needs to be implemented for studio employees for off-site work and during emergencies.

- **Redundant internet:** dual-WAN needs to be implemented as a network redundancy solution to prevent internet disruption and protect business profits, since clients cannot book if one system is down.

2.3 Security and Scalability Requirements

Since this boutique studio handles a lot of sensitive information, such as client information, payment methods, and IoT Reformers that collect data, the network must be structured to isolate different kinds of data and allow for scalability in the future.

- **Network segmentation:** VLANs must be implemented to segment the network into multiple networks for Staff, POS, IoT, CCTV, Guest, and the management server. The VLAN will have strict inter-VLAN firewalls to keep these networks with different information separate, safe, and organized.
- **High uptime:** Redundant internet service provider to ensure constant and stable network operations for the booking system, reformer machines, and studio operations.
- **Scalable Cloud Architecture:** The cloud service provider needs to handle thousands of client records and booking requests while maintaining a record of them as the studio expands to other locations.
- **Monitoring and Data Protection:** live visibility of the network health, Wi-Fi performance, cloud uptime, and device status. Ensuring backups, encrypted connections, and secure storage for camera data and client information.
- **Scalability:** The next two studios to open need to be easily integrated by the leading studio network through a design that allows adding a new VLAN, a scalable cloud service provider, and studio-to-studio VPN connections.

3. Logical Network Segmentation (Technical)

3.1 Network Topology

The network will have a star-shaped topology that is hierarchically organized, which is based on Cisco's enterprise design model, meaning these will be the components:

1) One edge/gateway router (handles internet, routing, VPN)
2) One core/access switch (PoE, VLAN-aware, connects all local devices)
3) Wireless access points for staff and guest Wi-Fi
4) Separate logical networks (VLANs) for Staff, POS, IoT, CCTV, Guest, and Management server.
5) Cloud connectivity for the booking platform, payment processing, and remote access.

Traffic flows from endpoint devices to the access switch, then to the router, and finally to the cloud. Inter-VLAN communication is achieved via router-on-a-stick using subinterfaces on the gateway router.

3.2 VLAN Segmentation

VLAN ID	VLAN NAME	Usage	Linked Devices
10	Staff	Employee computers, instructor tablets, office laptops	Staff devices and workstations
20	POS	PCI-compliant payment terminals	Checkout register, POS device
30	IoT	Data from reformers	Iot Reformers
40	Guest	Guest Wifi	Client phones
50	CCTV	Studio Surveillance	IP cameras
99	Management (Mgmt)	Network controls and management	Router, switch, AP

Having this VLAN segmentation ensures that guests on the network cannot access networks used for studio operations, and that the payment processor doesn't interfere with other networks.

3.3 IP Addressing

Each VLAN will have its own IP subnet, enabling easy differentiation and scaling to meet business needs. The subnets will use a /24 CIDR subnet for simplicity and its ability to host 254 IP addresses per subnet. Using a /24 subnet also makes it easier for staff to manage networks, allowing space for network growth. It is the best practice for small businesses, not wasteful, and still flexible.

IP Addressing Plan per VLAN will look like:

VLAN ID	VLAN NAME	Subent	Default Gateway
10	Staff	192.168.10.0/24	192.168.10.1
20	POS	192.168.20.0/24	192.168.20.1
30	IoT	192.168.30.0/24	192.168.30.1
40	Guest	192.168.40.0/24	192.168.40.1
50	CCTV	192.168.50.0/24	192.168.50.1
99	Management (Mgmt)	192.168.99.0/24	192.168.99.1

3.4 Default Gateways and Inter-Vlan routing Default Gateways

Each VLAN will have its own default gateway for its subnet, configured on the router's subinterfaces. An example of this encoding is configuring the router like so for the Staff VLAN

```
interface g0/0.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0
```

This creates an interface for each VLAN on the router and configures it according to its IP address.

For inter-VLAN routing, which allows data to move between different VLANs on a single network, the router-on-a-stick method will be used, dividing a router's interface into subinterfaces based on the VLANs created. This is a cost-friendly method for a small business, and it allows for broadcast domains, which are network segments, to be clearly separated.

