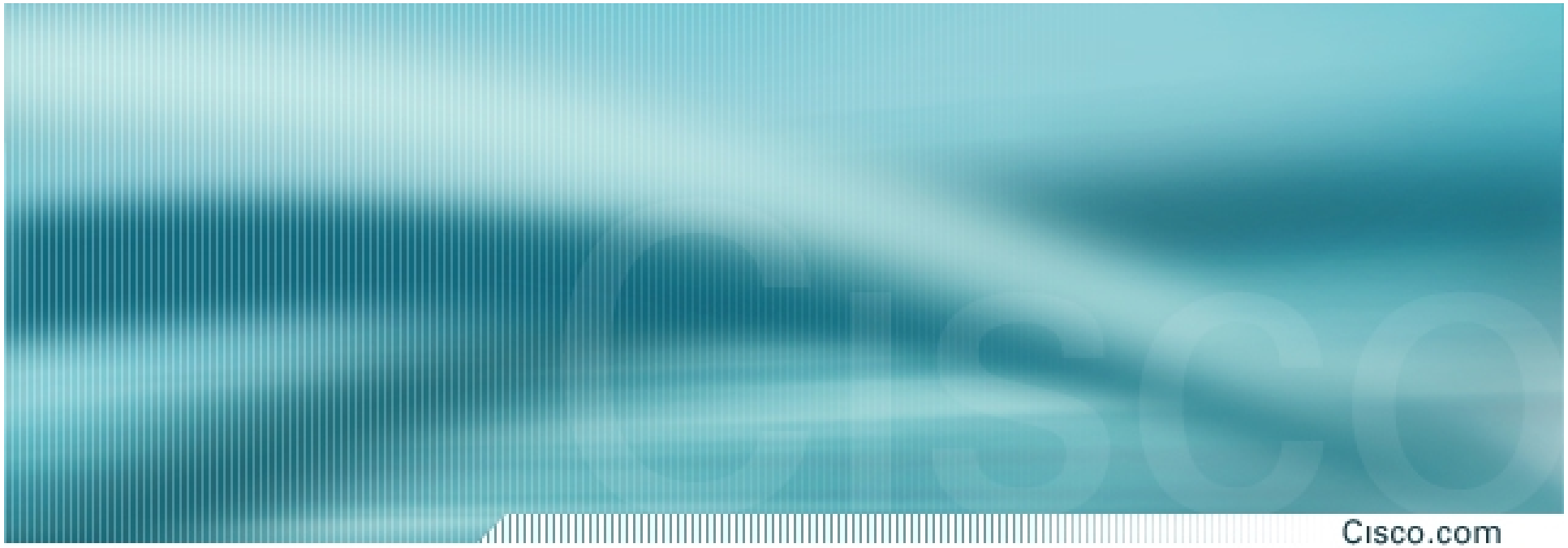
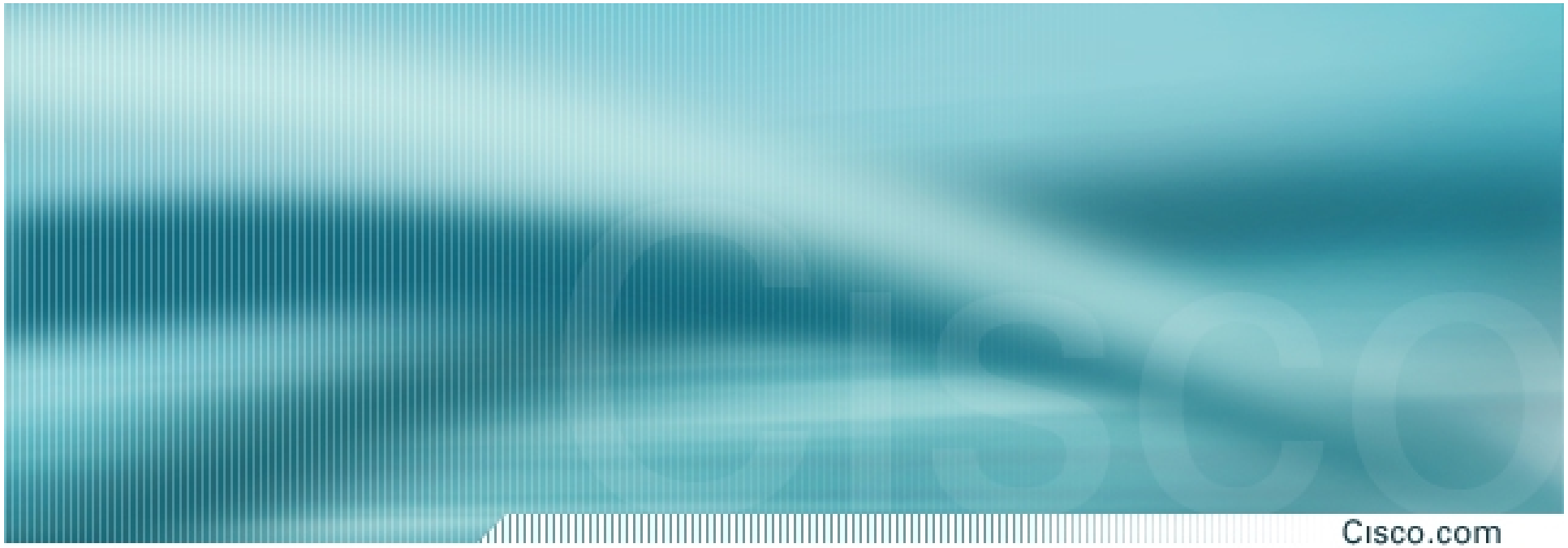


