Wireless LAN Security

Outlines:

- Benefits
- Standards
- Functionality
- Security Issues
- Solutions and Implementations

By: Arash Habibi Lashkari
July - 2010

Benefits

- Increased productivity
  - Improved collaboration
  - No need to reconnect to the network
  - Ability to work in more areas
- Reduced costs
  - No need to wire hard-to-reach areas

Standards

- IEEE 802.11
- IEEE 802.11b
- IEEE 802.11a
- IEEE 802.11e
- HiperLAN/2
- Interoperability

802.11

- Published in June 1997
- 2.4GHz operating frequency
- 1 to 2 Mbps throughput
- Can choose between frequency hopping or direct sequence spread modulation

802.11b

- Published in late 1999 as supplement to 802.11
- Still operates in 2.4GHz band
- Data rates can be as high as 11 Mbps
- Only direct sequence modulation is specified
- Most widely deployed today

802.11a

- Also published in late 1999 as a supplement to 802.11
- Operates in 5GHz band (less RF interference than 2.4GHz range)
- Users Orthogonal Frequency Division Multiplexing (OFDM)
- Supports data rates up to 54 Mbps
- Currently no products available, expected in fourth quarter

802.11e

- Currently under development
- Working to improve security issues
- Extensions to MAC layer, longer keys, and key management systems
- Adds 128-bit AES encryption

HiperLAN/2

- Development led by the European Telecommunications Standards Institute (ETSI)
- Operates in the 5 GHz range, uses OFDM technology, and support data rates over 50Mbps like 802.11a

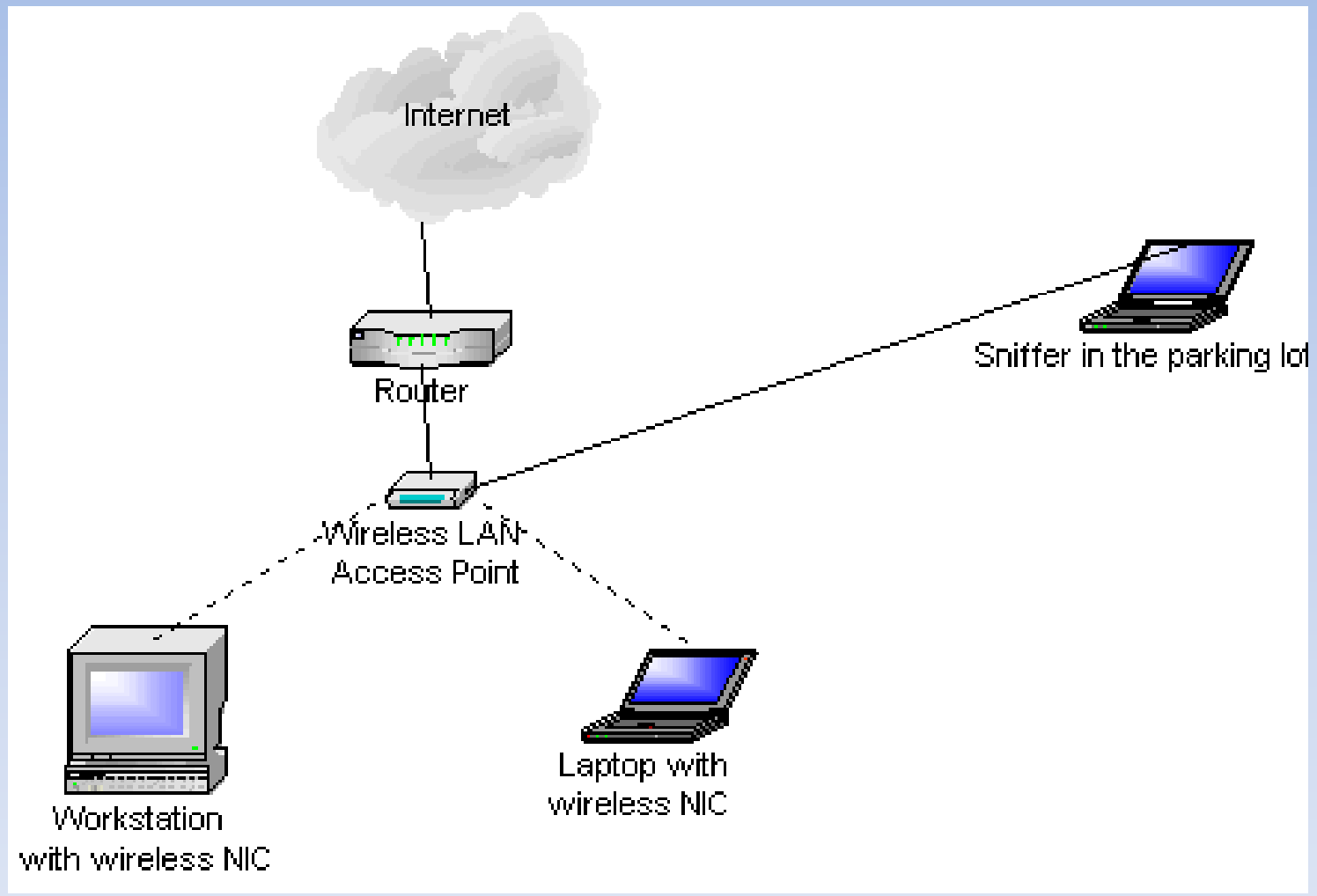
Interoperability

- 802.11a and 802.11b work on different frequencies, so little chance for interoperability
- Can coexist in one network
- HiperLAN/2 is not interoperable with 802.11a or 802.11b