4. Physical Network

4.1 Hardware

The physical network components of the studio will need the following hardware:

- One Gateway Router
  - This router will be the direct connection to the internet service provider and the default gateway for all VLANs created for the separate studio functions discussed earlier, such as the staff and guest VLANs.
- One Layer Two PoE Access Switch
  - The switch provides the wire connections to all the end devices on the network, such as CCTV cameras and Wi-Fi access points.
  - The switch is demonstrated in the model diagram discussed in section 6, which shows a Cisco 2960 switch.
- One Wireless Access Point Router
  - This device is responsible for broadcasting the staff and guest Wi-Fi networks, and each is mapped to its respective VLAN: the staff one to the Staff VLAN and the guest one to the Guest VLAN.
  - The wireless access point is modeled in the Section 6 demo as a device named WRT300N.

Aside from the hardware for the physical network topology, the end devices that will be integrated into the network are the following:

- Two Staff PC's
  - One will be used at the front desk for check-in and one for office back-room operations.
- One POS Terminal Device
  - This device is part of the POS VLAN and is modeled as a PC in section 6, which is responsible for securing end-to-end payments.
- One IoT Device
  - This device is an IoT Control Hub device. Since the reformer studio has eight reformers that come with pre-attached and sensores the data of each reformer will aggregate to the Iot Control Hub according to the reformer machine number and its own data which stores it all in one place simplifying the data collection into one IoT VLAN instead of a separate one for each reformer machine.

- Two CCTV Cameras
    - The two cameras are modeled as two PCs in the demo in Section 6. These are the end devices that aggregate data to the CCTV VLAN.
- One Management Server
    - This server device provides the services required, such as DNS and DHCP.

4.2 Cabaling Plan

The studio network will use standard Ethernet cables to connect all the network components. The cable connection plan is the following:

- Router to Switch Connection
    - The router used, which is a Cisco 2911 router, connects to the switch through its GigabitEthernet0/0 port, which has a 1 Gbps transmission speed, and helps carry all the traffic from the inter-VLAN routing to the Cisco 2960 switch to the Fa0/24 port of the switch, which is a 100 Mbps speed switch port for the access layer. The Fa0/24 port on this switch is configured as a trunk port, which aggregates traffic from all VLANs and enables inter-VLAN communication.
- Switch to End Devices
    - All switch-to-end device connections will also use a straight-through copper cable that connects through the switch's Fast Ethernet ports.

4.3. Wireless Connection Plan

Regarding the wireless access point (Wi-Fi), it will show two service set identifiers (SSIDs): guest Wi-Fi and staff Wi-Fi.

- SSID 1: PilatesbyRaina_STAFF
    - This wireless network is connected to VLAN 10, which is for staff, and it will be WPA3-secured, which strongly encrypts and protects data flowing on that network, since it is only used by staff.
- SSID 2: PilatesbyRaina_GUEST
    - This wireless network is connected to VLAN 40, which is for guests and configured with client isolation, so it does not interfere with the operations network.

4.4 Port Connections and Device Placement Plan

To summarize the studio's port connections for all end devices and where they are placed, this table summarizes how this will be executed:

Device	VLAN	Switch Port	Placement
Staff PC 1	10 - Staff	Fa0/1	This PC will be at the front desk and is used to check clients in, handle business inquiries, and assist clients.
Staff PC 2	10 - Staff	Fa0/2	This PC will be inside the office room and will be used for studio management, business plans, and operations information
POS Terminal	20 - POS	Fa0/4	A payment system that is a device at the front desk and is also linked with payments happening on online bookings
IoT Device	30 - IoT	Fa0/5	This collects all sensor data from the reformers and integrates the data into its respective VLAN on the network
CCTV 1	50 - CCTV	Fa0/6	Security camera placed inside the studio
CCTV 2	50 - CCTV	Fa0/7	A security camera placed on the entrance
Managemnt server	90 - Mgmt	Fa0/8	Management operations storage server placed in the office
WRT300N AP1	40 - Guest	Fa0/9	Access point for guest and staff wifi
Router 2911	Trunk	Fa0/24 (Trunk)	Holds VLANs 10, 20, 30, 40, 50, 99

5. Cloud Service Plan

For clients to book classes online, the studio will use a cloud-hosted booking system from AWS to ensure high availability and scalability.

5.1 Client Application, Database, and Security

The application, which will include the daily Pilates class schedule and availability, will be configured using an AWS Lightsail App Instance, which allows an app to be created for the booking portal and schedule and linked to the payment integrator established in the studio's POS system. This service has 2 vCPUs, 8 GB of RAM, and 160 GB of SSD storage, making it highly scalable and efficient.