Wireless LAN Security

Thomas Latzer - tlatzer@cisco.com

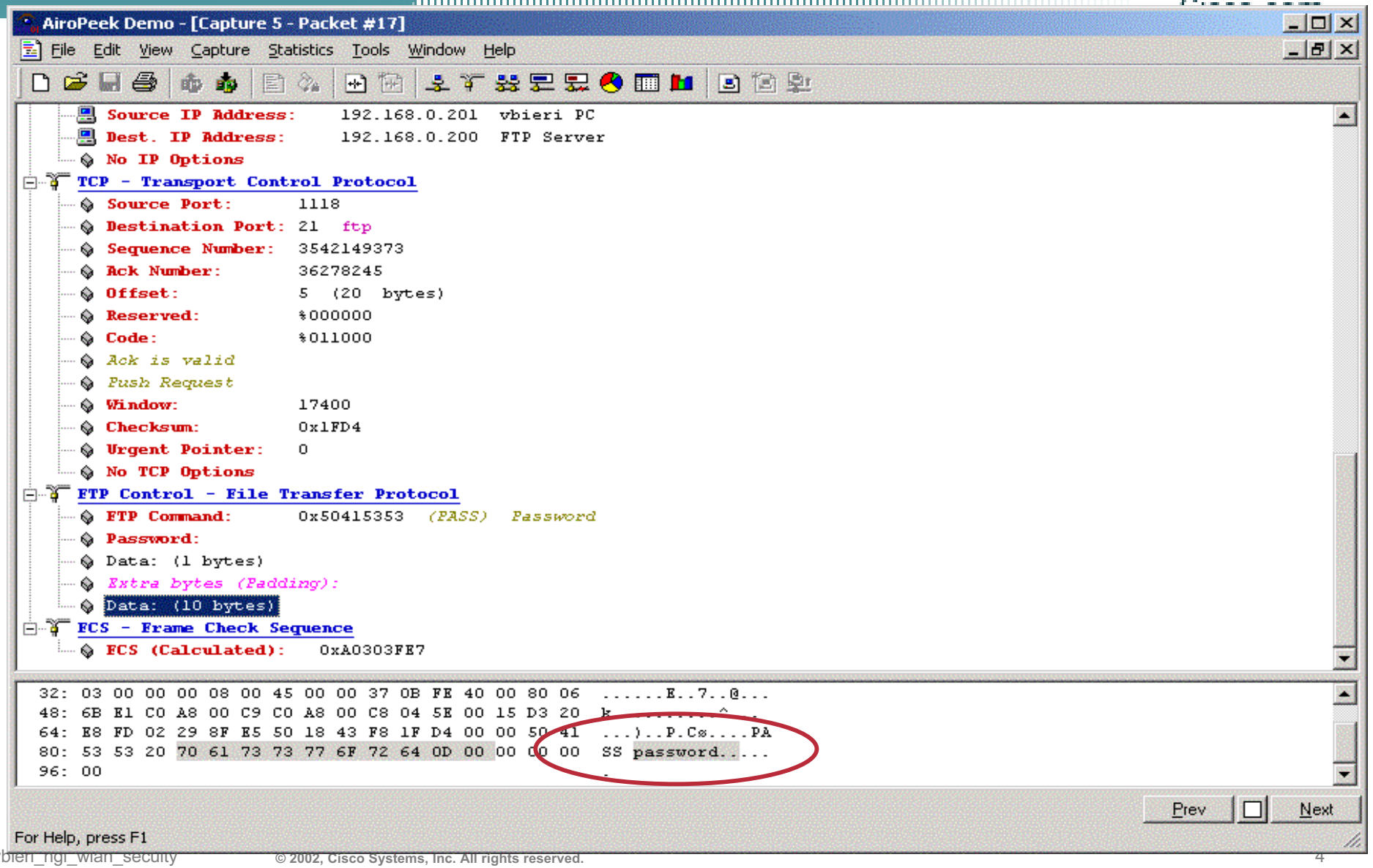
Agenda

- 802.11 WLAN Security Features
- 802.11 Security Issues
- 802.1X and EAP for 802.11
- Cisco Security Extensions
- Standard Update



802.11 WLAN Security Features

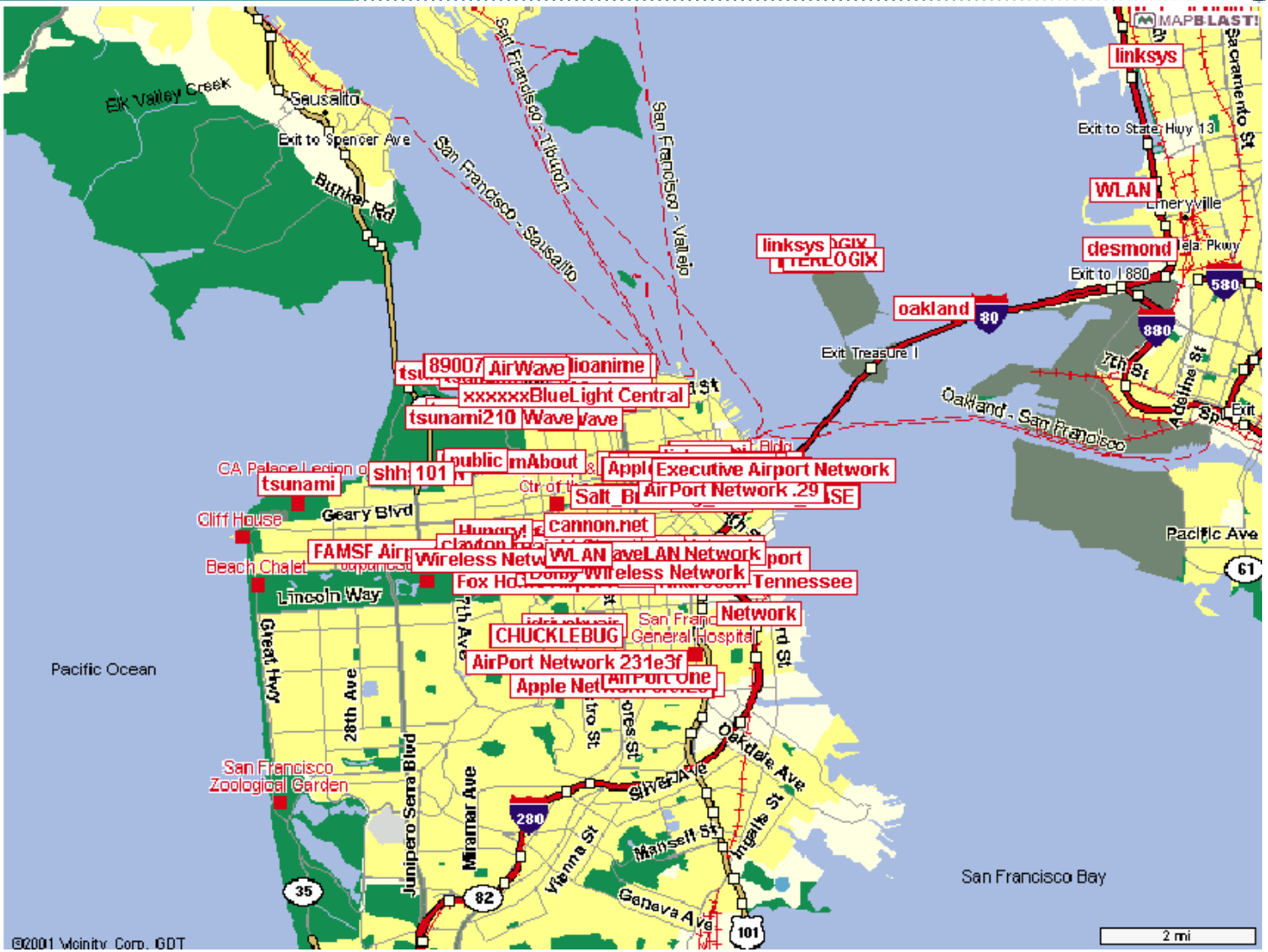
Traffic is in the Clear



SSID problem

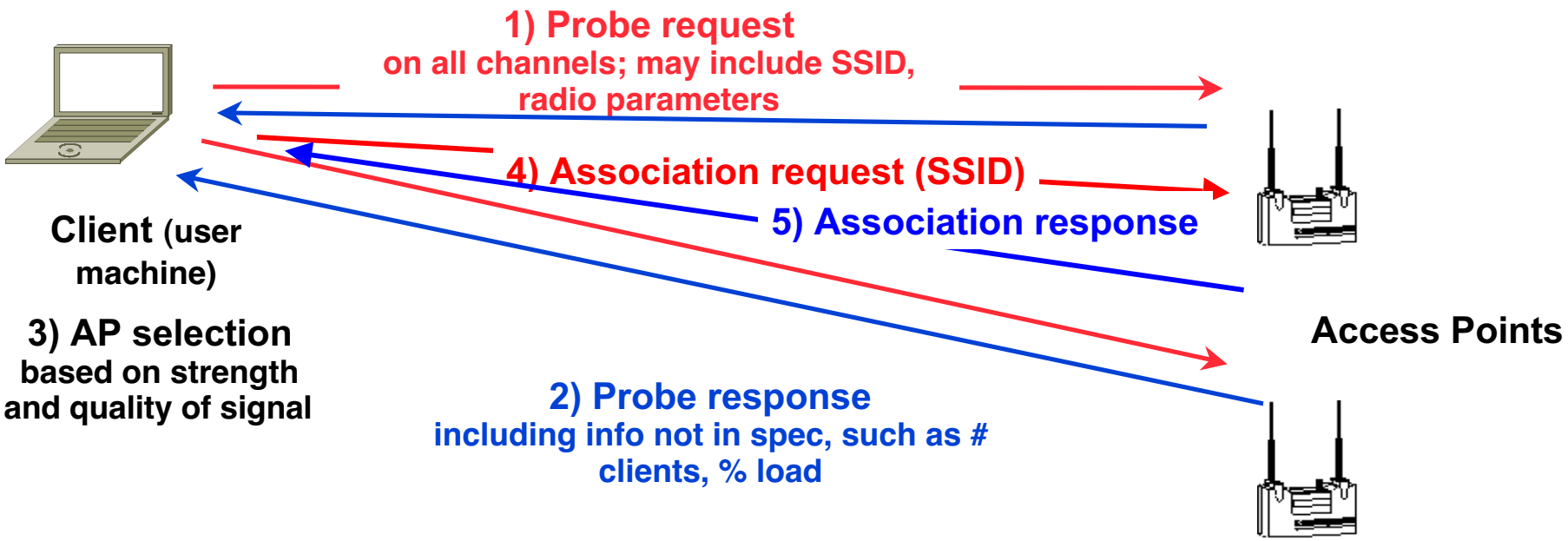
- **32 ASCII characters string**
- **Sent in the clear** *(see AP beacon and STA probe frames)*
- **Under 802.11, any client without SSID will associate to any AP regardless of AP's SSID**
- **AP Beacon frames used by Windows XP to present the list of available SSID**
- **This is NOT a security feature!**