Functionality

- Basic Configuration
- Secure LAN
- WLAN Communication
- Intermediate WLAN
- VPN

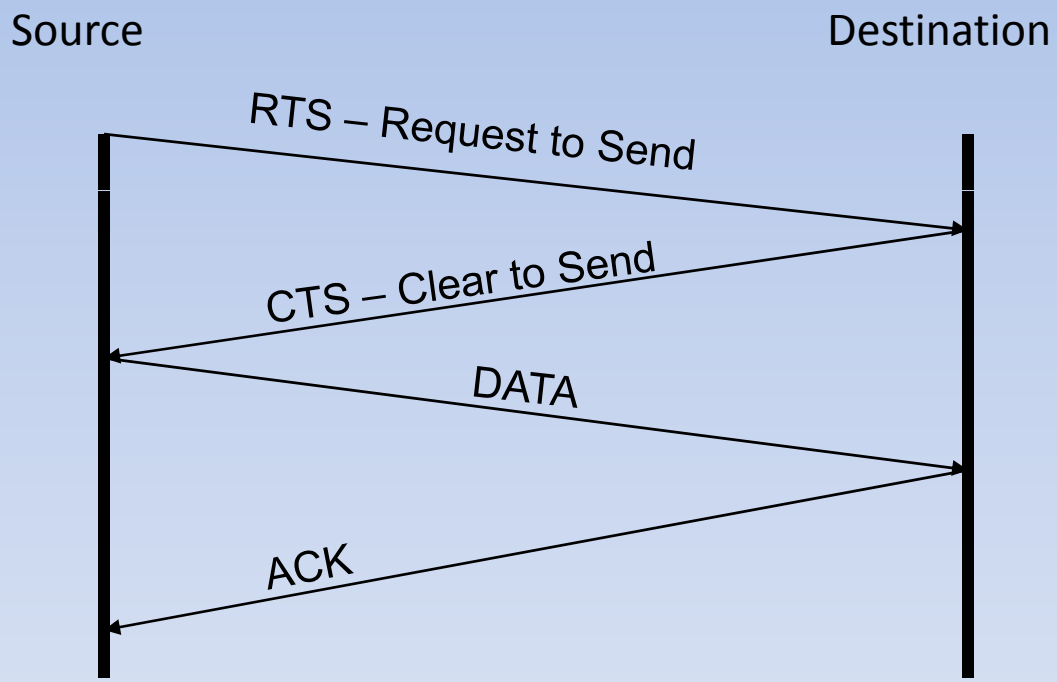
Basic Configuration



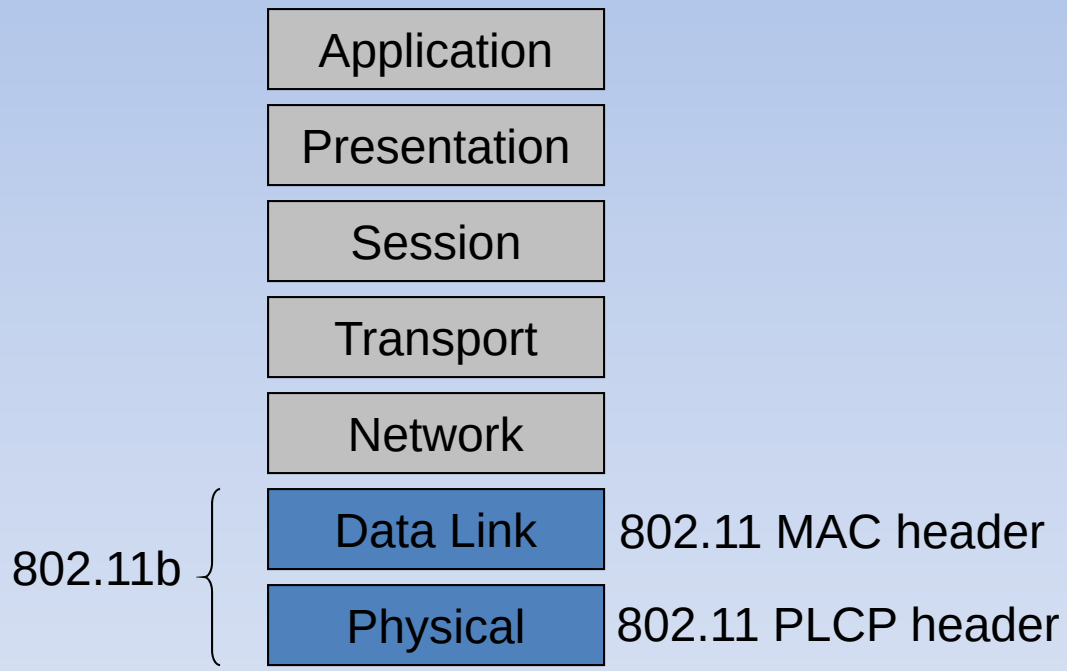
802.11 Communication

- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) instead of Collision Detection
- WLAN adapter cannot send and receive traffic at the same time on the same channel
- Hidden Node Problem
- Four-Way Handshake

