

WLAN Security

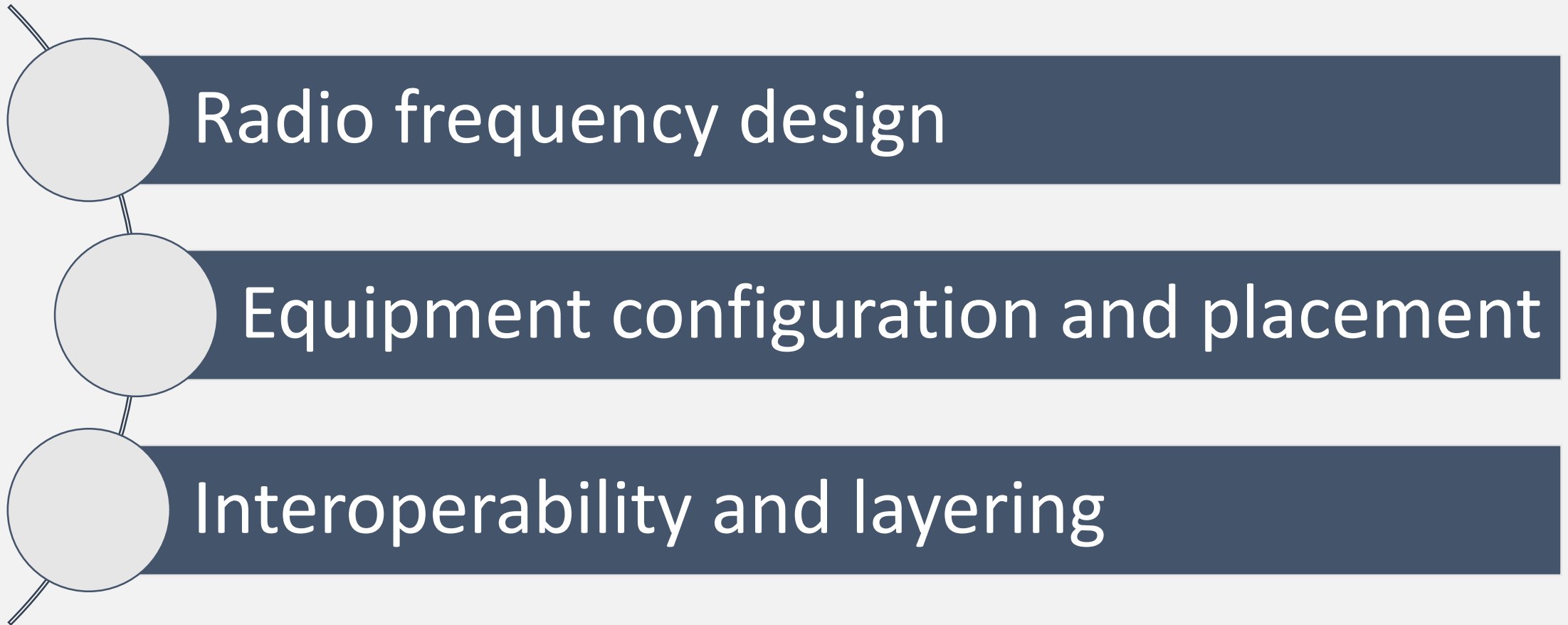


Overview

- Describe how proper design and installation contribute to basic security.
- Describe security methods such as SSID masking, MAC filtering, authentication and association, VPNs, and VLANs
- Describe best practices for firmware updates, periodic security checks and physical inventory



Design and Implementation Considerations for Basic Security



Radio Frequency Design

- Critical to restrict the RF coverage to the premise's boundaries
 - Radio pollution broadcasts beyond a property degrades performance among neighboring wireless networks
- Consider using semi-directional antennas and lowering the power



Equipment Configuration and Placement

- Place access point in a central location
 - RF travels through walls and windows, so avoid locating unit close to a wall or door
- Limit signal outside of desired areas
 - Adjust access point's power to ensure adequate coverage without excessive external radiation
 - Consider antenna type and coverage pattern
 - Ensure necessary coverage at the lowest power setting and least amount of leakage/noise




