

WLAN Security



Why WLAN Security?

Wide availability and low cost of IEEE 802.11 wireless equipment

802.11 standard ease of use and deployment

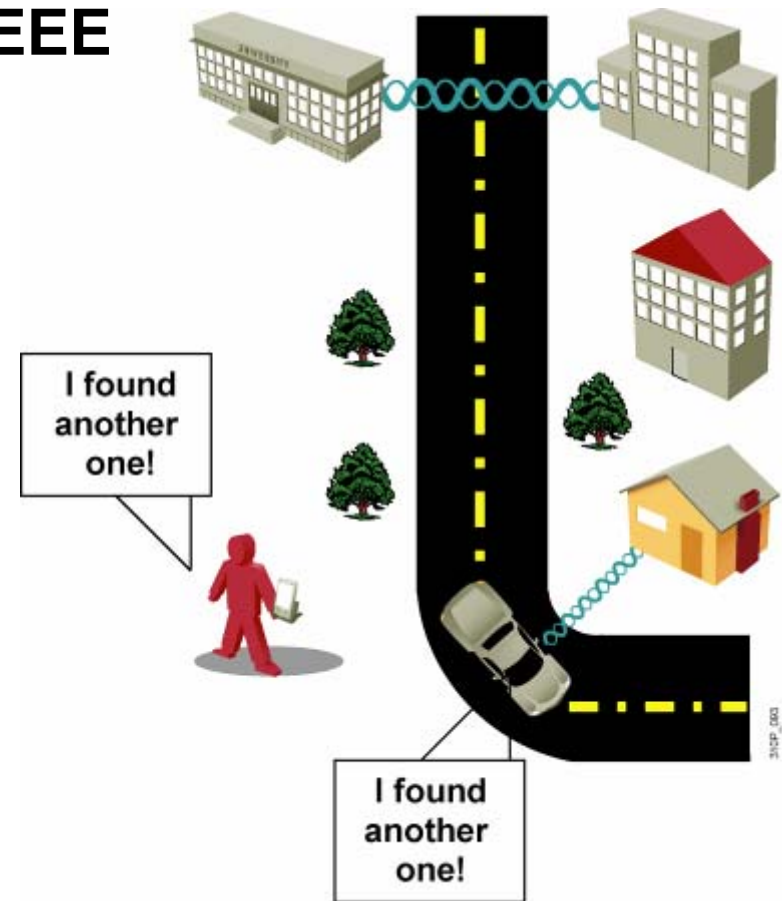
Availability of sniffers

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”

Find “Open” Networks; Use Them to Gain Free Internet Access



HACKERS

Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs



EMPLOYEES

Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs



WLAN Sniffing and SSID Broadcasting

The screenshot displays the Sniffer Wireless interface. The main window title is "Sniffer Wireless - Local, 802.11 Wireless LAN DS Channel 1 - Signal Level 79 % - [Snif2: Decode, 195/336 802.11 LANs Frames]". The interface includes a menu bar (File, Monitor, Capture, Display, Tools, Database, Window, Help) and a toolbar with various icons. A table at the top shows captured frames, with frame 195 selected. The table columns are No., Status, Source Address, Dest Address, Summary, Len (B), Rel. Time, and Delta Time. The selected frame 195 has Source Address Airtont31669C, Dest Address Airtont500292, and Summary "802.11: 1.0 Mbps, Signal=100%, Probe response". Below the table, a detailed view of the frame's contents is shown, including DLC (Data Link Control) fields. The "Service Set Identity" field is highlighted with a blue oval and contains the value "LINC5". A black arrow points from this field to the "Summary" column of the frame table above. At the bottom, there is a hex dump of the frame data and a status bar with the text "For Help, press F1" and a page number "201".