Four-Way Handshake



OSI Model


Application
Presentation
Session
Transport
Network
Data Link
Physical
802.11b
802.11 MAC header
802.11 PLCP header

Security Issues and Solutions

- Sniffing and War Driving
- Rogue Networks
- Policy Management
- MAC Address
- SSID
- WEP

War Driving

- Default installation allow any wireless NIC to access the network
- Drive around (or walk) and gain access to wireless networks
- Provides direct access behind the firewall
- Heard reports of an 8 mile range using a 24dB gain parabolic dish antenna.

Rogue Networks

- Network users often set up rogue wireless LANs to simplify their lives
- Rarely implement security measures
- Network is vulnerable to War Driving and sniffing and you may not even know it

Policy Management

- Access is binary
- Full network access or no network access
- Need means of identifying and enforcing access policies

MAC Address

- Can control access by allowing only defined MAC addresses to connect to the network
- This address can be spoofed
- Must compile, maintain, and distribute a list of valid MAC addresses to each access point
- Not a valid solution for public applications

Service Set ID (SSID)

- SSID is the network name for a wireless network
- WLAN products common defaults: “101” for 3COM and “tsunami” for Cisco
- Can be required to specifically request the access point by name (lets SSID act as a password)
- The more people that know the SSID, the higher the likelihood it will be misused.
- Changing the SSID requires communicating the change to all users of the network

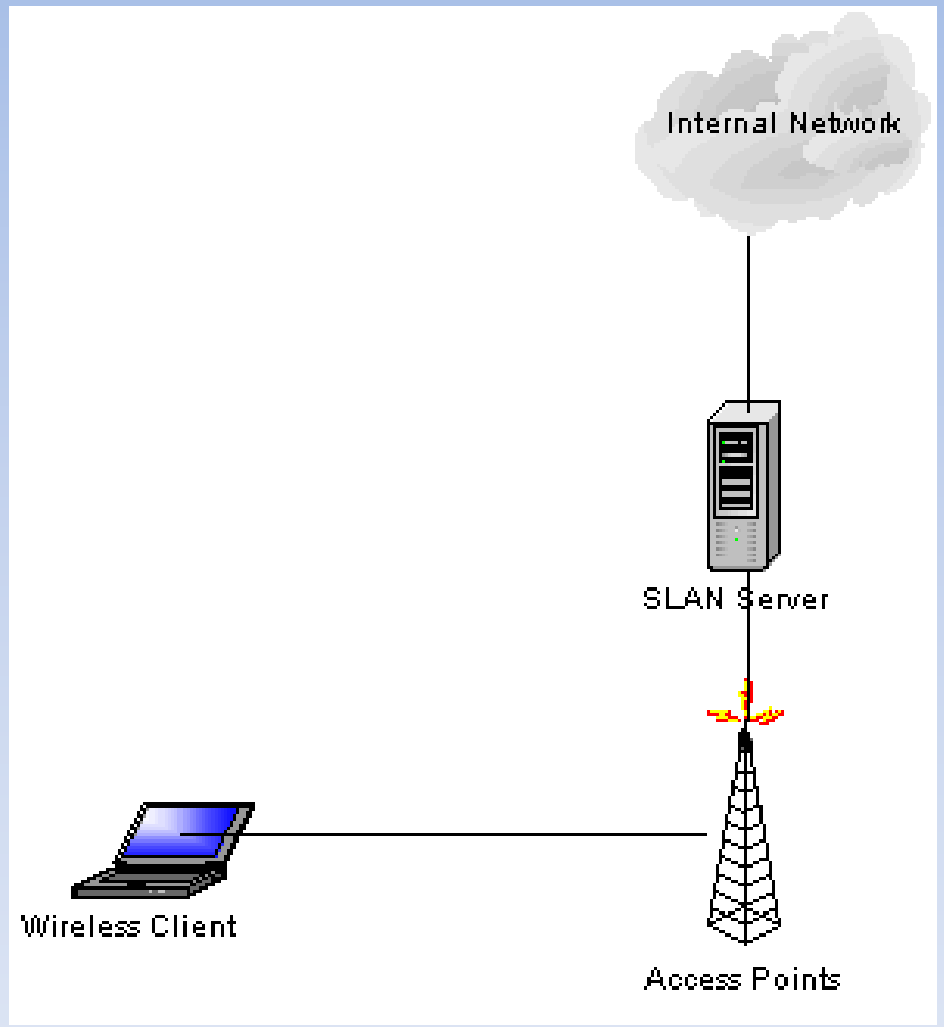
Wired Equivalent Privacy (WEP)