Interoperability and Layering

- Check for dead spots by walking the premises with a device that has a Wi-Fi indicator
- Resolve a persistent low signal:
 - If problem is a lack of coverage, use wireless extender or wireless repeater
 - If problem is a lack of throughput and capacity use an overlay
- Consider Wi-Fi roaming strategy



Access Restriction

- 
- SSID obfuscation
 - MAC filters
 - VPN over wireless
 - Virtual local area networks

SSID Obfuscation

- Emulator example: [LAPAC2600 AC2600 Dual Band Access Point \(linksys.com\)](http://linksys.com)
- Service set identifier (SSID) segmentation
 - Creates and assigns different SSIDs for different types of users, protocols, functions, or departments
- Users connected to same access point, but in different departments, for example, can be logically grouped and segregated by SSID/VLAN pairs
- Each SSID can be configured with different security parameters, making the security model scalable



SSID Obfuscation (Cont.)

- Only good for avoiding casual or opportunistic access to network
 - Cracking tools can still find it easily
 - It makes setup more difficult
 - It makes guest access more difficult
 - It opens the client to a rogue AP attack



MAC Filters

- MAC addressing is fundamental way in which devices communicate using frames at Layer 2
- MAC filters are used in a “deny by default, permit by exception” scheme
 - Only MAC addresses on list are permitted access
- Not practical in very large or public networks
- MAC addresses can be spoofed; MAC filtering not especially effective against a skilled attacker



