Configuring Public Wi-Fi in Libraries

Introduction

As digital access becomes increasingly essential, public libraries are evolving into community technology hubs. one key feature in this evolution is installation of public wi-fi, while offering free internet enhances the library's services it also presents, it also presents challenges related to security, network, performance, and user safty.

This project explores how to configure public wi-fi in libraries effectively, covering access control, content filtering, router placement, and prevention of unauthorised devices.

1. Open Access Vs. Password Secured Network

Open Access Network

Open Network allows user to connect without entering a password. While convient, they are also vulnerable to:

- Data interception (eg: Snooping or man in the middle attacks)
- Unauthorized Usage
- Reduced user accountability

There networks may be apporiate for very short-term or low-risk users, but they offer little to no protection for users or the library's internal systems.

Password-Secured Networks

Password Secured wi-Fi uses encryption protocols like WPA2 or WPA3, which offer:

- Better data security
- Access control
- Potential for usage tracking

Libraries can also implement a captive portal, where users must agree to terms or log in with a library card, ensuring responsible use while still maintaining accessibility.

Recommendation: Use Password Secured wi-fi with captive portal access for a secure and controlled public connection

2. Recommended Filtering Tools For Public Networks

Filtering tools are essential to prevent access to harmful or inappropiate websites and protect users from online threats

Top Filtering Tools

1. openDNS (cisco umbrella)

A cloud-based solution offering.

- Malware/phishing blocking
- Web content categorization
- Easy setup with DNS changes

2. cleanBrowsing

A DNS filtering tool with various modes (Family, Adult, Security):

- Simple setup
- Effective for child-safe environments

B. Pfsense with SquidGuard

A more advanced, open source firewall.

- Allows detailed contain filtering
- Requires network administration skills

A. FortiGuard web Filtering

A professional-grade, hardware integrated solution:

- Real time updates
- Suitable for large library systems

Recommendation: use open DNS or cleanbrowsing for libraries with limited IT resources

Large setup may benefit from pfSense or fortinet

1. Suggest Optimal Router Placement for Signal Coverage

Proper placement ensures strong, consistent coverage:

- Central Location: Placement routers centerally in the building to reduce dead zones
- Avoid Barriers: Keep away from thick walls, metal shelves, and microwave ovens
- Ceiling mount or High Placement: Improves signals propagation in open spaces like reading areas.
- Use Multiple Access Points (APs): For large libraries, use mesh networks or enterprise APs connected via ethernet backhaul.
- Conduct Site Survey: Use tools like Netspot or Ekahau to map coverage and adjust accordingly

4. Preventing Rogue Access Points

A rogue access point (AP) is an unauthorized device that connects to or mimics a legitimate networks, potentially allowing attackers to intercept data.

Steps to Prevent Rogue APs

1. Wireless Intrusion Detection / Prevention (WIDS / WIPS)
   - Monitors and blocks suspicious devices (eg: cisco Meraki, Aruba)
2. MAC Address Whitelisting
   - Only approved hardware can act as APs
3. 802.1X Authentication
   - Verifies devices through a centralized RADIUS server

4. Port Security and Physical Access control

- Disable unused ports and secure access closets

5. Routine Network Audits

- Use tools like kismet or Aircrak-ng to scan for rogue SSIDS

Recommendation: combine automated detection tools with strong physical and policies to maintain network integrity.

Conclusion

Public Wi Fi in libraries is a valuable service that promotes digital inclusion and learning. However, it must be deployed with attentation to security, content control, and performance. By choosing secured ones, implementing effective filtering. optimizing router placement, and proactively preventing rogue devices.

libraries can create a safe and reliable digital space for all users.