- Designed to be computationally efficient, self-synchronizing, and exportable
- Vulnerable to attack
  - Passive attacks to decrypt traffic based on statistical analysis
  - Active attacks to inject new traffic from unauthorized mobile stations, based on known plaintext
  - Dictionary-building attack that, after analysis of a day's worth of traffic, allows real-time automated decryption of all traffic
- All users of a given access point share the same encryption key
- Data headers remain unencrypted so anyone can see the source and destination of the data stream

Secure LAN (SLAN)

- Intent to protect link between wireless client and (assumed) more secure wired network
- Similar to a VPN and provides server authentication, client authentication, data privacy, and integrity using per session and per user short life keys
- Simpler and more cost efficient than a VPN
- Cross-platform support and interoperability, not highly scalable, though
- Supports Linux and Windows
- Open Source

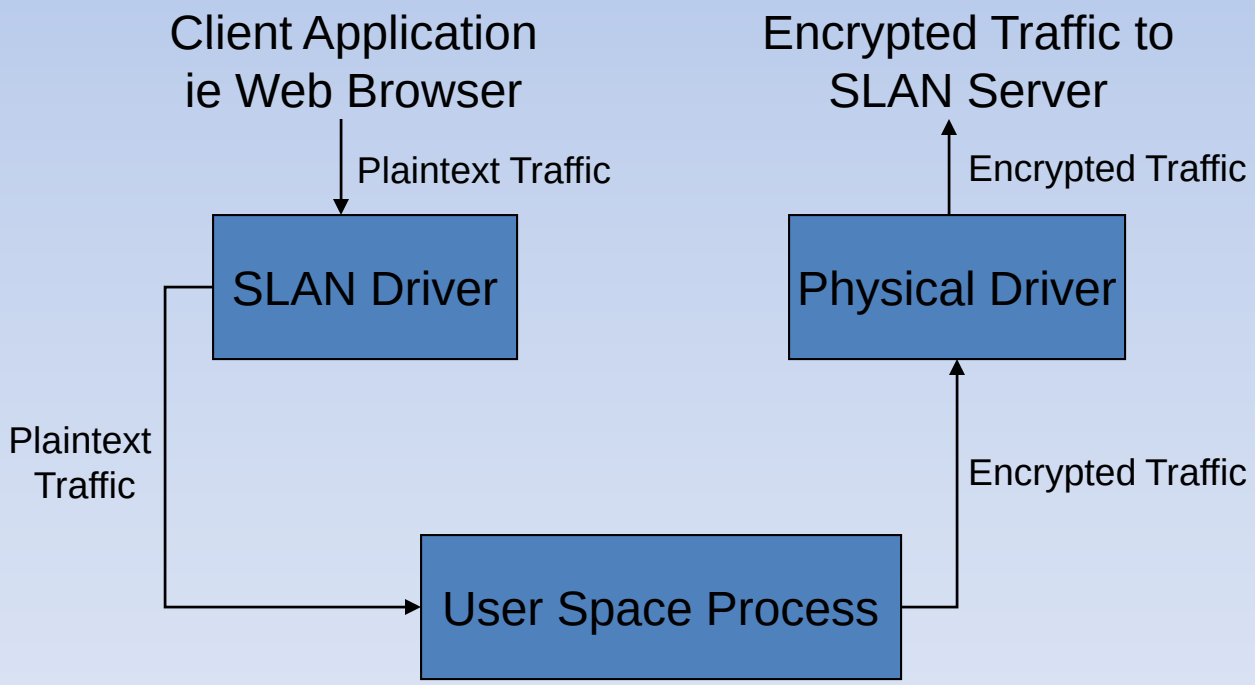
SLAN Architecture



SLAN Steps

1. Client/Server Version Handshake
2. Diffie-Hellman Key Exchange
3. Server Authentication (public key fingerprint)
4. Client Authentication (optional) with PAM on Linux
5. IP Configuration – IP address pool and adjust routing table

SLAN Client


Client Application
ie Web Browser
Plaintext Traffic
SLAN Driver
Encrypted Traffic to
SLAN Server
Encrypted Traffic
Physical Driver
Plaintext
Traffic
Encrypted Traffic
User Space Process