Setup AP with Hidden ID and Connect One Client

Use Monitor Mode or Microsoft Network Monitor to sniff for SSID and MAC address

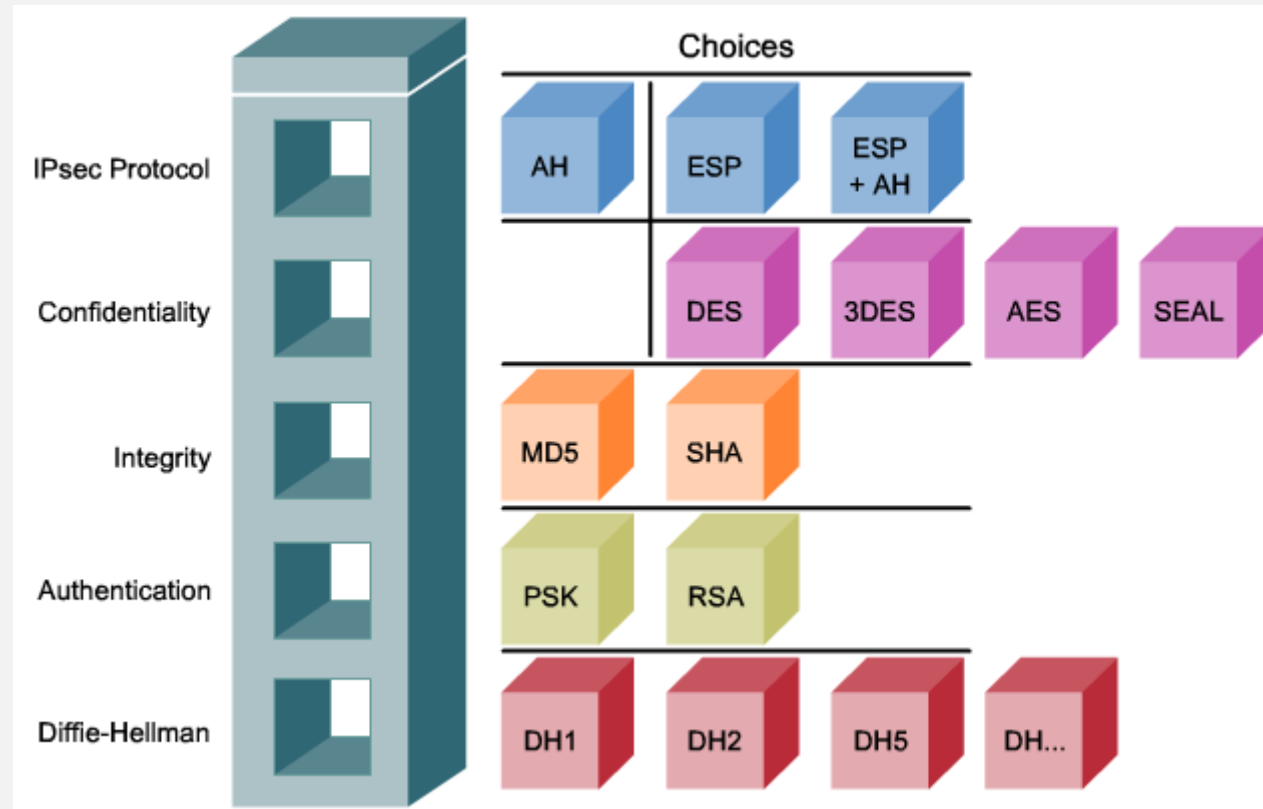


VPN over Wireless

- Post 802.11-2007, layer 2 security solutions were provided by encryption
- Has made VPN usage in the WLAN somewhat redundant
- VPNs for secure Wi-Fi access operate at Layer 3; attacker can get access to both the Layer 2 and Layer 3 connections before the VPN tunnel is established
- VPNs are useful when using a public (non-secured) Wi-Fi



IPSEC



User Segmentation with VLANs

Internal user segmentation

- Often accomplished via virtual local area networks (VLANs)

External user segmentation

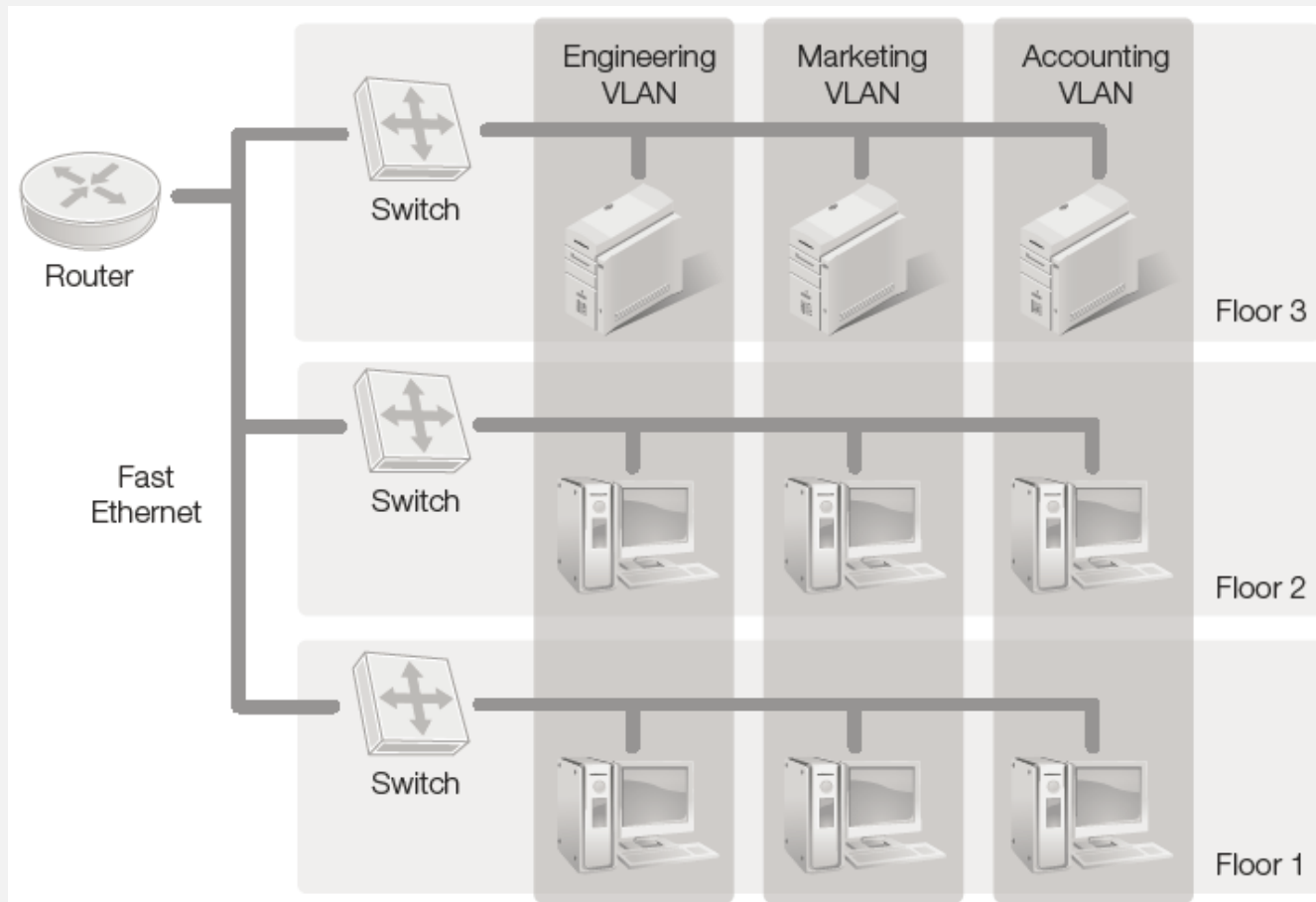
- Often achieved with a wireless connection outside corporate firewall or a VLAN; both allow direct access to Internet