No.	Status	Source Address	Dest Address	Summary	Len (B)	Rel. Time	Delta Time
195	[1]	Airtont31669C	Airtont500292	802.11: 1.0 Mbps, Signal=100%, Probe response	52	0:00:08.434	0.000.649

Detailed frame content (DLC fields):

- DLC:0. = Independent Basic Service Set is off
- DLC: ... 00.. = No point coordinator at Access Point
- DLC: ...1 = Privacy
- DLC: ..0. = Short Preamble option is not allowed
- DLC: .0... = Packet Binary Convolutional Coding Modulation mode option is not allowed
- DLC: 0... .. = Channel agility is not in use
- DLC: Capability information field #2 = 00
- DLC: 0000 0000 = Reserved
- DLC: Element ID = 0 (Service Set Identifier)
- DLC: ...Length = 5 octet(s)
- DLC: ...Service Set Identity = "LINC5"**
- DLC: Element ID = 1 (Supported Rates)
- DLC: ...Length = 4 octet(s)
- DLC: ...Supported Rates information field = 82
- DLC: 1... .. = Basic Service Set Basic Rate

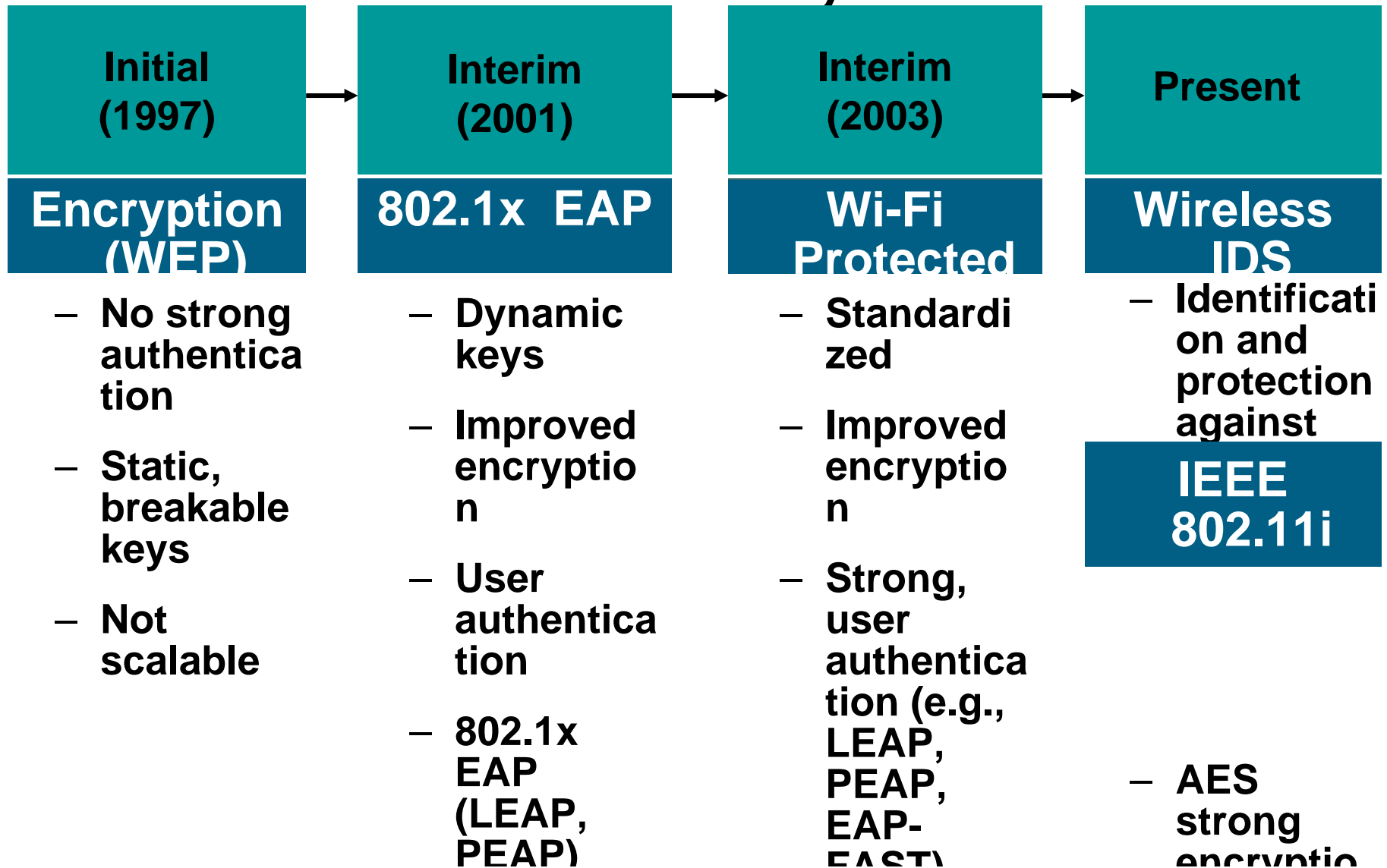
Hex dump:

```
00000000: 50 00 3a 01 00 40 96 50 02 92 00 40 96 31 66 9c P...@IP...@lf|
00000010: 00 40 96 31 66 9c a0 17 c7 46 39 22 cc 00 00 00 .@lf| .CF9"l...
00000020: 64 00 11 00 00 05 4c 49 4e 43 35 01 04 82 84 8b d....LINC5....
00000030: 96 03 01 01 |...
```