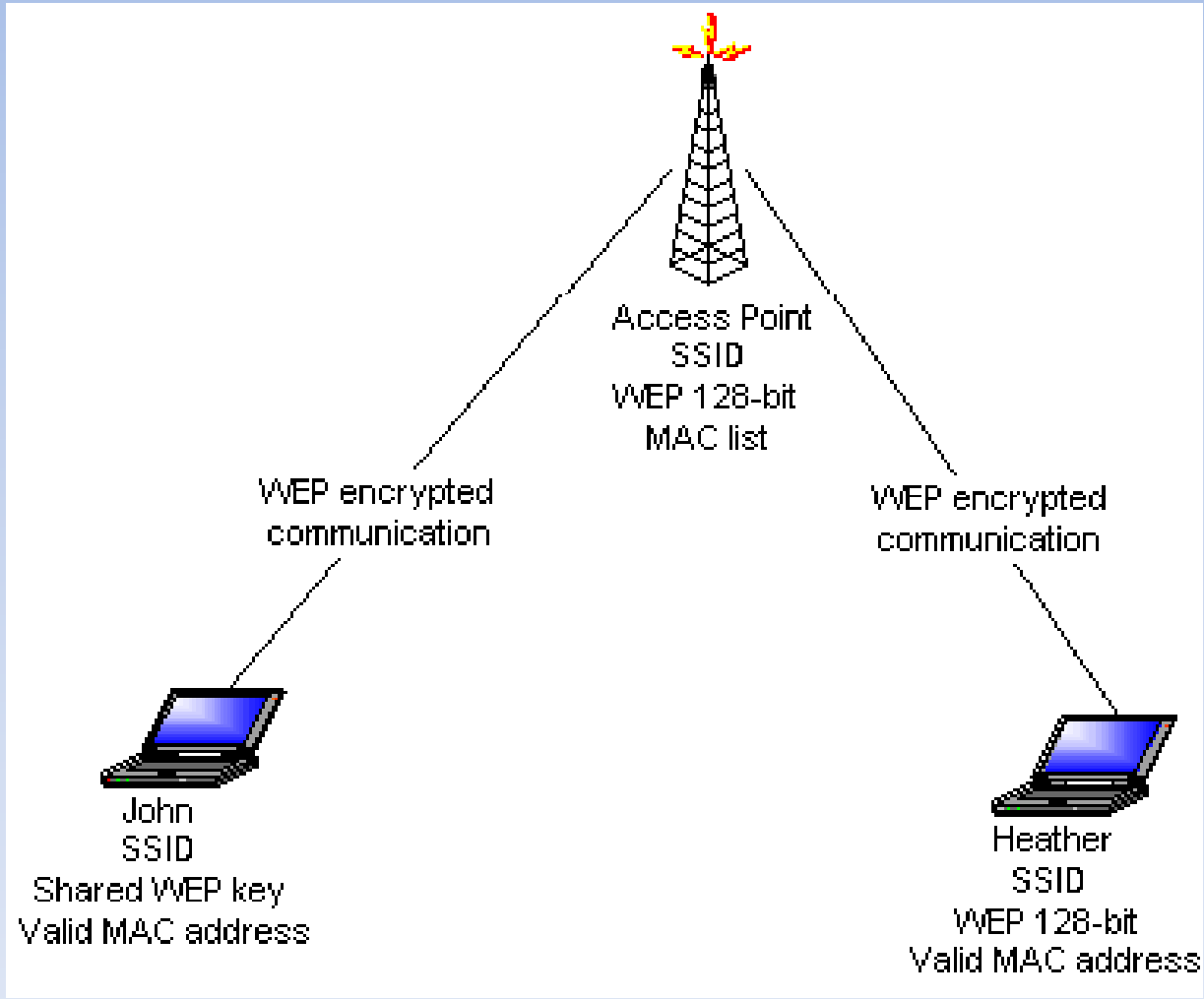
WLAN Implementations

- Varies due to organization size and security concerns
- Current technology not ideal for large-scale deployment and management
- Will discuss a few tricks that can help the process and a few technologies under development to ease enterprise deployments

Basic WLAN

- Great for small (5-10 users) environments
- Use WEP (some vendors provide 128-bit proprietary solution)
- Only allow specific MAC addresses to access the network
- Rotate SSID and WEP keys every 30-60 days
- No need to purchase additional hardware or software.