Virtual Local Area Networks (VLANs)

- Is a Layer 2 technique whereby network designer logically segregates traffic, assigning it to a specific VLAN using some identifier
- Is one way to isolate visitor traffic and confine it to external, untrusted areas
- Can provide logical segmentation based on protocol, MAC address, function, or application
- All packets coming from client assigned to a VLAN are tagged with VLAN number (called 802.1Q tagging or VLAN tagging)
- Scalable in large networks because VLAN association spans physical switches
- Client authenticates via RADIUS



VLAN Example




Implementing VLANs Demonstration

- EA9500 Emulator
- Wireless VLANs – SSID can be changed
- VLAN tagging
 - <https://www.cloudshark.org/captures/008c321f16ab>
- Tunneling – Double tagging
 - <https://www.cloudshark.org/captures/001010a25ef6>



Ongoing Management Security Considerations



Firmware upgrades

Physical security

Periodic inventory

Wireless IDS/IPS

Firmware Upgrades

- Bugs, flaws, or vulnerabilities are occasionally discovered in a vendor product, like a wireless access point
- Hackers look for unpatched equipment and quickly expose bugs, etc. and disseminate exploits
- Vendor provides patches and new firmware to fix issues
- Examples:
 - <https://www.zdnet.com/article/unpatched-vulnerability-identified-in-79-netgear-router-models/>
 - <https://www.zdnet.com/article/wifi-firmware-bug-affects-laptops-smartphones-routers-gaming-devices/>

Physical Security for Wireless Networks

- Control radiation of RF signal outside the premises.
- Secure physical access to the building or office.
- Physically secure internal systems.
 - Lock doors to rooms containing access to switches
 - Install security doors (with audit logs) for data centers or network labs
- Conduct regular sweeps: survey RF power levels.
- Shut down all switch ports not in use.



Periodic Inventory

- Keep up-to-date inventory of all devices authorized to connect to WLAN
 - Use MAC filtering to audit MAC addresses traversing WLAN
 - Identify them as known or unknown
 - Can perform a "scream test" to identify unfamiliar MAC addresses
 - remove it and wait for the screams. If someone screams, put it back.
- Periodic inventory helps to minimize device creep



Intrusion Detection and Prevention Systems

- Use deep packet inspection to look inside packets traversing a network
- IDS is purely a detection system
 - Raises a flag if it detects suspicious activity on the wire or over the air
- IPS actively confronts and blocks any suspicious traffic it detects



Intrusion Detection and Prevention Systems: WIPS

- Wireless IDS or IPS referred to as WIPS. Two types:
 - **Network-based WIPS:** Consists of sensors that are either in line or configured in promiscuous mode so they can sample and analyze all traffic crossing the network. A centralized server and console analyze and present the results.
 - **Host-based WIPS:** Is an application on a server, client, or device that monitors for threats in applications, operating systems, and files, as well as known suspicious behavior.
 - Snort is an example product



WLAN Protocol Filtering

- Prevents the use of certain protocols on WLAN, which can help mitigate security threats
- Two types of protocol filtering:
 - **EtherType protocol filtering:** Uses a protocol identifier to identify the protocol to be blocked
 - **IP protocol filtering:** Configured on access point by specifying well-known port number for the specific protocol
- Enables low-level granular control of network protocols allowed or denied on wireless segment
- Might block torrents or SMTP (used to transfer email between servers) so you don't become a spam relay

Summary

- Radio frequency design and equipment placement for security
- Limiting access through network configuration
- Network security practices for WLANs