Regarding the database that will be integrated into the application, the studio will use AWS Lightsail Managed MySQL/PostgreSQL. This database server automatically backs up daily and is Multi-AZ and highly available, meaning it has multiple available zones in case of failure, since it always has a standby copy of the data that can be restored to other areas of the system. The data stored in this database will include client profiles, instructor availability, membership information (such as classes used and remaining in a client's package), payment methods saved on client accounts, and class reservations (future and past).

Cloudflare will provide security for the following databases and information. This service can be integrated with AWS configurations, and it will ensure DDoS protection to prevent attacks on the system. Through Cloudflare and AWS protocols, they will guarantee TLS encryption, identity and access management controls, and automatic patching in the cloud.

5.2 Cloud Storage

All files related to administrative tasks and studio operations will be stored in the cloud for accessibility. The following services will be used to secure files.

- AWS S3 Buckets
  - This service will store all studio monthly reports, like payrolls, market, and management documents.
  - This service will store recently accessed files and automatically archive them to the S3 Glacier AWS service.
- AWS S3 Glaceir

    - This service is used for archival documents that always need ot be kept but not accessed frequently, like CCTV snapshots, legal and financial records, logs of previous cash flow, and old booking records.
- Studio-Cloud Sync
    - This is a business operations service that syncs physical business operations to the cloud. This service will be used on the local management server in the physical studio network to sync and report back to the AWS Sand, ensuring data security and preventing data loss by enabling recovery and dual access points for daily studio operations.

5.3 Domain Name System and SSL

The studio will use DNS hosting via AWS Route 53, a DNS web service that handles IP address translation. This is crucial to ensure the app's health is always secure and to plan for routine failures. SSL certificates, which AWS issues to authenticate identities in an application and ensure encrypted connections between the web server and the user's browser, are an industry standard and are always required for a secure app, as they use AES-256 encryption.

5.4 Cloud Monitoring and Network Services

Since the cloud will have critical files and information, it is essential to note that through using AWS and Cloudflare, there are included monitoring protocols which will be used as part of the service:

- AWS CloudWatch
    - This is integrated with AWS services and tracks, logs, and reports CPU, storage availability, and RAM usage. It also alerts when utilization exceeds capacity and tracks whether the database is performing accurately.
- Cloudflare Analytics
    - Cloudflare services include a built-in analytics service that monitors web traffic, blocks unsafe IP addresses, provides live threat alerts, and uses caching to speed up client access.

In terms of services that the studio will also use to monitor the physical network, they will be:

- DHCP
    - Dynamic Host Configuration Protocol will be configured in the router in the studio, which will secure the VLANs linked to the router and ensure dynamic addressing for all end devices, making IPs constantly changing and less likely to be attacked.

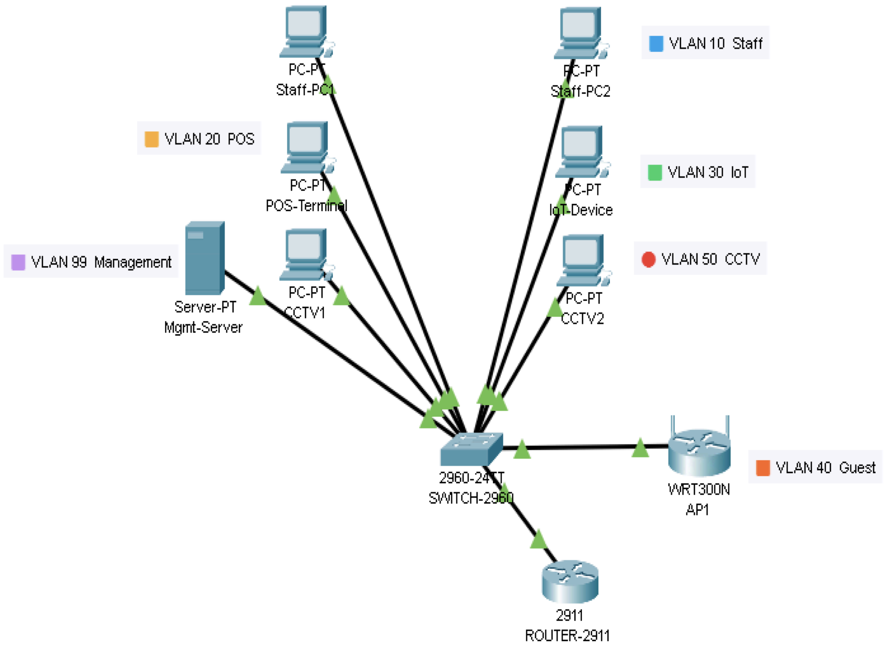
- Internal DNS
    - The router manages this in the studio and ensures that internal networks, especially ones like those for management and staff, are secure and can be efficiently managed.
- NAT
    - The router will be configured to perform NAT, meaning it uses a single public IP address for multiple devices on a private network to access the internet, so the internal network can be better protected since outbound private IPs aren't displayed on the web.
- VPN
    - VPN will be used for remote access processes that occur outside the studio, and traffic will be encrypted using IPSec, which guarantees maximum security. Only VLAN 99 has access, protecting other VLANs from being accessed outside the studio.