War Driving…



Association Using 802.11SSID

- **Association is the process of associating a client with a given access point (described here without SSID beacon frames)**



MAC Filtering

- A list of allowed or disallowed MAC addresses
- Same shortcomings as static WEP key management

Wired Equivalent Privacy - WEP

- **Prevent link-layer eavesdropping**

  → not end-to-end security

- **As secondary role WEP controls network access**

- **Uses the RC4 stream cipher of RSA Data Security for encryption**

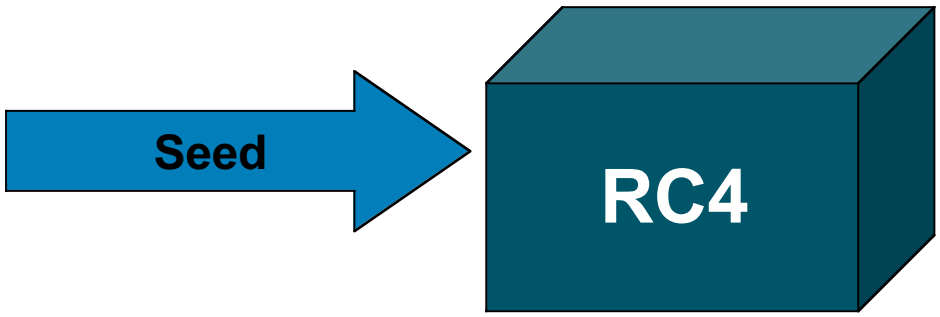
- **Key must be shared by both the access point and mobile stations.**

WEP (Cont.)

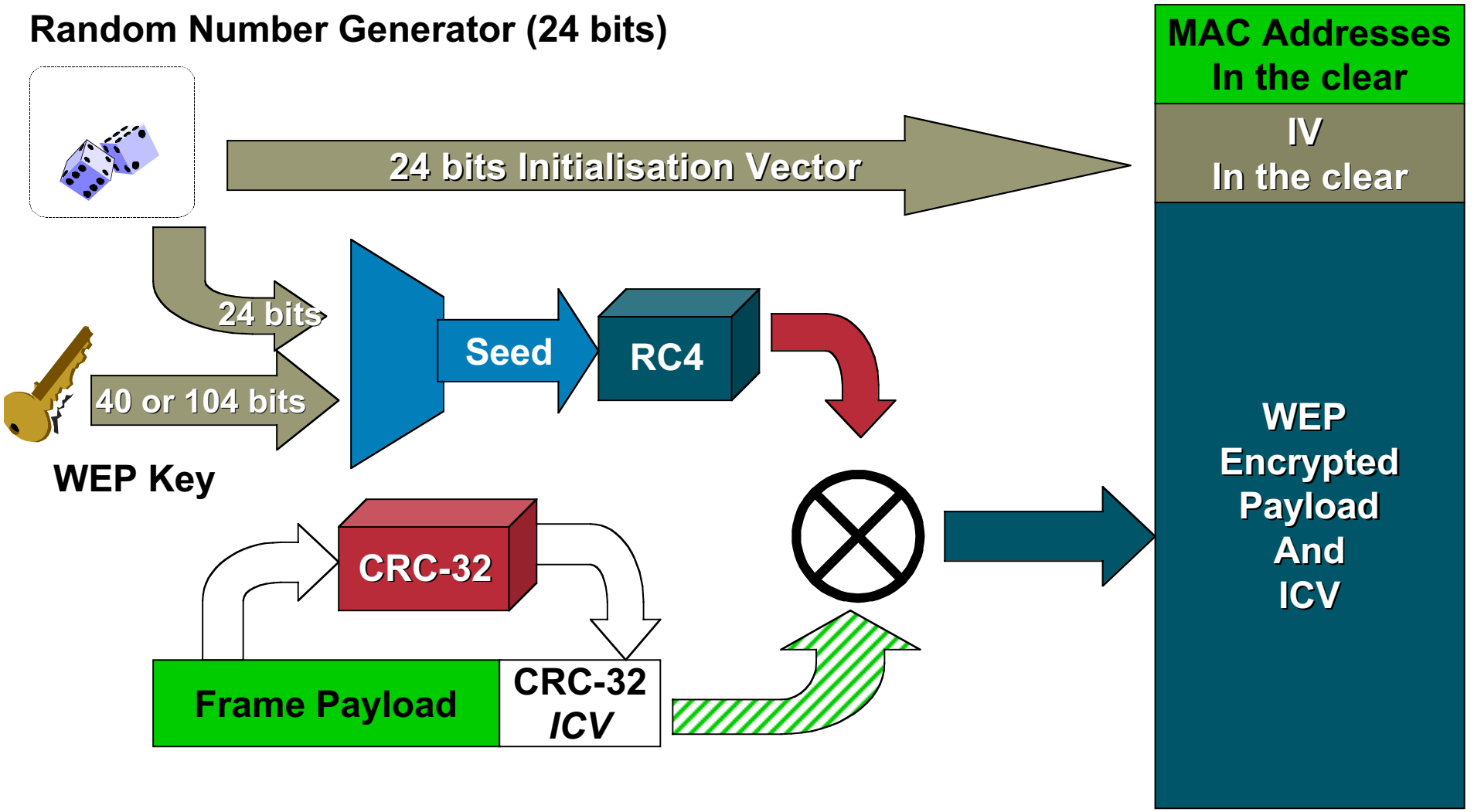
- IEEE choose to use 40-bits keys.
- Several vendors use 104-bits keys
- Only a few have implemented WEP in HW.
- Each frame includes an integrity check value, ICV, based on CRC-32, which is encrypted by WEP
- The MAC addresses are sent in the clear
- Key distribution / negotiation is not mentioned in the standard.

