ASSIGNMENT -5

NAME : S.CH~~M~~ANDRA SIDDHARDHA.

REG NO :192525222

COURSE NAME : Computer Networks

COURSE CODE : CSA0735

COURSE FACULTY : Dr. Rajaram & Dr. Anand.

Topic : A Firm Ensures Email Access Across Devices.

Ensuring Secure Email Access across Devices.

scenario:

A company with 100 employees manages secure email access across multiple devices. Each employee handles an average of 10 MB of email data per day.

Parameters:

- Number of employees: 100
- Daily email data per employee: 10MB.

a) Differentiate POP3 vs IMAP in Functionality.

Feature	POP3 (Post office Protocol v3)	IMAP (Internet Messag access Protocol)
storage	Emails are downloaded and removed from server	Emails stay on t server
accessibility	Accessible from one device	synchronizes acro multiple devices
Folder support	Limited folder organization	Full support for ser side folders

b) estimate Monthly storage Required.

given

- 100 employees
- 10 MB emails per day per employee
- 30 days in a month.

calculation.

Total per day = 100 × 10 MB = 1000 MB = 1 GB

Monthly storage = 1 GB/day × 30 = 30 GB

Estimated Monthly storage : 30 GB

c) suggest TLS configuration for secure access

To insure secure email transmission the following TLS.

1. use TLS 1.2 or TLS 1.3 only.

   - older versions like TLS 1.0/1.1 are deprecated and insecure.

2. Enable SMTP, IMAP and POP3 over TLS

   - SMTP over TLS : Port 587.
   - IMAP over TLS : Port 993.
   - POP3 over TLS : Port 995.

3. use trusted SSL/TLS certificates

* Issued by a reliable certificate authority (CA)

d) Recommended an Anti-Phishing Policy.

1. User Awareness Training.

* Regular sessions to teach employees how to identify suspicious emails and links

2. Multi-factor Authentication.

* Adds an extra security layer to users email accounts

3. Report and Respond system.

* Encourage staff to report phishing attempts and have a defined process to respond.

4. Link and attachment scanning.

* Automatically scan embedded link and attachments for threats before opening.

Conclusion:

secure email access requires a combination of proper protocols, storage planning, encryption practices, and user vigilance. Implementing IMAP with TLS, monitoring storage growth and enforcing anti-phishing.