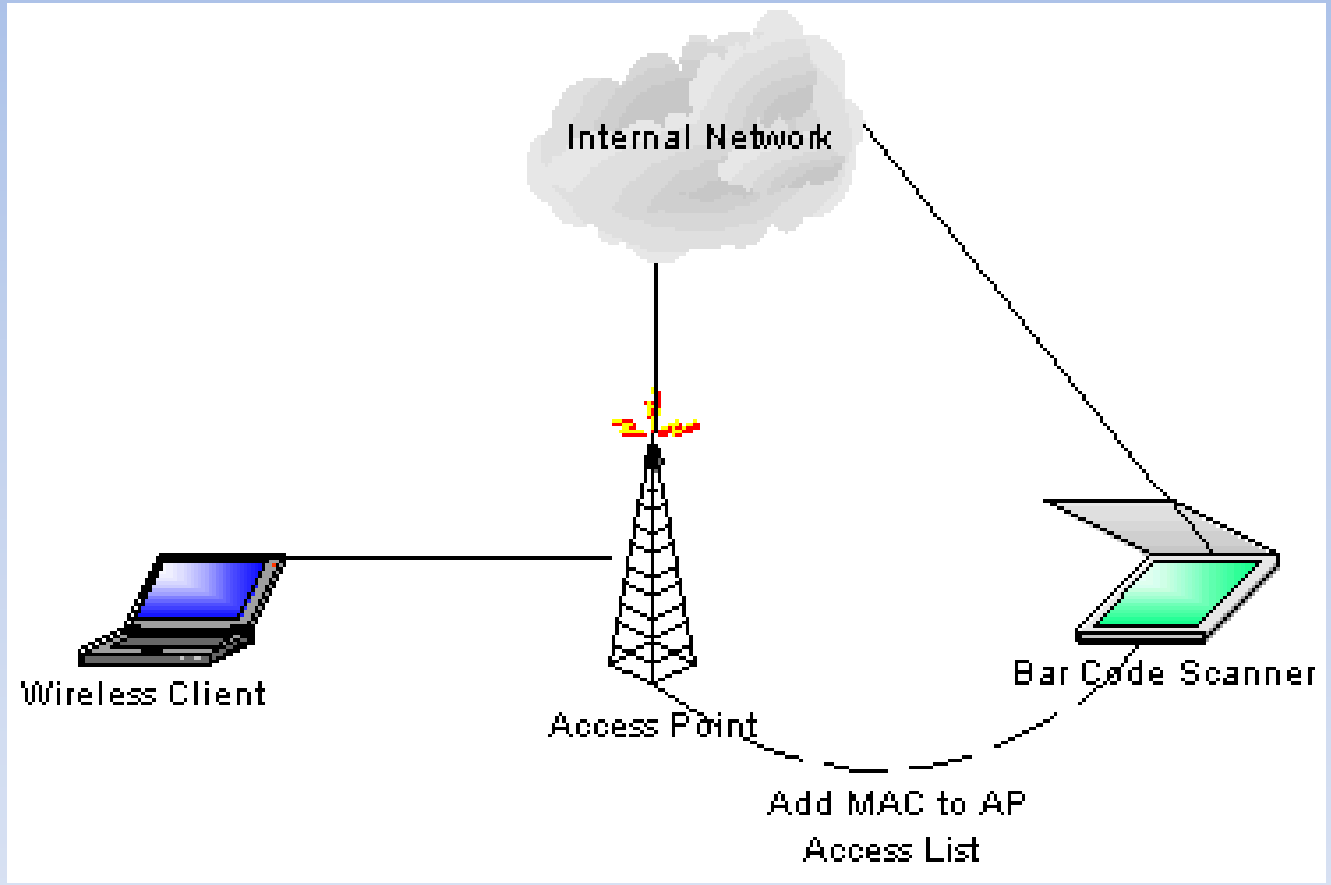
Basic WLAN Architecture



Intermediate WLAN

- 11-100 users
- Can use MAC addresses, WEP and rotate keys if you want.
- Some vendors have limited MAC storage ability
- SLAN also an option
- Another solution is to tunnel traffic through a VPN