Stream Ciphers

- **RC4 is a stream cipher** *(used notably by SSL)*
- **Expands a key** *(also called seed)* **into an infinite pseudorandom bit stream** *(called key stream)*



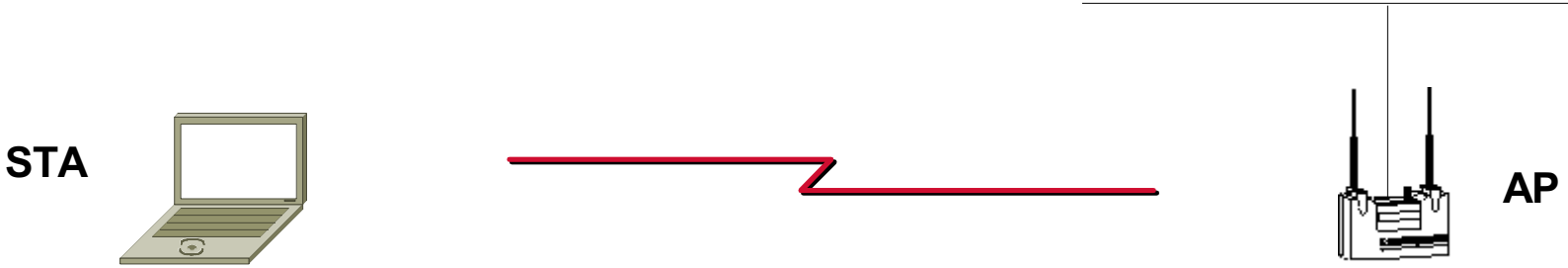
802.11 WEP Encryption



Association != Authentication

- Association is the process of associating a client (STA) with an access point (AP)
- Authentication is the process of verifying the credentials of a STA desiring to associate to an AP

802.11 Client Authentication



Open Authentication

Authentication request →

← Authentication response

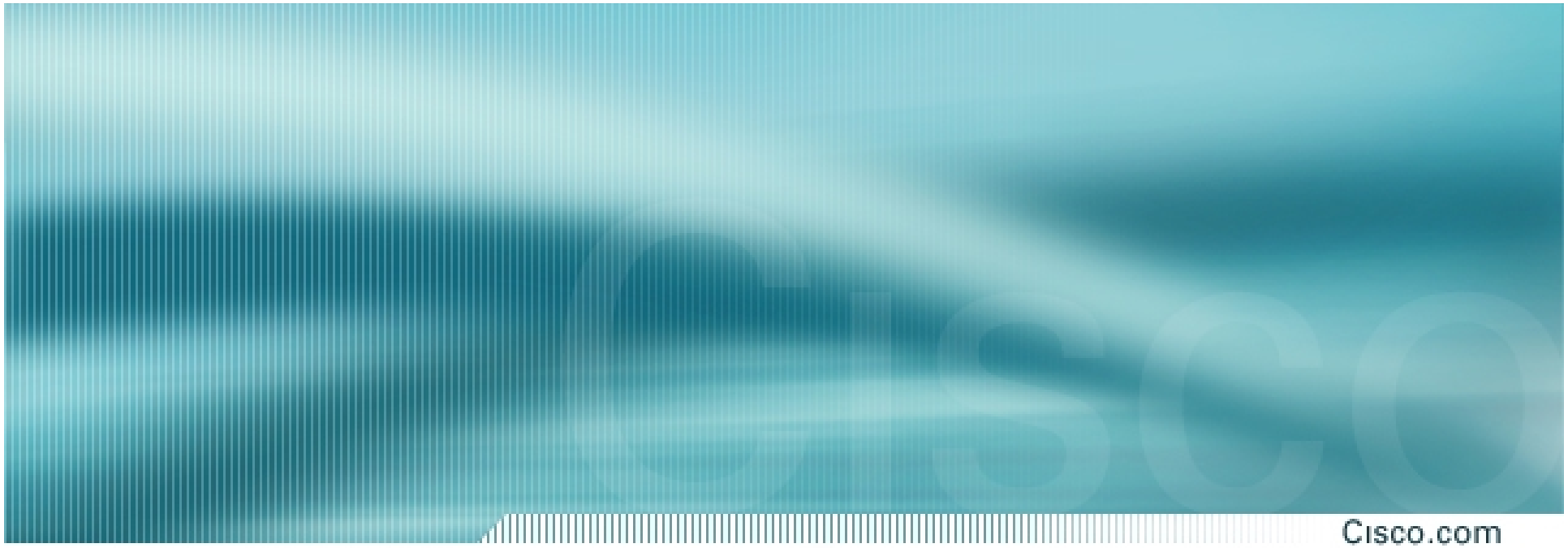
Shared-Key Authentication

Authentication request →

← 128 bits Challenge text packet

WEP Encrypted challenge text packet →

← WEP Encrypted Authentication response



802.11 Security Issues

Issues of WEP

- Stateless Protocol
  - → Replay Attack
- Linear Checksum
  - → Packet Modification (bits flip)
- IV Reuse (Collision)
- Key stored in NIC
- Bad IV for RC4 (airsnort)

Bad IV For RC4

- FMS Attack, July, 25th, 2001
- Paper from S. Fluhrer (Cisco Systems), I. Mantin and A. Shamir (Weizmann Institute)

  WEP 40 bits cracked in 15-30 minutes

  scales linearly with key length
- Leverages 'Weak' IVs

  large class of weak IVs that RC4 is using

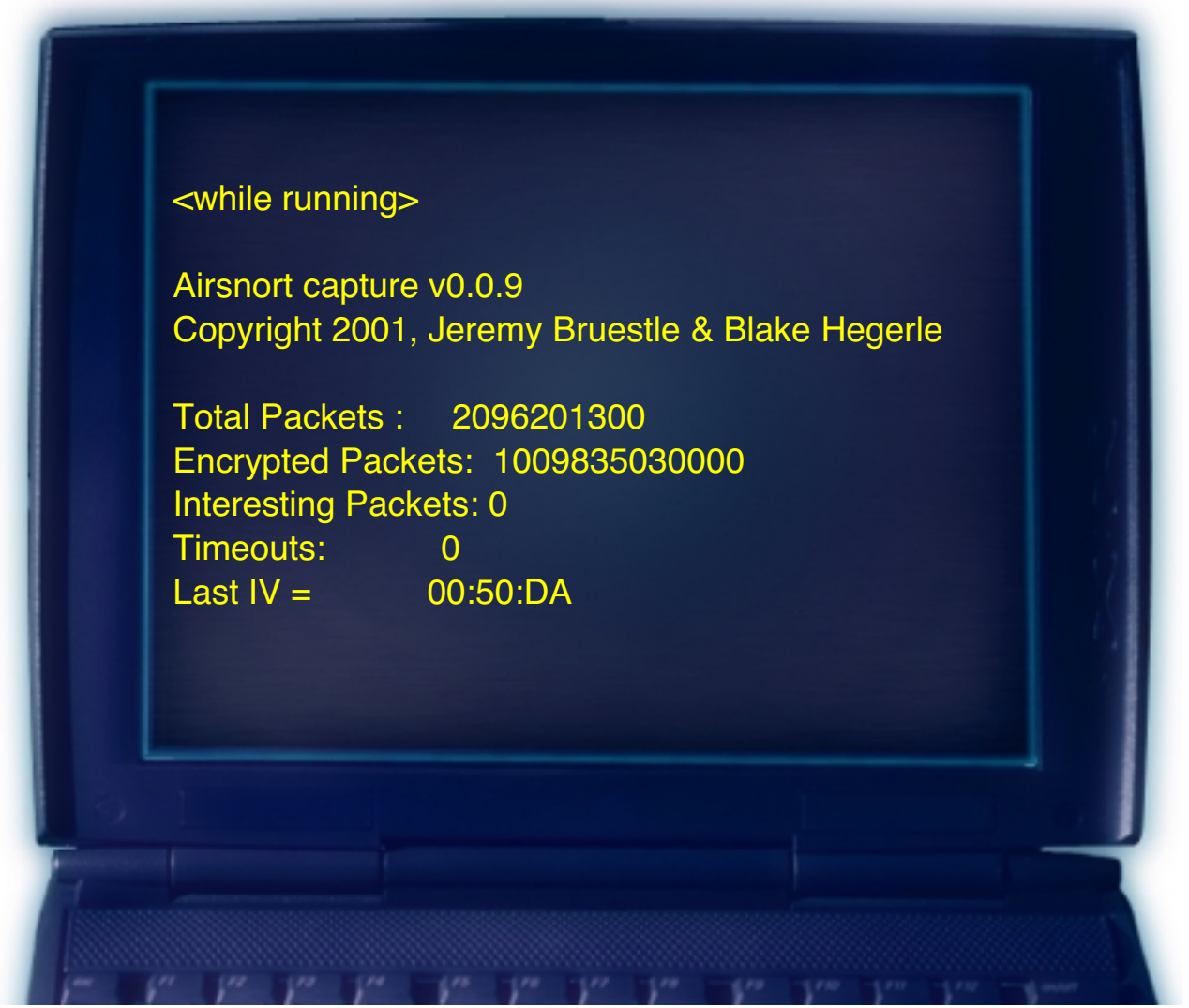
  passive attack, but can be more effective if coupled with active attack.

