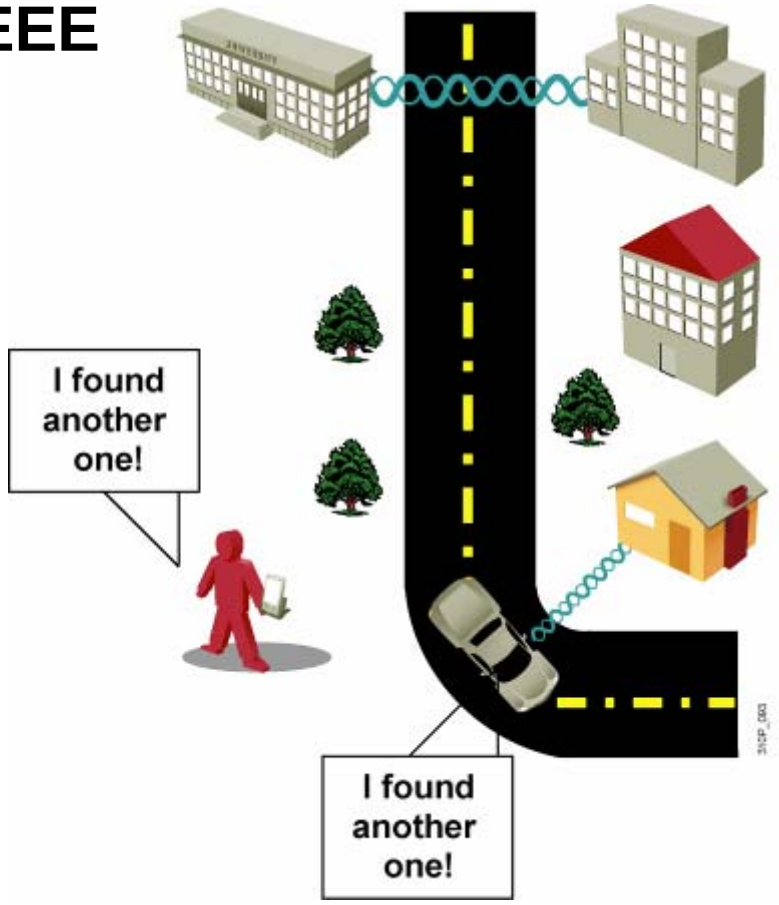
WLAN Security

Why WLAN Security?

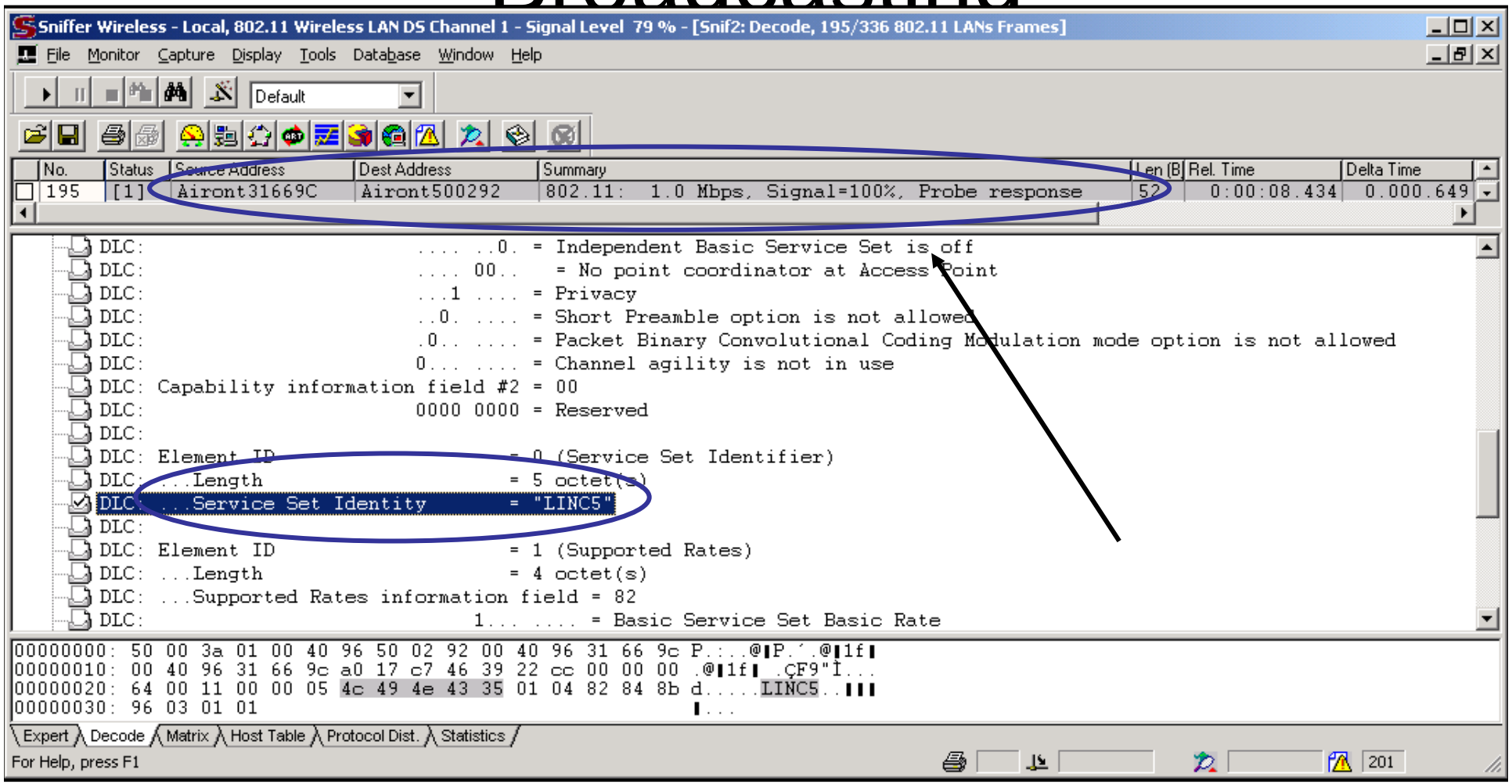
- **Wide availability and low cost of IEEE 802.11 wireless equipment**
- **802.11 standard ease of use and deployment**
- **Availability of sniffers**
- **Statistics on WLAN security**
- **Media hype about hot spots, WLAN hacking, war driving**
- **Nonoptimal implementation of encryption in standard Wired Equivalent Privacy (WEP) encryption**
- **Authentication vulnerability**