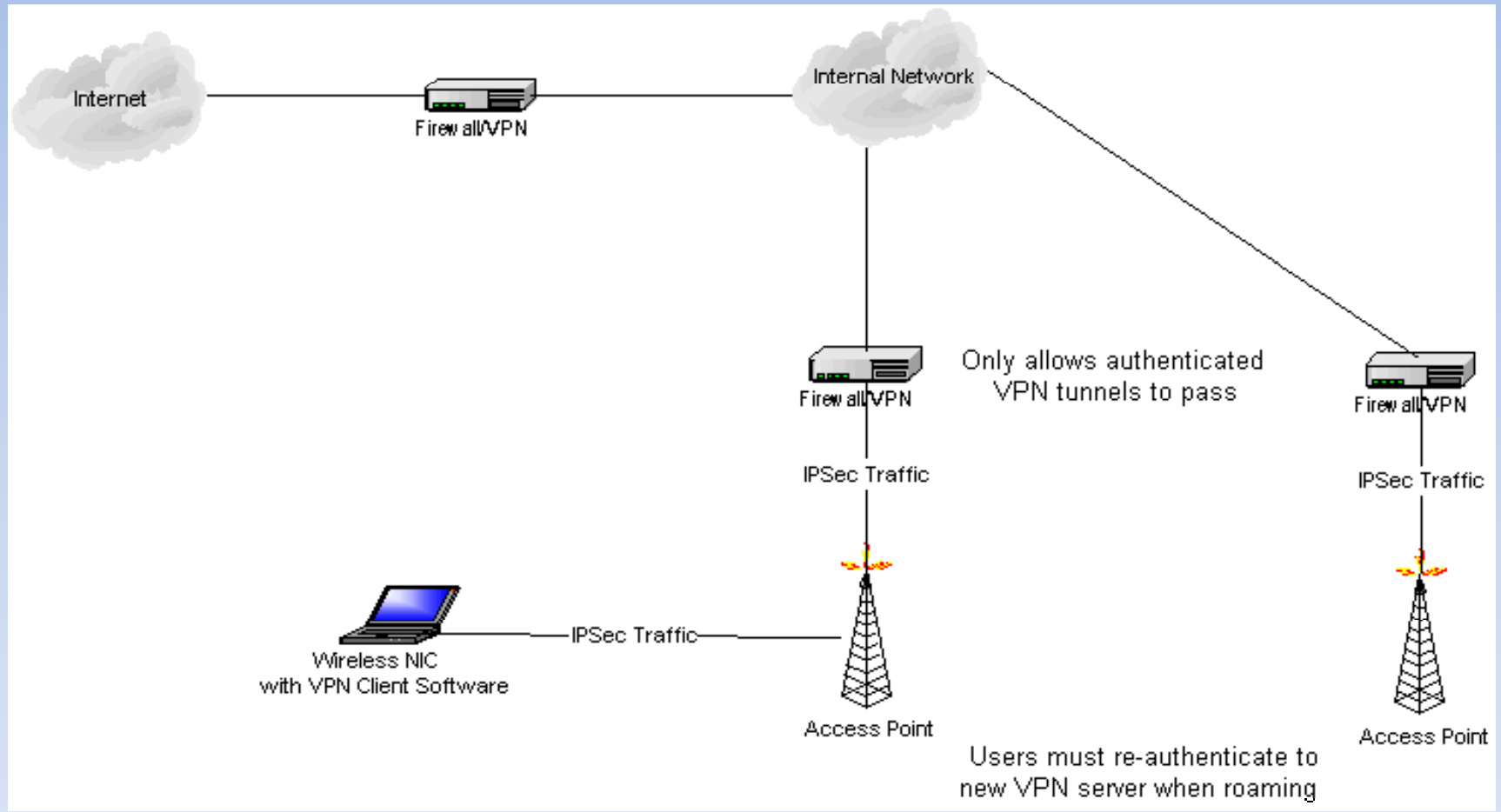
Intermediate WLAN Architecture



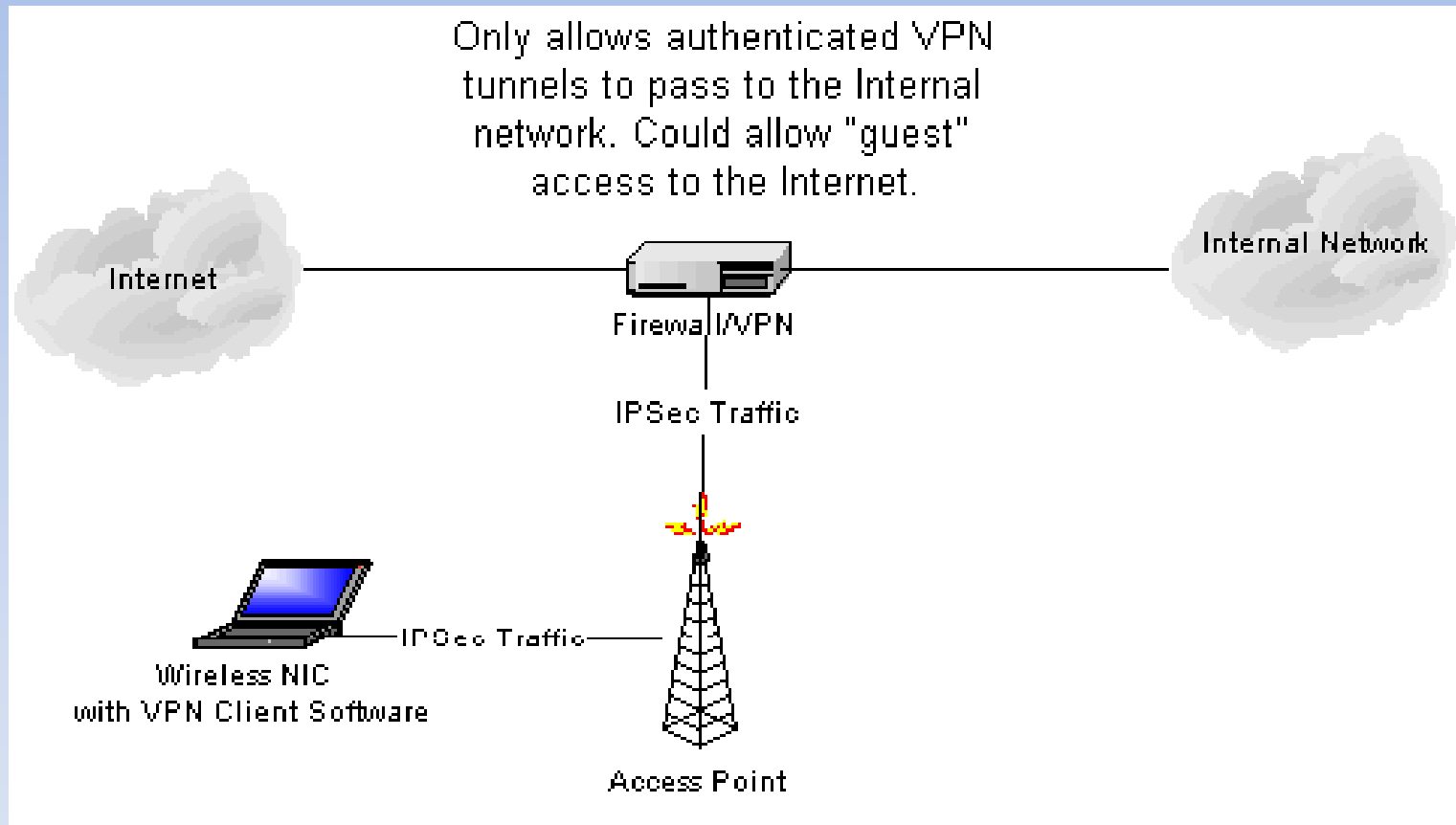
VPN

- Provides a scaleable authentication and encryption solution
- Does require end user configuration