Airsnort (1)

- Capture enough packets

- A passive listener can recover the secret WEP key by listening into enough packets.

- Enough = 5-6 millions packets



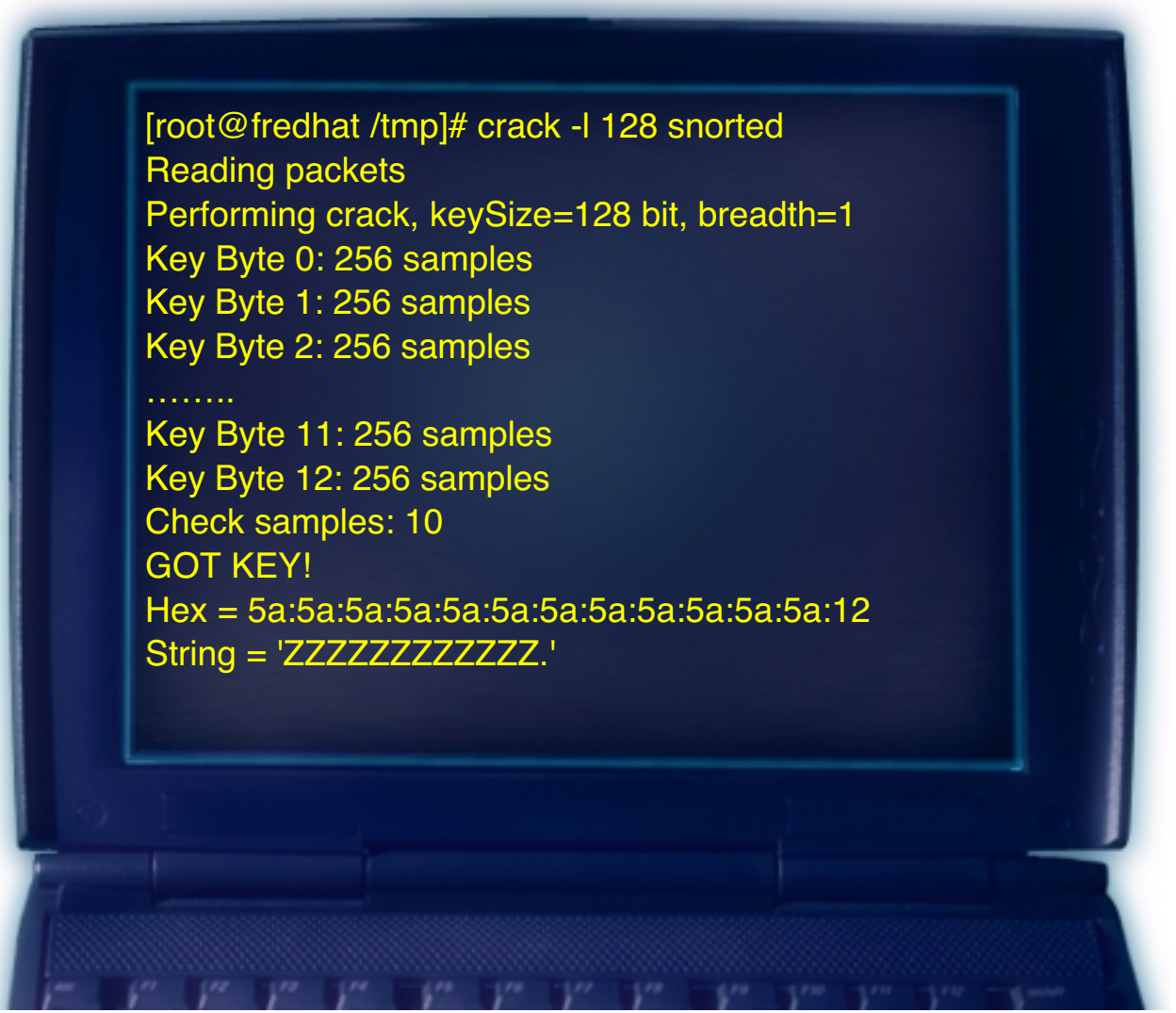
Airsnort (2)

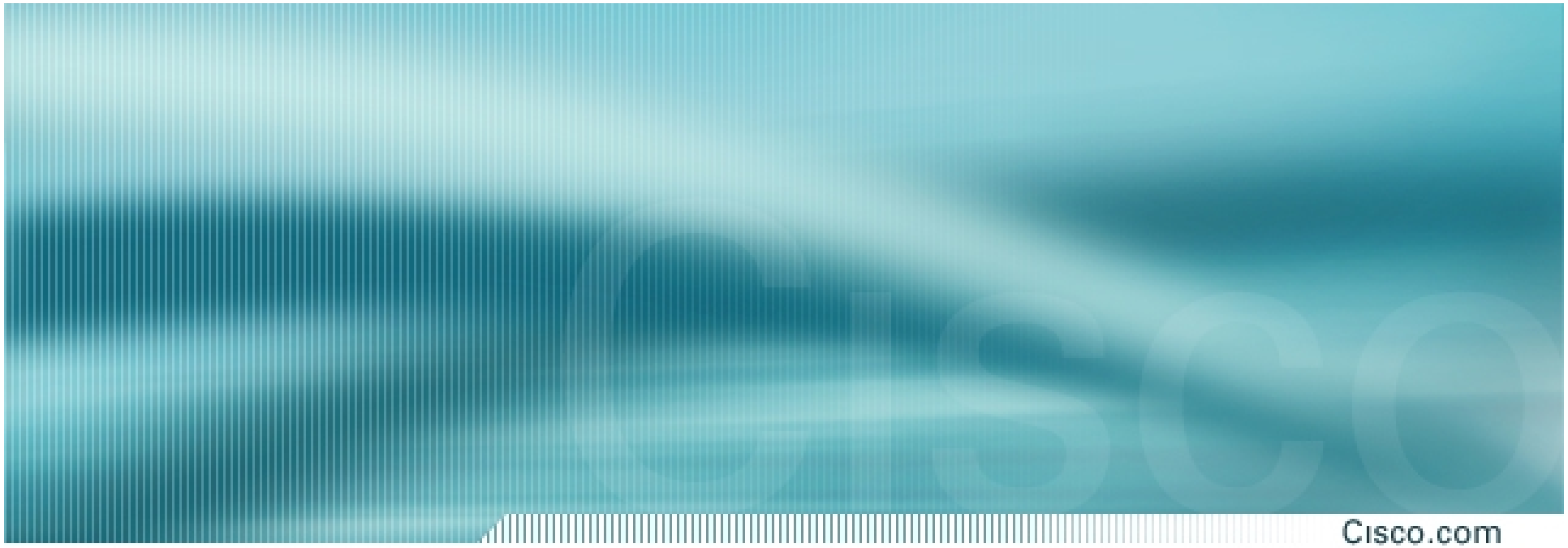
- Crack phase

- For every byte of the key, there are 256 weak IVs.