6. Physical Studio Network Packet Tracer Demonstration

To fully envision the logical and physical setup of the studio's network, a Packet Tracer demonstration was created to show how all devices on the network connect visually. This demonstration is configured according to the devices used: a Cisco 2911 router and a Cisco 2960 PoE switch, and, for each VLAN, a trunk link is configured to demonstrate the router-on-a-stick model.

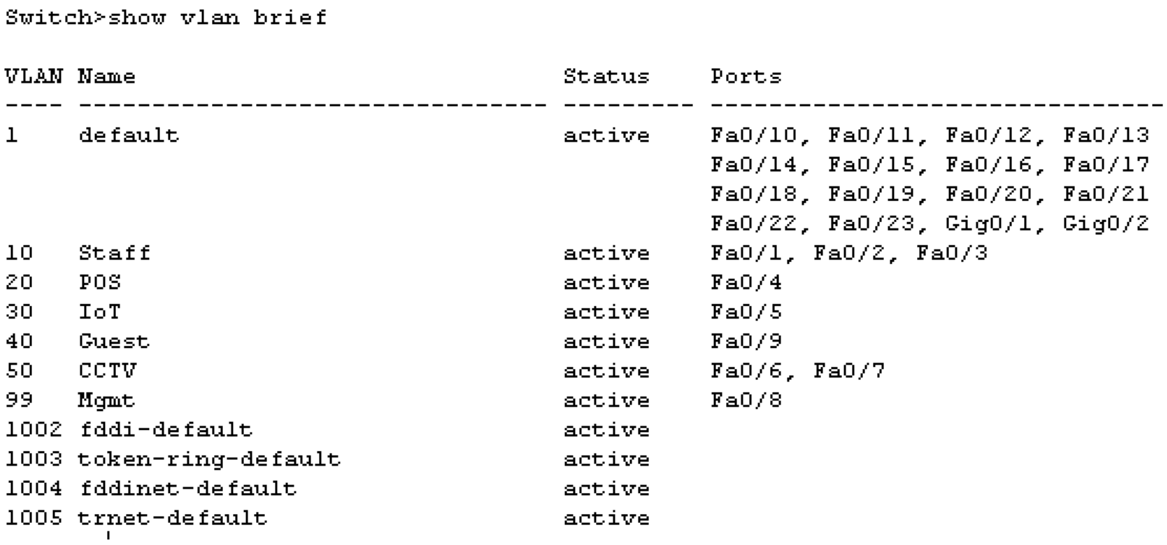
6.1 Physical Topology

The following diagram shows the physical network discussed in Section 4. This demo shows the router, which handles inter-VLAN routing, DHCP, and NAT, and serves as the network's default gateway. Then it is connected to the switch, which serves as the access layer for the labeled VLANS. The end devices for each VLAN can be seen like the two staff computers in VLAN 10, POS terminal in VLAN 20, IoT device is VLAN 30, the wireless router for the guest and staff wifi in VLAN 40, the two CCTV cameras in VLAN 50 and the management server in VLAN 99 with it all being connected to the trunk which is the router through the switch.