Mitigating the Threats

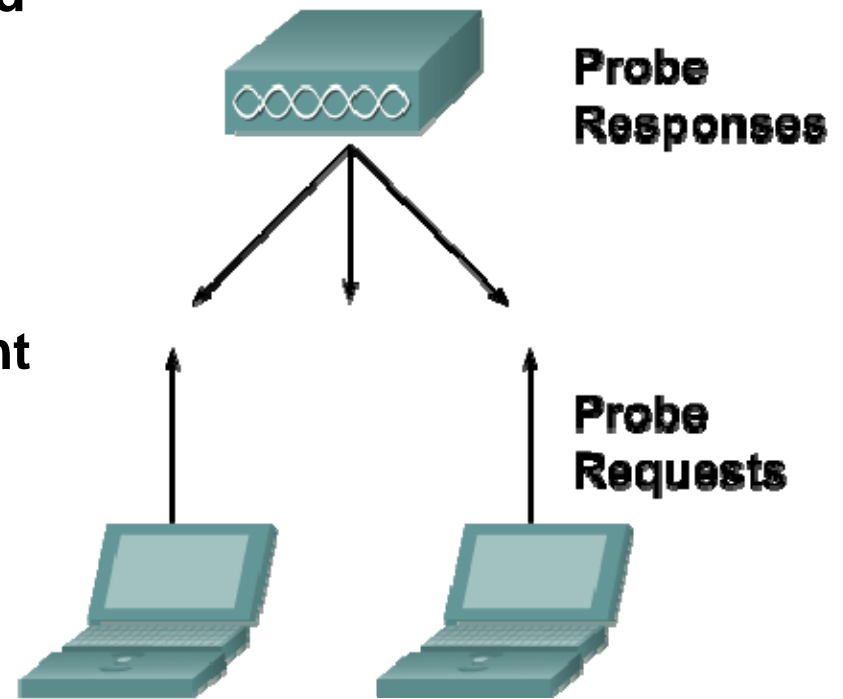
Control and Integrity	Privacy and Confidentiality	Protection and Availability
Authentication	Encryption	Detection System (IDS)
Ensure that legitimate clients associate with trusted APs.	Protect data as it is transmitted and received.	Track and mitigate unauthorized access and network attacks.