- 13 key bytes * 256 = 3315 packets to get all weak keys

- You do not need sometimes all of the weak keys to break the WEP key





802.1X and EAP for 802.11

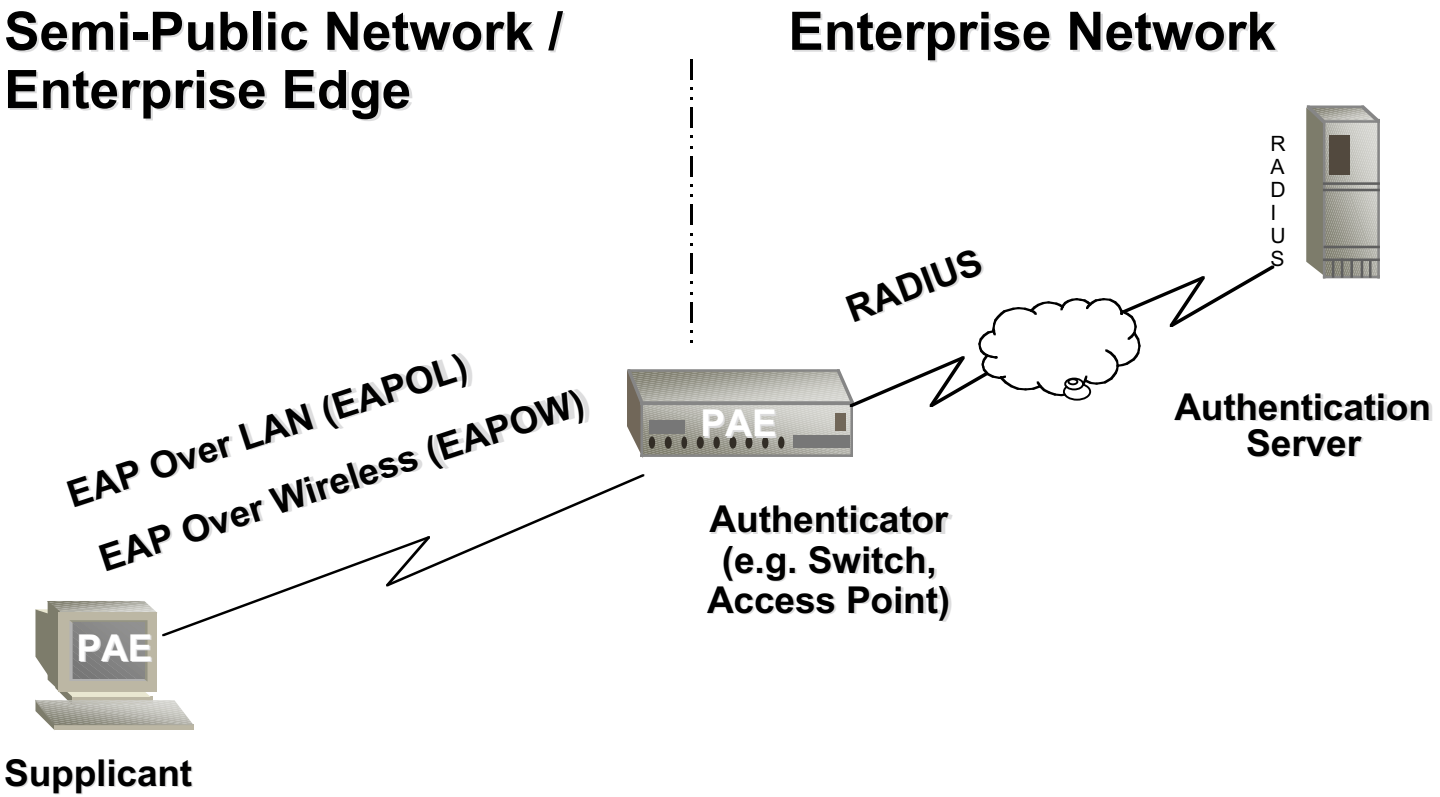
Advantages of 802.1x for Wireless LAN Security

- **Improved user authentication: username and password**
- **Dynamic, session-based encryption keys**
- **Centralized user administration**

  RADIUS support (RFC 2138, 2139) for centralized authentication, authorization, and accounting

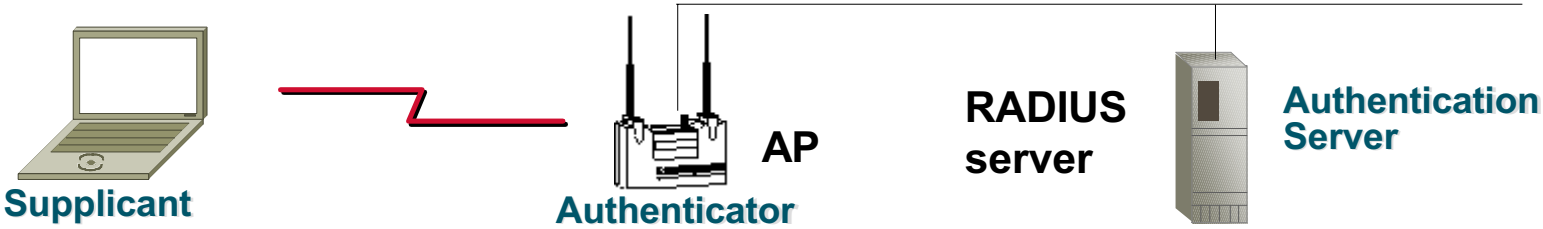
  RADIUS/EAP (draft-ietf-radius-ext-07.txt) for forwarding of EAP packets within RADIUS

General Description IEEE 802.1X Terminology



801.X/EAP Steps

Cisco.com



EAPOL Start → — Start process

← Identity request — Ask client for identity

Identity response → — Provide identity

Access request → — Pass request to RADIUS

← Access challenge

← EAP request

EAP response →

Perform sequence defined by authentication method (e.g. EAP-TLS, LEAP)