6.2 VLAN and Router Configuration

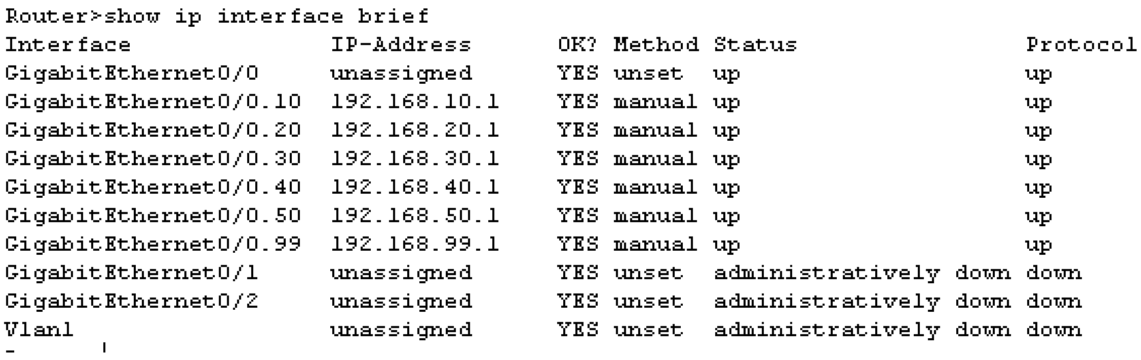
The packet tracer demo was also configured according to the VLAN segmentation plan and the way each VLAN is connected to specific Fast Ethernet ports on the switch. The table below shows the switches' command prompt output, showing how the VLANS are configured to be separate from their end devices on the switch, as discussed in section 4. The figure at the bottom represents how the router was configured according to the



```
Switch>show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Gig0/1, Gig0/2
10   Staff                            active    Fa0/1, Fa0/2, Fa0/3
20   POS                              active    Fa0/4
30   IoT                              active    Fa0/5
40   Guest                            active    Fa0/9
50   CCTV                             active    Fa0/6, Fa0/7
99   Mgmt                             active    Fa0/8
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

The figure below shows how the router was configured to allow for inter-VLAN routing as planned. Every subinterface had the correct IP address for its VLAN's default gateway. Also, every subinterface shows as up and running, indicating that inter-VLAN operations are working; GigabitEthernet 0/0 is up, meaning the trunk is receiving all traffic from the VLANs.



```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.30.1    YES manual up                    up
GigabitEthernet0/0.40  192.168.40.1    YES manual up                    up
GigabitEthernet0/0.50  192.168.50.1    YES manual up                    up
GigabitEthernet0/0.99  192.168.99.1    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

6.3 Testing Connectivity

To further prove the functionality of this network design plan, the connectivity of Staff-PC1 was tested to see if it can communicate with all other devices across the network VLANs through a ping test, which demonstrated that each ping was successful, as seen below, meaning network connectivity and traffic can flow through the network segmentations. This command output is by Staff-PC1 to the different end devices' IP addresses.

C:\>ping 192.168.10.11 Pinging 192.168.10.11 with 32 bytes of data: Reply from 192.168.10.11: bytes=32 time=3ms TTL=128 Reply from 192.168.10.11: bytes=32 time<1ms TTL=128 Reply from 192.168.10.11: bytes=32 time<1ms TTL=128 Reply from 192.168.10.11: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.10.11: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 3ms, Average = 0ms	C:\>ping 192.168.10.1 Pinging 192.168.10.1 with 32 bytes of data: Reply from 192.168.10.1: bytes=32 time<1ms TTL=255 Reply from 192.168.10.1: bytes=32 time<1ms TTL=255 Reply from 192.168.10.1: bytes=32 time<1ms TTL=255 Reply from 192.168.10.1: bytes=32 time<1ms TTL=255 Ping statistics for 192.168.10.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.20.10 Pinging 192.168.20.10 with 32 bytes of data: Request timed out. Reply from 192.168.20.10: bytes=32 time<1ms TTL=127 Reply from 192.168.20.10: bytes=32 time<1ms TTL=127 Reply from 192.168.20.10: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.20.10: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms	C:\>ping 192.168.50.10 Pinging 192.168.50.10 with 32 bytes of data: Request timed out. Reply from 192.168.50.10: bytes=32 time<1ms TTL=127 Reply from 192.168.50.10: bytes=32 time<1ms TTL=127 Reply from 192.168.50.10: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.50.10: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

7. Storage Plan

Although the cloud will be used to store critical business documents, such as customer information and administrative documents that are discussed in section 5, the studio will have a hybrid approach of storing CCTV recordings and daily operations files locally in the physical network of the studio rather than the cloud, which allows for storage to be more scalable and cost-efficient.

7.1 Daily Operation Files Storage Plan

Since the studio requires string constantly renewing documents such as class schedules, daily reports, training packets, inventory and stock update logs in order to merge these locally stored files in the physical network and the cloud a local network attached storage file also known as NAS will be attached to the management server in the studio that is VLAN 99 which allows for files from the studio to be shared on the cloud but it will be configured to only be accessible by the Staff VLAN to ensure security. The NAS folder will follow the server message block (SMB) protocol which lets computers on the same network be able to share files and since this links these files on the cloud they will also be backed up like the files on the cloud through the AWS S3 service. This approach allows employees to constantly access important documents without slowing down the cloud with too many requests.