Wireless LAN Security Threats

"WAR DRIVERS"	HACKERS	EMPLOYEES
Find "Open" Networks; Use Them to Gain Free Internet Access	Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs	Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs
	 THE WALL STREET JOURNAL. Hackers Can Penetrate Wireless Network *The weakness is another reminder of the difficulty in implementing effective network security.*	

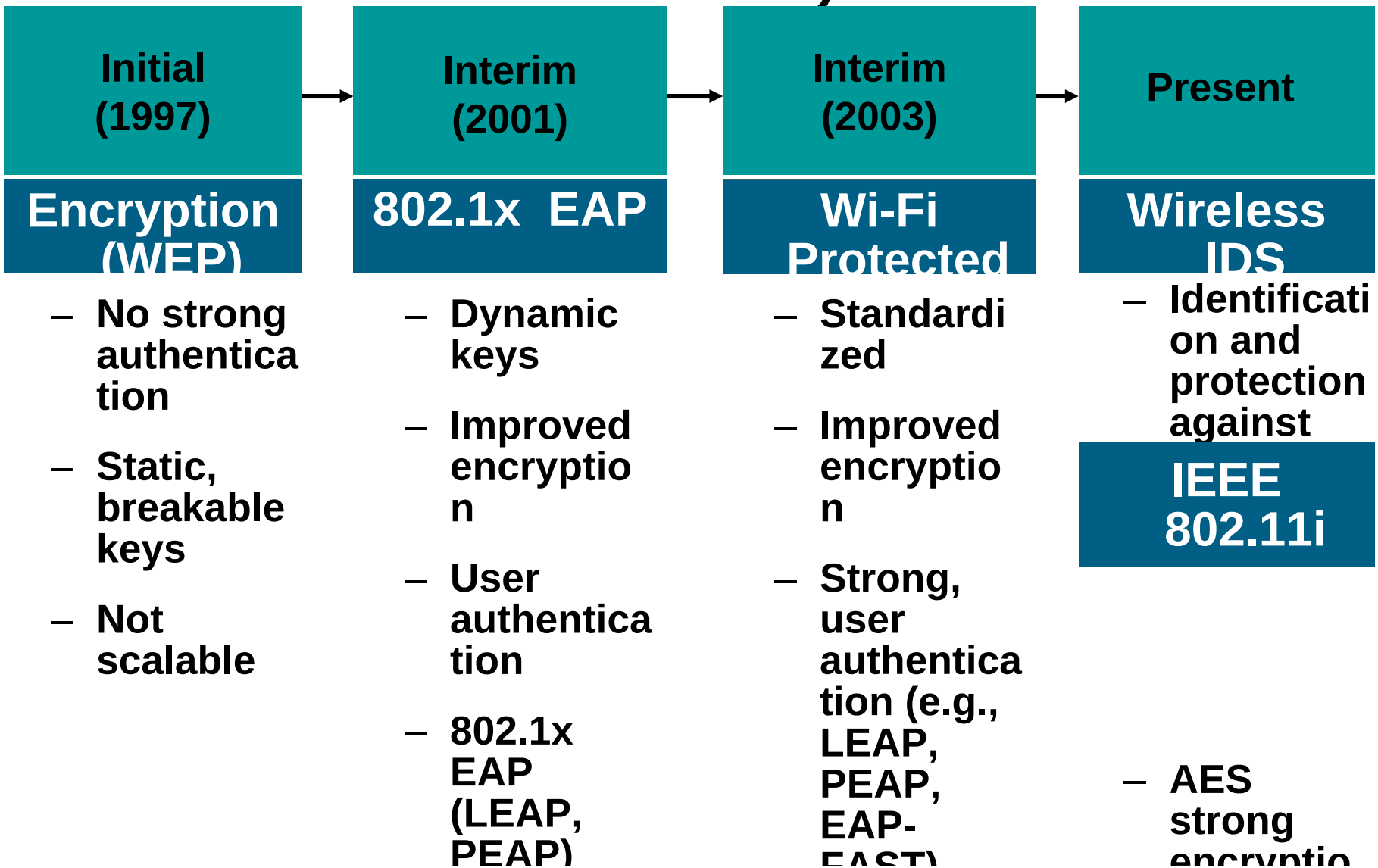
WLAN Sniffing and SSID Broadcasting



Mitigating the Threats

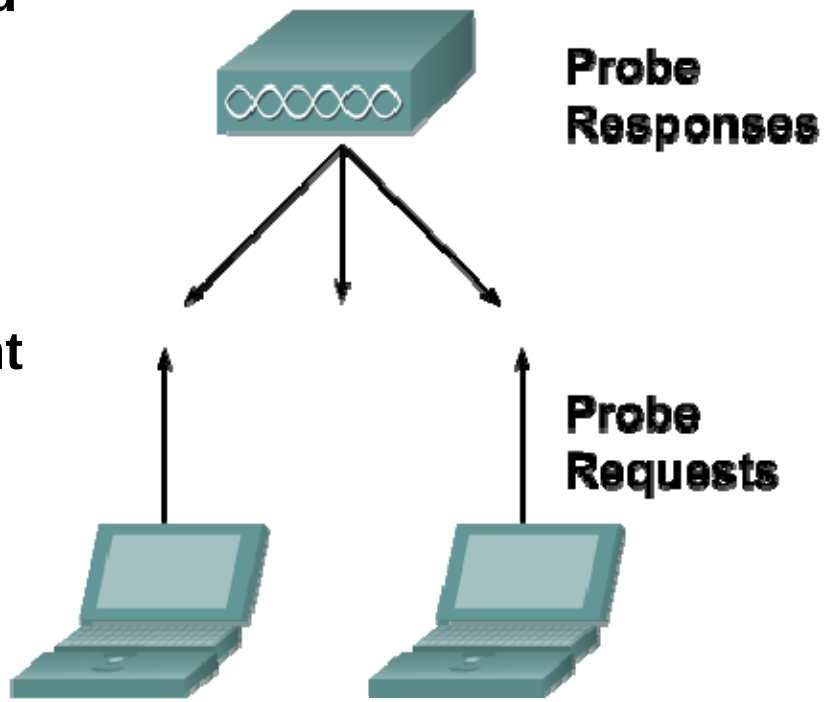
Control and Integrity	Privacy and Confidentiality	Protection and Availability
Authentication	Encryption	Detection System (IDS)
Ensure that legitimate clients associate with trusted APs.	Protect data as it is transmitted and received.	Track and mitigate unauthorized access and network attacks.