Client receives or derives session key

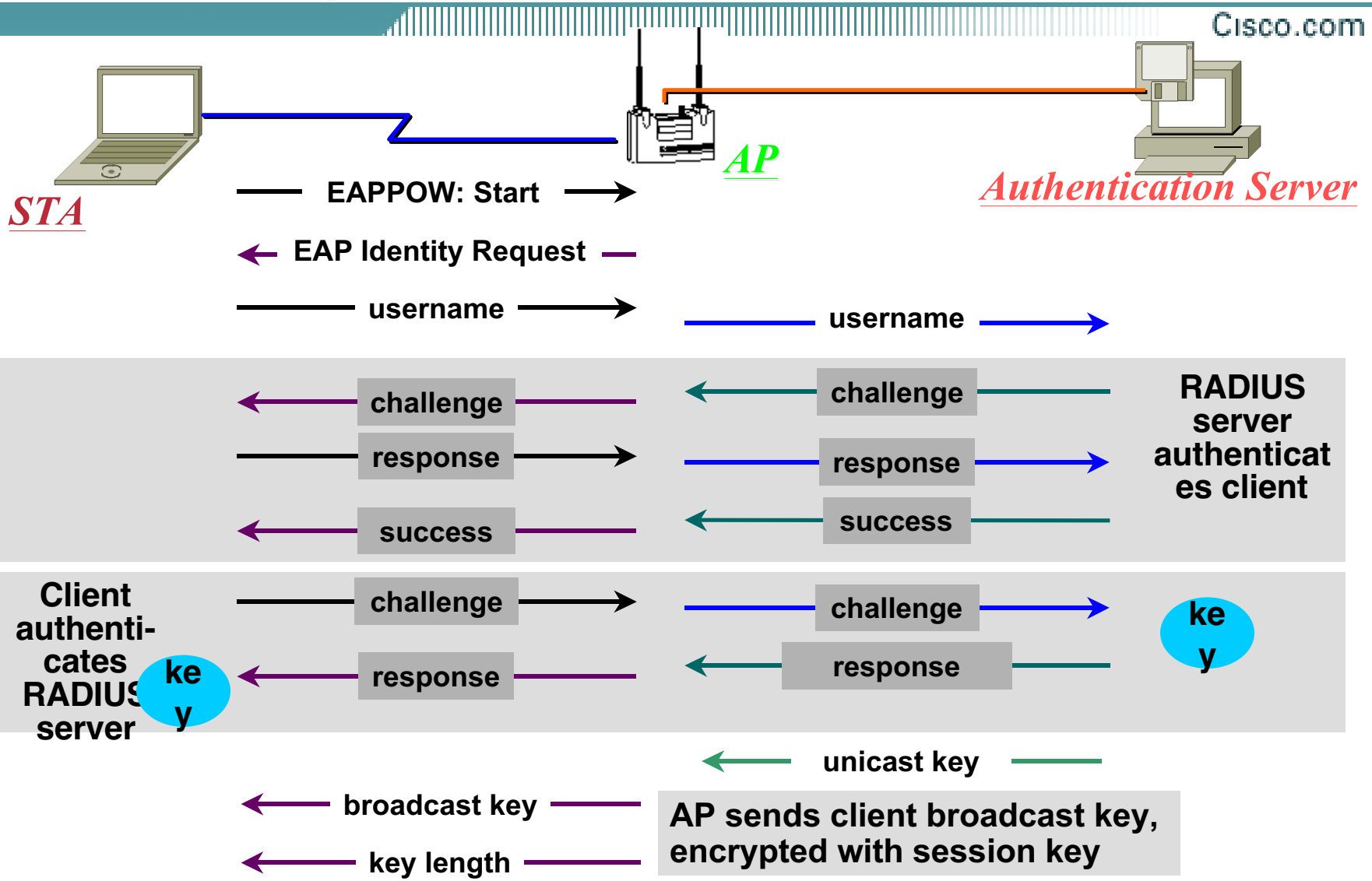
Access request →

← Access success — Pass session key to AP

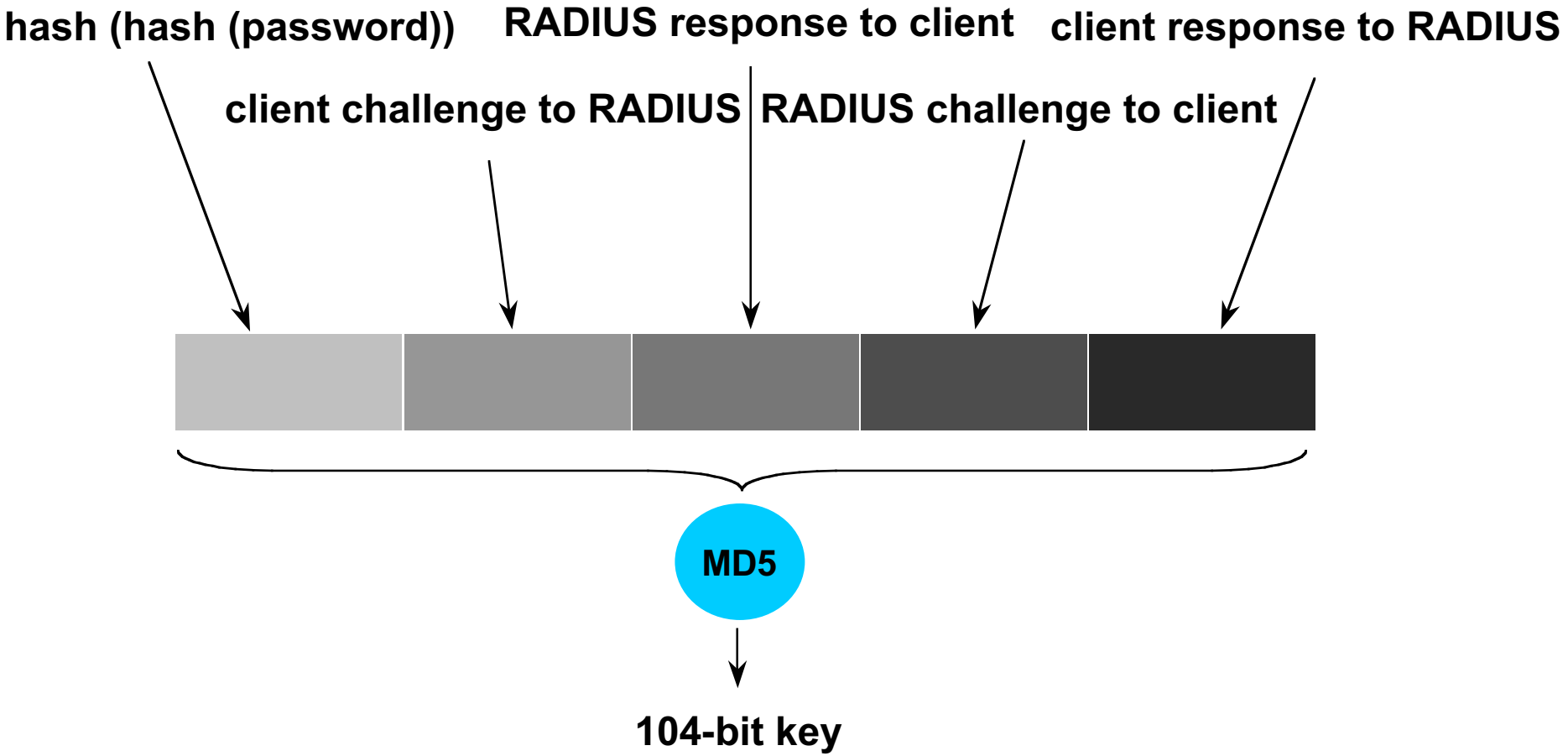
← EAP success — Start using WEP

← EAPOW key — Deliver broadcast key, encrypted with session key

LEAP Steps: Cisco Mutual Authentication

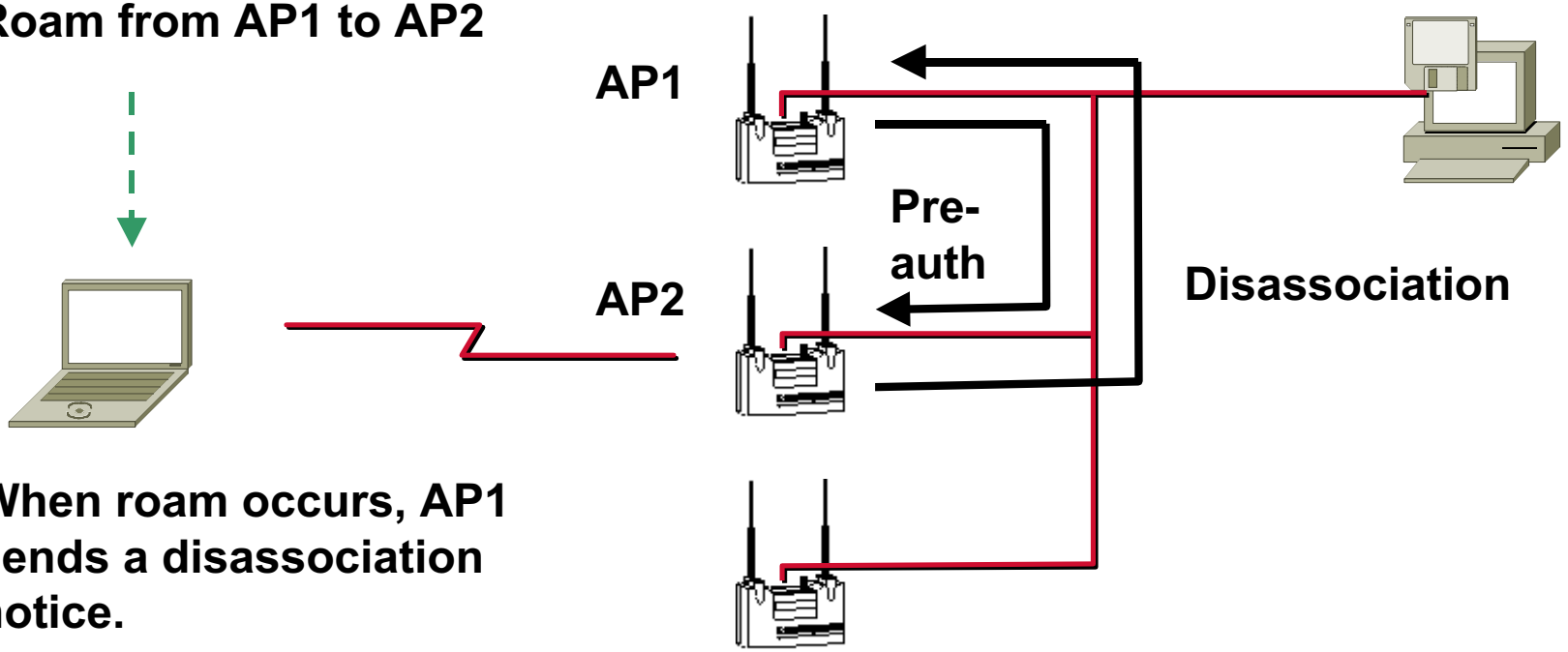


Deriving the Session Key (Cisco LEAP)



Pre-Authentication and Roaming

Roam from AP1 to AP2



When roam occurs, AP1 sends a disassociation notice.

AP2 associates client, cached key and retrieves queued data from AP1.

Availability

- Cisco Aironet access points support 802.1X and EAP

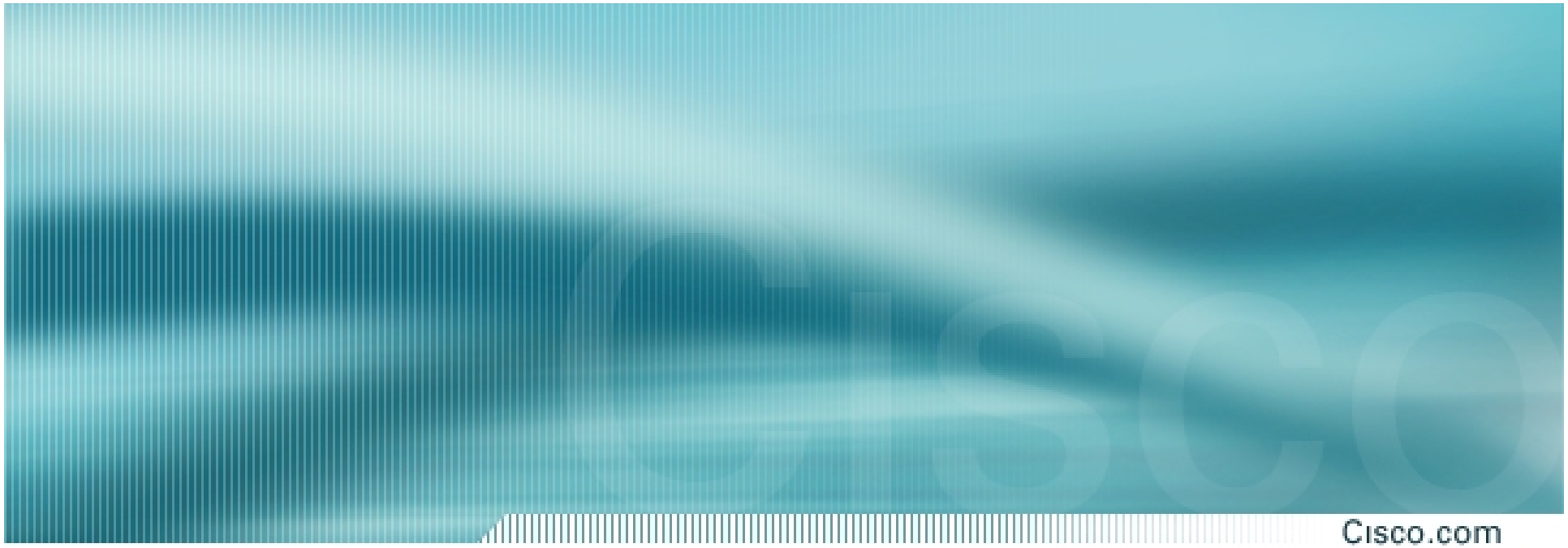
  AP can act as 802.1X “middleman” when wireless client and authentication (RADIUS) server support authentication type

- Cisco introduced LEAP in December 2000

  Is supported by Cisco Aironet client adapters on wide range of client operating systems (Windows, CE, Mac OS, Linux)

- Microsoft supports EAP-TLS authentication type in Windows XP and Windows CE 4.0