7.2 CCTV Storage Plan

Since CCTV recordings take up an alot of space and bandwidth, they will be saved locally. The studio's network will attach a local network video recorder (NVR), which stores CCTV footage, to the CCTV VLAN 50. The NVR will have around 4 TB of storage and can retain footage for about 45 days.

To keep more permanent records of CCTV footage, the preconfigured cloud will be used to store weekly footage snapshots and summaries from the NVR device to the AWS S3 Glacier service, which archives these non-frequently accessed files for compliance and record purposes in case of any incidents.

7.3 General Studio Storage Capacity Requirements

Since the studio will require storage on-premises and on the cloud, this table summarizes the storage GB requirements for all data being stored for the studio.

Type of Storage	Estimated Size	Contents of Storage
Cloud Service Booking Database	10-12 GB	Customer data (profiles and saved information) and Scheduling Files
Cloud Saved Businesses Files	30-50 GB	Administrative, legal, and business operation documents
Local Network Attached Storage (NAS)	40-60 GB	Daily accessed files for running the studio
CCTV Recordings	4TB	NVR recordings from the 2 CCTV cameras in the studio
Cloud Archived Files	Varies based on the number of archived files	CCTV Snapshots and rarely accessed files were moved from the AWS S3 Bucket to Glacier

8. Cost Plan

After providing an overview of all the physical components and cloud services needed to build this secure network, this section outlines the costs of crafting it, including required hardware, network infrastructure, cloud services, security, and labor to assemble it. The cost plan ensures typical market prices, allowing for a high level of security and the ability to expand the business to other studio locations in a seamless way.

8.1 Hardware Costs for Physical Studio Network

Item	Quantity	Item Cost	Total Cost	Purpose
Cisco 2911 Router	1	$4,311.00	$4,311.0	The core router of the network that allows inter-VLAN routing
Cisco 2960 Switch (24-port)	1	$699.99	$699.99	Segments the VLANS's
Staff PC's	2	$939.99	$939.99	Front desk and office PC's
POS Device	1	$459.00	$459.00	Shopify POS Terminal Countertop Kit PCI compliant payment device for in-studio purchases
IoT Device	1	$800	$800	An Android tablet that connects to the sensors on the reformers and aggregates all data on its interface
CCTV Cameras	2	$189.99	$379.98	Security cameras in the studio
Local NVR Machine	1	$449.99	$449.99	CCTV Recording Device
Wireless Acess Point	1	$150	$150	Guest Wifi Network
Network Cables	1 (cable package)	$169.99	$169.99	CAT6A network patch pane and cable package

The total hardware cost is $8,359.94, a one-time cost.

8.2 Cloud Infrastructure Cost

The studio's cloud infrastructure is used for booking and critical document storage, which AWS will provide through two services.

Booking Platform and Database Service Requirements & Costs - AWS Lightsail

Service	Monthly Cost	Annual Cost	Purpose
Lightsail App Hosting (Medium Instance)	$40	$480	Creates a booking site and makes API endpoints (URLs)
Managed MySQL Database (Medium)	$50	$600	Database for clients, payment methods, and classes
Load Balancer (Optional Future)	$10	$120	Ensures redundancy in case the platform needs to expand

Total Cloud Infrastructure $1,200.00 annually.

Aside from required cloud services for the booking platform, the cloud services are also required to store critical studio documents. This table goes over the cloud storage services and prices for AWS 3.

Service	Monthly Cost	Annual Cost	Purpose
Operational Document Storage S3 Standard 50 GB	$1.15	$14	Stores business files on the cloud
Daily Backups S3 Standard 100 GB	$2.30	$28	Stores the local data base daily snapshots and NAS device snapshots
CCTV Archival S3 Glacier 500 GB	$2.00	$24	Stores the weekly snapshots from the CCTV cameras to AWS Glacier

Total cloud storage services are $66.00 annually.

8.3 Internet Service Provider Cost

To run the CCTVs, POS, and booking platform smoothly, these are the costs for highly redundant internet.

Service	Monthly Cost	Annual Cost	Purpose
Bussniess Fiber Wifi	$130	$1560	The leading internet to run studio operations
Backup Cable	$70	$840	Cable used for automatic failover response

Total Internet service provider costs are $2400.00 annually.

8.4 Labor Cost

Since the network has different components that need to be installed this table factors in the labor fees of installing each part of the network. This is assuming the network will be installed by an IT consulting firm that takes the typical business hourly rate of $120 for small business in 2025.