Evolution of Wireless LAN Security

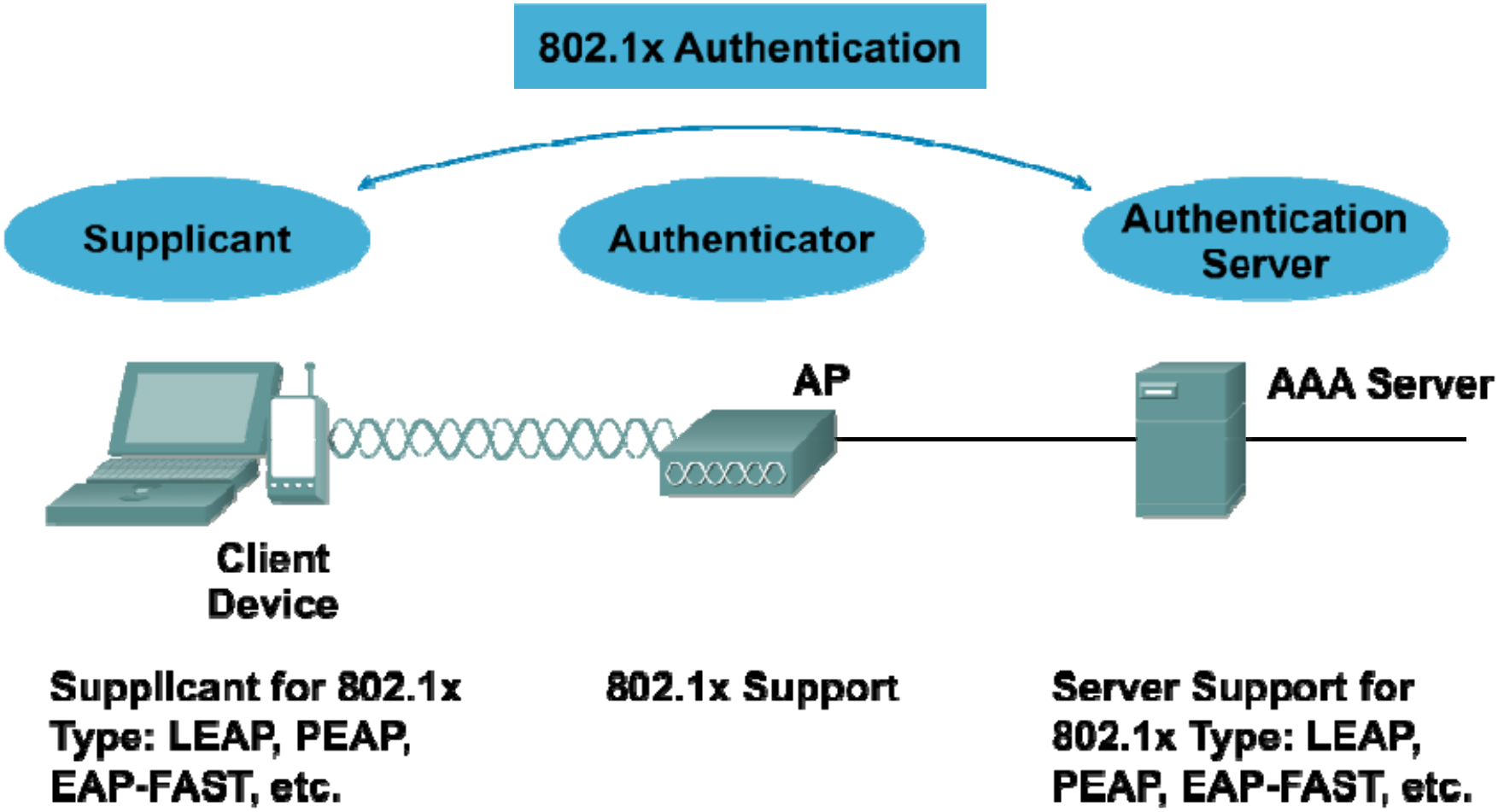


Wireless Client Association

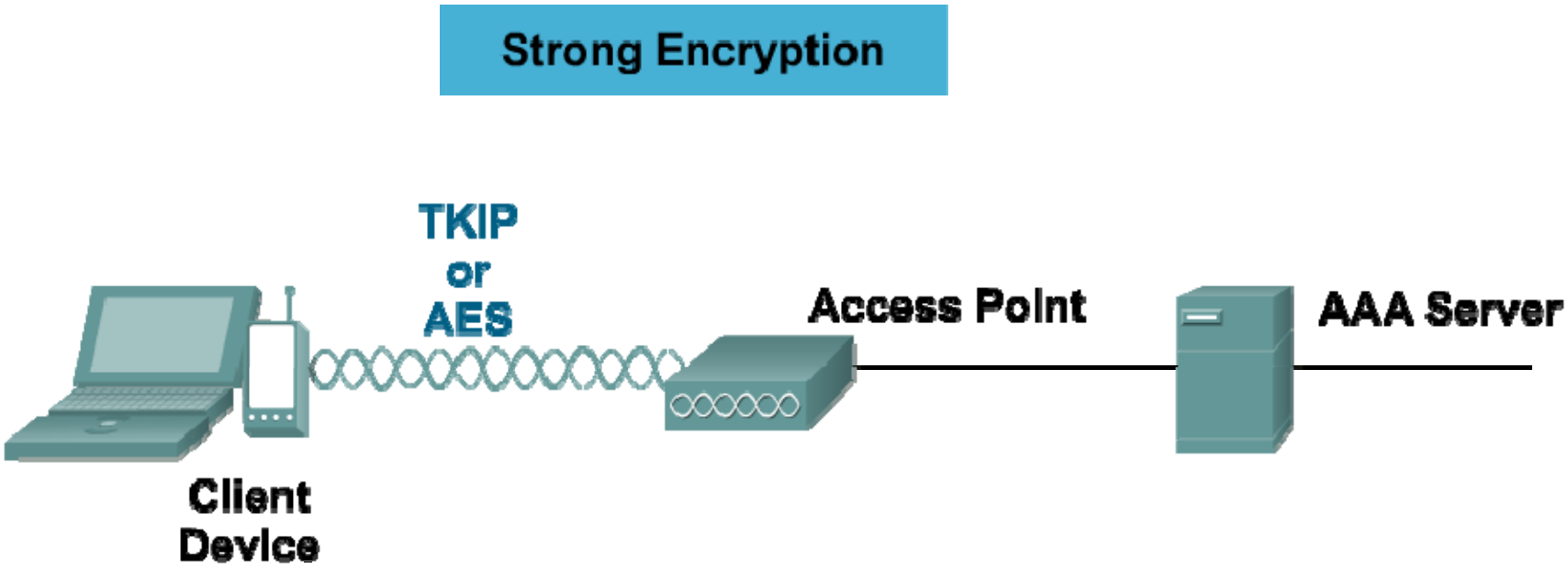
1. **Access points send out beacons announcing SSID, data rates and other information.**
2. **Client scans all channels.**
3. **Client listens for beacons and responses from access points.**
4. **Client associates to access point with strongest signal.**
5. **Client will repeat scan if signal becomes low to reassociate to another access point (roaming).**
6. **During association SSID, MAC address and security settings are sent from the client to the AP and checked by the AP.**



WPA and WPA2 Authentication



WPA and WPA2 Encryption



Wi-Fi Protected Access

- **What are WPA and WPA2?**
  - **–Authentication and encryption standards for Wi-Fi clients and APs**
  - **–802.1x authentication**
  - **–WPA uses TKIP encryption**
  - **–WPA2 uses AES block cipher encryption**
- **Which should I use?**
  - **–Gold, for supporting NIC/OSs**
  - **–Silver, if you have legacy clients**
  - **–Lead, if you absolutely have no other choice.**

Gold

WPA2/802.11i

- **EAP-Fast**
- **AES**

Silver

