Wireless Local Area Network Design and Security Plan for an L Shaped Facility

Posted on September 13, 2018

Introduction

A wireless local area network for an L-shaped facility must provide reliable coverage without treating the building as one open rectangle. Corners, walls, metal fixtures, offices, meeting rooms, storage areas, and a food court can attenuate or reflect radio signals. A sound design therefore begins with a site survey and capacity estimate rather than with a fixed assumption that three access points will always be sufficient. The network must also protect client, employee, financial, and design information throughout its lifecycle (National Institute of Standards and Technology, 2012).

The original plan correctly identified the need for dual-band service, multiple access points, secure placement, user authentication, and staff training. However, several technical details require modernization. Channels 2, 5, and 10 overlap in the 2.4 GHz band and can create interference. WPA-PSK shared passwords and MAC-address filtering do not provide strong enterprise access control. A current plan should use centrally managed access points, non-overlapping channels, network segmentation, strong authentication, monitoring, and documented incident response (National Institute of Standards and Technology, 2012, 2020).

Facility Requirements and Risk Assessment

The L-shaped floor plan creates two radio-frequency problems. First, a signal placed near one end of the building may need to pass through several walls before reaching the other leg. Second, the inside corner may create a coverage shadow. The food court and meeting areas may have high client density, while records or design-custody areas may require tighter security. The network must therefore be designed for both coverage and capacity.

Before equipment is installed, the organization should document the floor plan, wall materials, ceiling heights, expected number of users, device types, application requirements, and locations of wired network closets. Voice, video conferencing, cloud applications, file transfers, and guest browsing have different performance needs. A predictive radio-frequency model should be followed by an onsite survey because building materials and interference sources may differ from drawings.

The risk assessment should identify data handled by the facility. Customer names, addresses, telephone numbers, account information, employee records, financial data, product drawings, and organizational plans require confidentiality and integrity. Availability is also important because a

network outage may stop meetings, transactions, printing, authentication, and access to shared files. Security controls should therefore address unauthorized access, interception, malware, rogue access points, denial of service, lost devices, and administrative misuse (National Institute of Standards and Technology, 2012).

Wireless Architecture for the L-Shaped Building

A reasonable starting design would place one access point in each major leg of the L and another near the corner or high-density shared area. The exact number should be confirmed by survey results. Access points should normally be ceiling-mounted in secure locations, positioned away from large metal objects, microwave ovens, and other sources of interference. Directional antennas may be useful in corridors or specialized spaces, but omnidirectional enterprise access points are often more appropriate for office coverage. Antenna choice should follow measured requirements rather than a general desire to keep the signal inside the walls.

The network should support both 2.4 GHz and 5 GHz, with 5 GHz preferred for capable devices because it offers more non-overlapping channels and usually less congestion. Newer equipment may also support 6 GHz where devices and regulations permit. The 2.4 GHz band should be retained for older or specialized devices that cannot use higher bands, but channel planning should use non-overlapping channels such as 1, 6, and 11 where applicable. Automatic radio-resource management can adjust channels and transmit power, but its decisions should be reviewed.

Transmit power should be balanced so that client devices can communicate in both directions. Increasing access-point power does not solve every coverage problem because a low-powered client may hear the access point but be unable to transmit back reliably. Excessive power can also increase co-channel interference and cause clients to remain connected to a distant access point. Additional access points at appropriate power are often better than a small number operating at maximum strength.

All access points should connect to the wired network through managed switches, preferably using Power over Ethernet. Central management allows consistent configuration, firmware updates, logging, radio optimization, and detection of unauthorized devices. Redundant switching, backup power for critical equipment, and documented replacement procedures improve availability.

Logical Network Segmentation

The wireless network should not place every user and device on one shared internal segment. Separate virtual LANs and security policies should be created for corporate users, guests, managed mobile devices, printers or operational equipment, and administrative management. Segmentation limits movement if one device is compromised and allows each group to receive appropriate access (National Institute of Standards and Technology, 2020).

The employee network should reach authorized business systems according to role. A guest network should provide internet access while blocking direct access to internal resources and other guest devices. Printers and Internet of Things devices should be isolated because they may have weaker security and infrequent updates. Management interfaces for access points, switches, and controllers should be reachable only from an administrative network using authorized accounts.

Firewall rules should follow least privilege. Employees do not need unrestricted access to every server, and guest traffic should not enter internal address space. Sensitive applications should use encrypted protocols in addition to wireless encryption. Network access control can assess whether managed devices meet requirements such as current patches, endpoint protection, and approved configuration (National Institute of Standards and Technology, 2020).