and a strong knowledge of VPN technology
- Users must re-authenticate if roaming between VPN servers

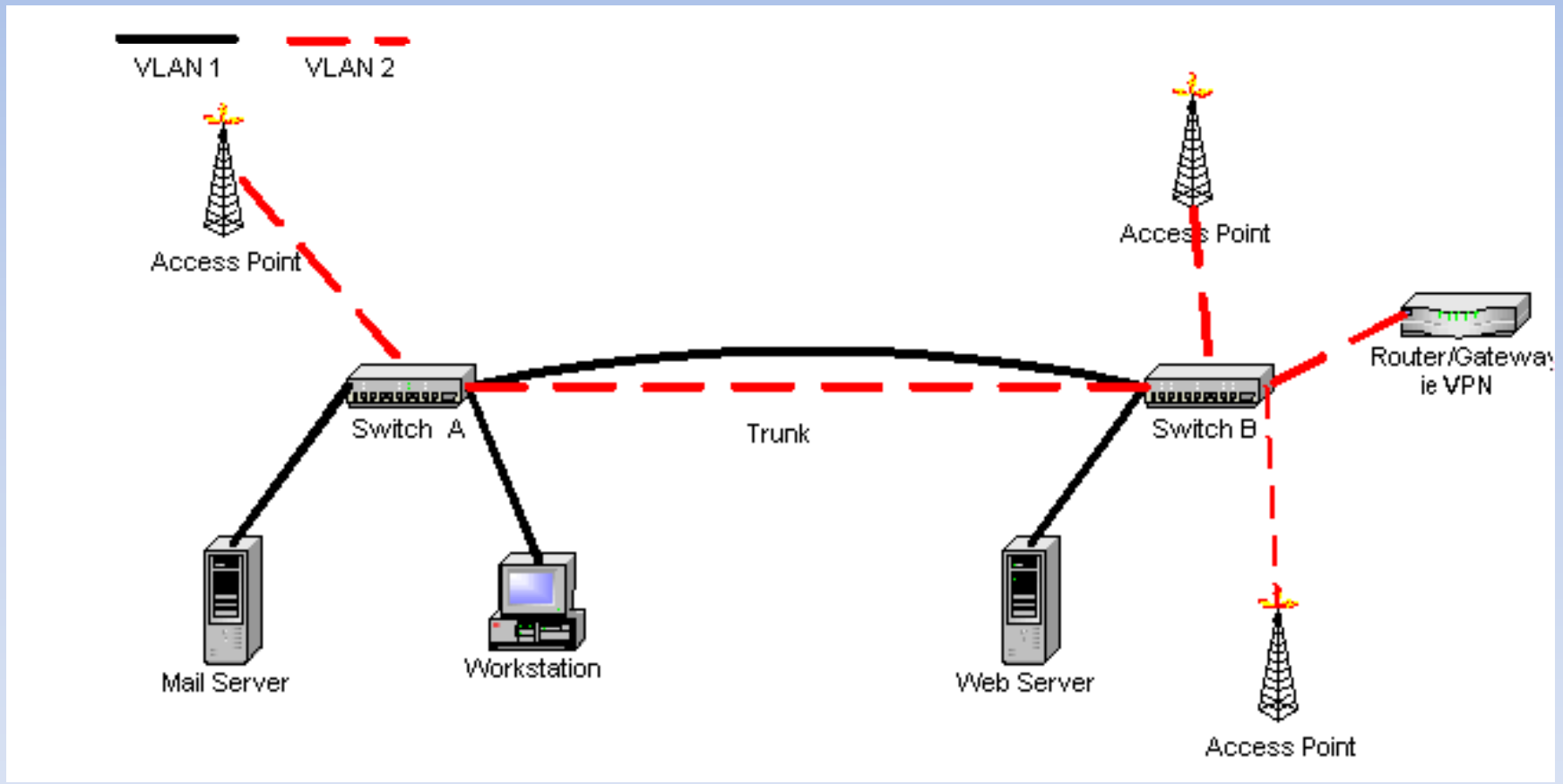
VPN Architecture



VPN Architecture



VLAN Architecture



Questions