Task	Required Hours	Hourly Rate	Total Cost
Network Design Plan and Documentation Records	10	$120/hr	$1200
Hardware Installation with Cables	8	$120/hr	$960
Routing set up (including VLAN segmentation and firewalls)	5	$120/hr	$600
Cloud Infastcture Set Up	3	$120/hr	$360
CCTV and NVR Installation + Configuration	4	$120/hr	$480
Network Tests and Troubleshooting Service	5	$120/hr	$600

Total labor cost is $4320.00, one-time cost.

8.5 Total Costs Combined

Network Componenet	**Cost**
Hardware	**$8,359.94**
Cloud Infastrcture	**$1,266.00**
Internet Service Provider	**$2400.00**
Labor Cost	**$4320.00**

This totals the first-year cost of opening the studio, including all network components, to **$16,345.94.** This price guarantees opening a studio with a network that is not only secure but also aligns with the long-term goals of expanding the studio, meaning initial investment in a network that is easily and affordably expandable was a critical factor in configuring the design.

9. Expansion and Scalability Plan

9.1 Customer Number Expansion Plan

Before planning to expand the network to other studio locations, the customer numbers will grow significantly from the first month of opening through the first year. Increased customer growth will affect the booking platform's request load, database size, storage, and Wi-Fi connections. To mitigate that expansion, the only changes needed are through AWS Lightsail, which is used for booking and file storage, and can have its CPU increased. AWS Lightsail allows adding a new instance, which enables more requests to run smoothly on the booking platform, and the database automatically adjusts based on the client accounts created. AWS Lightsail offers 256 GB of memory and 64 GB of CPU, with multi-core CPUs, which can easily handle this customer's expansion.

9.2 Network Scaling

The internal network will need to be scaled as more clients and staff come into the studio, meaning it needs to handle more clients on the Wi-Fi, additional staff devices, additional sensors added to the IoT device, and possibly CCTV recordings and cameras. Scaling the network to this need will be simple due to the preconfigured VLAN scheme, meaning only new switch ports will be needed to add devices to the VLANs. The CISCO 2960 switch already has 24 switch ports, and if more are needed, another CISCO 2960 can be stacked on top of the existing one to support more switch ports and connect more end devices. Regarding Wi-Fi, new access points can be added to the Guest VLAN 40 or the Staff VLAN 10 as needed, without changing the routing mechanism.

9.3 Scaling the Network to New Studio Locations

The network is built so it can expand simply when the next two studios open in different locations. The network can be adapted to other studios through a site-to-site VPN, which connects the main studio to the other two branches, and uses an IPsec tunnel to create a secure connection for data to move between the CISCO routers at each studio. Since the booking platform is in the cloud, it won't need to be adapted in each studio; the only requirement is that CCTV footage for each studio is stored locally in the NVR. Each studio location will still use the same physical hardware, including the router-on-a-stick, VLAN segmentation, Cloud connection, and CCTV storage.

9.4 Scaling Cost

Since the studio uses a hybrid physical and cloud network, the costs associated with expansion would be limited to the physical hardware discussed in section 8.1 when a new studio opens. Regarding the cloud infrastructure, the cost will only increase slightly to support additional storage for dividing files by studio location, but the services will remain the same. The approximate cost of opening each new studio location will be $8,359.94 for the hardware.

10. Security and Recovery Plan

With all the network aspects explained, this section explains how security is heavily implemented and underpins specific segmentation, and discusses how recovery of any data in the event of accidents or breaches will be handled.

10.1 VLAN Segmentation Security

The VLAN segmentation simplifies network operations and divides them, but it is a core aspect of the studio's security. The six VLANS are created to isolate sensitive systems that can cause issues if they interact, and that is why, in the VLAN configuration, inter-VLAN communication is put in restricted mode by default and only allowed in some instances, and that is why the guest wifi access point is entirely separate and not attached to the VLANs.

10.2 Router and Firewall Security

The network uses Access Control Lists (ACLs), which determine who can access parts of the network to ensure that the IoT VLAN can not access the Staff VLAN, the guest VLAN can not access any other VLAN, the POS VLAN cannot access the Guest or IoT VLAN, and the management VLAN can only reach the CCTV and NVR system. Also, all management interfaces require administrative authentication, and the router is configured to use SSH (secure shell) instead of telnet as its remote access protocol, since it implements encryption and authentication. All these restrictions grant the least privilege to all network segments.