WPA

- **EAP-Fast**
- **TKIP**

Lead

Dynamic WEP

- **EAP-Fast/LEAP**
- **VLANs + ACLs**

WLAN Security Summary

Open Access

No Encryption, Basic Authentication

Public “Hotspots”

Basic Security

40-bit or 128-bit Static WEP Encryption, WPA

Home Use

Enhanced Security

802.1x, TKIP Encryption, Mutual Authentication, Scalable Key Mgmt., Etc.

Enterprise

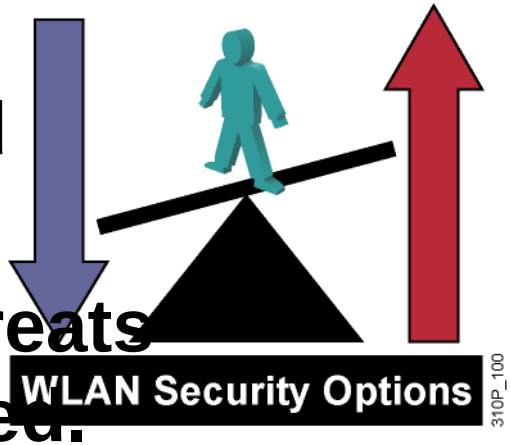
Remote Access

Virtual Private Network (VPN)

Business Traveler, Telecommuter

Security Evaluation

- **Evaluate effectiveness of encrypted WLAN statistics.**
- **Focus on proper planning and implementation.**
- **Estimate potential security threats and the level of security needed.**
- **Evaluate amount of WLAN traffic being sent when selecting security methods.**
- **Evaluate tools and options applicable to WLAN design.**



Activity

Packet sniffing programs have become more user friendly in recent years. NetStumbler is one of the easiest packet sniffers to use.

Read this short Wikipedia article about NetStumbler and decide for yourself if you want to download it and explore your wireless network. http://en.wikipedia.org/wiki/NetStumbler