Authentication and Encryption

The original proposal used WPA-PSK, which gives many users the same password. Shared credentials are difficult to revoke when an employee leaves and may be disclosed without accountability. An enterprise environment should prefer WPA2-Enterprise or WPA3-Enterprise with 802.1X authentication and a RADIUS server. Each user or managed device receives individual credentials or certificates, allowing access to be revoked without changing a password for the whole organization (National Institute of Standards and Technology, 2012).

Certificate-based authentication is stronger than passwords where device management supports it. Administrative accounts should use multifactor authentication, and default device credentials must be changed before deployment. Weak legacy protocols such as WEP should never be enabled. Protected management frames should be used where supported to reduce certain spoofing and disconnection attacks.

MAC-address filtering may be used as an inventory aid, but it should not be treated as a security boundary. MAC addresses can be observed and imitated. Device identity should be established through authenticated credentials, certificates, and management status rather than an address that the client controls.

Protecting Data and Administrative Access

Wireless encryption protects traffic between a client and the access point, but sensitive data should also be encrypted end to end. Web applications should use TLS, file services should use secure protocols, and confidential data stored on endpoints should be encrypted. Access to customer and financial records should be role-based and logged. Backups should be protected and tested so that ransomware or equipment failure does not destroy both production data and recovery copies.

Network administrators should use separate privileged accounts rather than daily user accounts.

Changes to firewall rules, access-point settings, and authentication systems should be logged. Configuration backups should be stored securely, and firmware should be obtained from trusted sources. Management traffic should not be exposed to guest networks or the public internet without a secure administrative method.

Monitoring, Maintenance, and Incident Response

NIST emphasizes that WLAN security must be maintained throughout design, deployment, operation, and monitoring. The organization should continuously review controller alerts, authentication failures, unusual traffic, rogue access points, and devices attempting to imitate authorized networks. Wireless intrusion detection can support this work, but alerts require investigation and tuning (National Institute of Standards and Technology, 2012).

Vulnerability scanning, configuration review, and periodic wireless assessments should verify that obsolete encryption, unnecessary services, default settings, and unauthorized access points have not appeared. Firmware and operating systems should be patched according to risk. An asset inventory should record each access point, switch, controller, certificate, and responsible owner.

An incident-response plan should explain how employees report suspicious connections, lost devices, phishing, unexpected access, or accidental exposure. The technical team should know how to isolate a client, disable credentials, preserve logs, assess affected data, and restore secure service. Monthly meetings may be useful during implementation, but ongoing awareness should also be built into orientation, brief reminders, simulations, and role-specific training.

Physical and Environmental Security

Access points should be mounted where tampering is difficult, but visibility alone is not a sufficient control. Network closets should be locked, visitor access documented, and switch ports protected. Unused ports should be disabled or assigned to a restricted network. Equipment in public areas requires secure mounting and protective enclosures where necessary.

The design should also account for power loss, heat, water leaks, and construction changes. Uninterruptible power supplies can protect controllers, switches, firewalls, and authentication services. Updated floor plans and post-change surveys are important when walls, furniture, or occupancy patterns change.

Validation and Acceptance Testing

After installation, technicians should measure signal strength, signal-to-noise ratio, roaming behavior, throughput, latency, and packet loss throughout the facility. Tests should be performed in the food

court, meeting spaces, offices, the inner corner, and records areas while the building is occupied. Capacity testing should simulate busy periods rather than evaluating only one device in an empty room.

Security acceptance testing should confirm that guests cannot reach internal systems, unauthorized users cannot join employee networks, management interfaces are restricted, and logs reach the monitoring platform. Failover, credential revocation, device onboarding, and incident procedures should also be tested. Documentation should record access-point locations, cable paths, channel assignments, power settings, VLANs, firewall rules, and support contacts.

Conclusion

A secure WLAN for an L-shaped facility requires more than strong radio signals. It needs measured coverage, sufficient capacity, non-overlapping channels, appropriate access-point placement, and centralized management. It must also separate user groups, authenticate individuals and devices, encrypt data, restrict administrative access, and monitor for threats (National Institute of Standards and Technology, 2012, 2020).

The proposed three-access-point layout is a reasonable starting hypothesis, not a final answer. A site survey should confirm whether it adequately covers the corner, food court, meeting rooms, and work areas. By replacing shared passwords and MAC filtering with enterprise authentication, segmentation, continuous monitoring, and lifecycle maintenance, the organization can support convenient wireless access without exposing its clients, employees, or intellectual property to unnecessary risk.

References

National Institute of Standards and Technology. (2012). *Guidelines for securing wireless local area networks (WLANs)* (NIST SP 800-153).

National Institute of Standards and Technology. (2020). *Zero trust architecture* (NIST SP 800-207).