10.3 Cloud Security

The reason AWS services are selected for booking and file storage in terms of security is that they use Hypertext Transfer Protocol Secure (HTTPS), which encrypts all data from the browser to the website. AWS also uses IAM roles to designate who can access the cloud. In terms of Cloudflare, it has distributed denial-of-service (DDoS) protection, which prevents attacks on the network for all the public-facing servers. Also, the database is encrypted using the industry-standard AES-256, and AWS automatically applies security patches.

10.4 Device Security

All staff PC's and the management server have anti-malware software and will constantly have the operating system updated. All devices must comply with a firm password policy and have device-level firewalls enabled, which all reduce the chances of malware or unauthorized access.

10.5 Physical Security

Part of network security is ensuring that physical security measures are in place, which is why CCTV cameras are placed at the entrances and at full view of the studio, the POS device will have a camera over it, and the NVR will be stored in a locked cabinet in the back office. The patch panels and router will also be placed securely within camera view and securely in the backroom.

10.6 Recovery Plan

Incidents and failures are always possible, and in the event of any equipment outages or failures, the cloud is always performing backups; the NVR device can always be replicated because of the snapshots it saves in the cloud. The internet service redundancy ensures operations can always keep running with the backup cable. The router and switch configurations will always be backed up and saved as text files, allowing them to be redeployed.

Resources Used

- https://cloudchipr.com/blog/aws-lightsail
- https://cheatsheetseries.owasp.org/cheatsheets/Network_Segmentation_Cheat_Sheet.html
- https://www.router-switch.com/tag/cisco+2911
- https://www.newfanglednetworks.com/products/cisco-catalyst-2960s-f24ts-s-switch?variant=14265281052716&country=US&currency=USD&utm_medium=product_sync&utm_source=google&utm_content=sag_organic&utm_campaign=sag_organic&srsltid=AfmBOoq3LADtMzW3YdMYMNnHQga2u-COiSiw1KHGVwNjxXzFq6tAesbB0G0
- https://www.hp.com/us-en/shop/pdp/hp-all-in-one-24-cr1000t-238-9p2v3av-1?s_kwcid=AL!20144!3!!!!x!!&gclsrc=aw.ds&jumpid=cs_con_nc_ns&utm_medium=cs&utm_source=ga&utm_campaign=US_CPS-bu_PMAX_Mix_dal_Other_Google-s_IC_ENG_CM016876_Bestseller&utm_content=sp&adid=&addisttype=xpla_with_promotion&9P2V3AV_1&cq_src=google_ads&cq_cmp=20552066544&cq_con=&cq_term=&cq_med=pla_with_promotion&cq_plac=&cq_net=x&cq_pos=&cq_plt=gp&gad_source=1&gad_campaignid=19965637803&gbraid=0AAAAAD-ppXjt_qoZ60YhsijPDi48B4W4V&gclid=Cj0KCQiA_8TJBhDNARIsAPX5qxQ-wtX-Fwba4g7cwyQOt-16RMCX1QWJ6KjImKtUANCnp167qIMtuNMaAm9VEALw_wcB
- https://hardware.shopify.com/products/pos-terminal-countertop-kit-for-usb-c-tablets?variant=47765480996886&country=US&currency=USD&utm_source=google&utm_medium=cpc&utm_campaign=RetailPOS_Shopping_AMER_US_Hardware&campaignid=20029254666&term=&adid=734481676750&matchtype=&network=g&gad_source=1&gad_campaignid=20029254666&gbraid=0AAAAADeTQBAzweMNJwmxq3gXGz7uth6Jx&gclid=Cj0KCQiA_8TJBhDNARIsAPX5qxQ9gPbrajFg0y4PCBM4dP5hnU_igJF8OQx1TPxilXk2QqsvvBcLI1caAr5OEALw_wcB
- https://www.ptsmobile.com/ET40AA-001C1B0-NA.html?gad_source=1&gad_campaignid=10027524381&gbraid=0AAAAAD_p2zIchlwtnUYiKIbA13aqB9PU9&gclid=Cj0KCQiA_8TJBhDNARIsAPX5qxQsEWVTIkYHxhcDQ62c5gqvJCxM4SDe57E6Bxd4zy4NIef72QtO1hoaAg6mEALw_wcB
- https://reolink.com/product/reolink-duo-3-poe/
- https://www.angi.com/articles/ethernet-installation-cost.htm
- https://www.business.att.com/portfolios/business-internet.html