Evolution of Wireless LAN Security

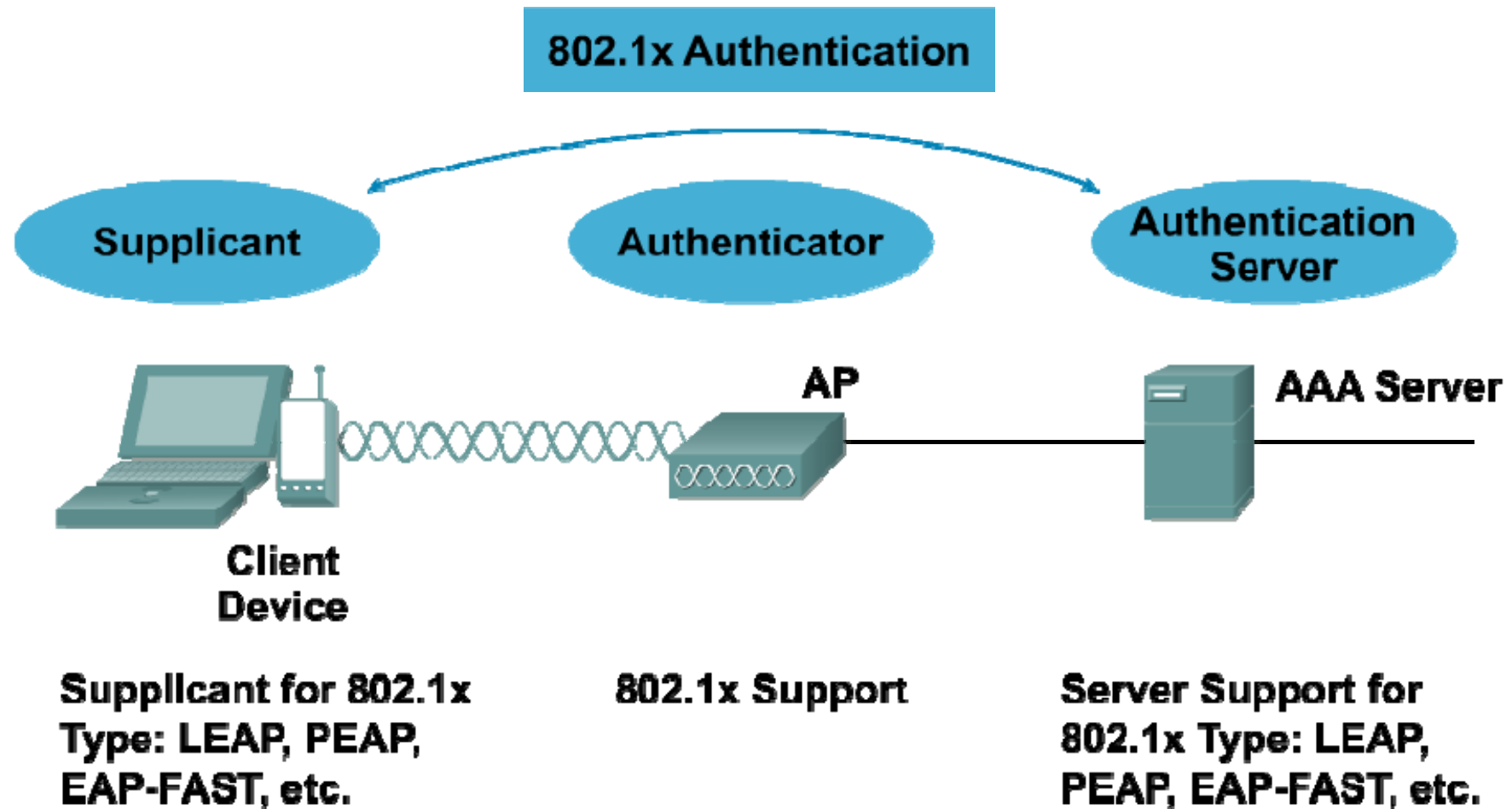


Wireless Client Association

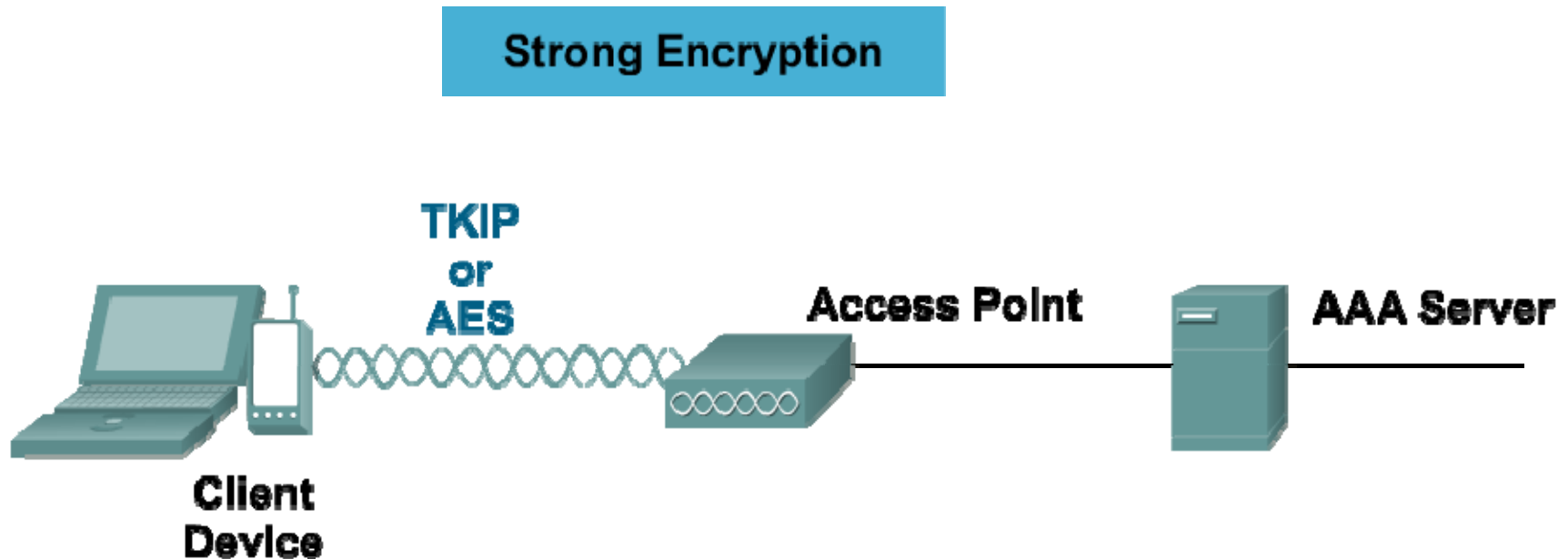
1. Access points send out beacons announcing SSID, data rates and other information.
2. Client scans all channels.
3. Client listens for beacons and responses from access points.
4. Client associates to access point with strongest signal.
5. Client will repeat scan if signal becomes low to reassociate 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

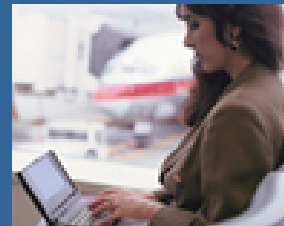
**802.1x, TKIP Encryption,
Mutual Authentication,
Scalable Key Mgmt., Etc.**



Enterprise

Remote Access

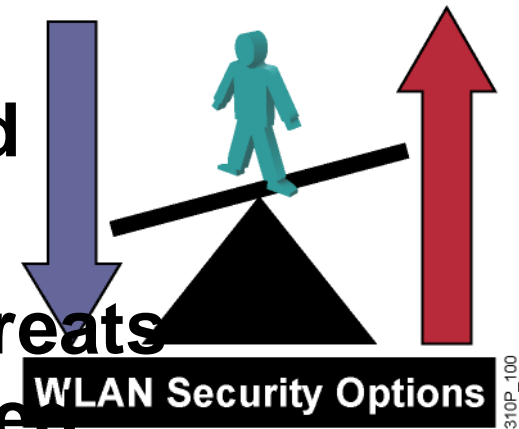
**Virtual
Private
Network
(VPN)**



**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>