  Cisco supports EAP-TLS with its client adapters (for the above OS’es) and APs



Cisco Security Extensions

Cisco Security enhancements

- December Release 11.10T
- Key Hashing to address WEP vulnerabilities

  → defeats airsnort
- New Message Integrity Check (better than CRC-32)

  → to address Bit Flipping and Replay attacks
- Broadcast Key rotation for LEAP

  → periodic change of Bcast key, generated by AP, sent to STA encrypted using their unicast WEP keys
- Pre-standard implementations

Message Integrity Check

- **The MIC will protect WEP frames from being tampered with.**
- **The MIC is based on Seed value, Destination MAC, Source MAC, and payload.**

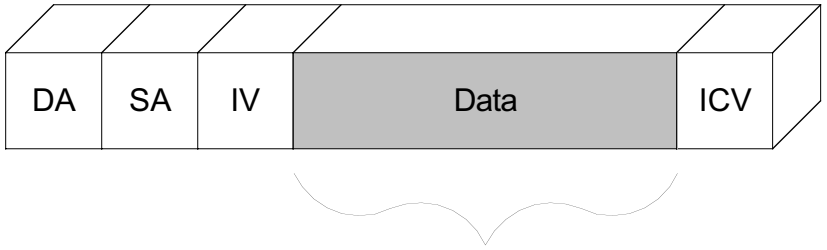
  Any change to these will change MIC value
- **The MIC is included in the WEP encrypted payload**

Message Integrity Check

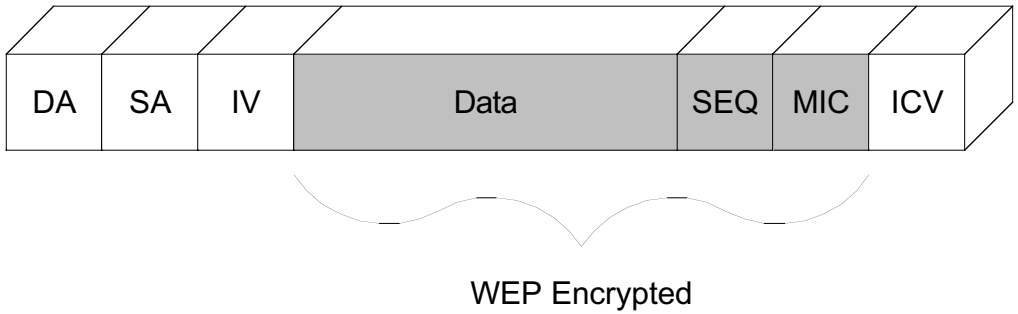
- **Unlike CRC32, MIC uses a hashing algorithm to stamp frame.**
- **The MIC is still pre-standards, so this is currently Cisco Proprietary.**

Message Integrity Check

WEP Frame - No MIC



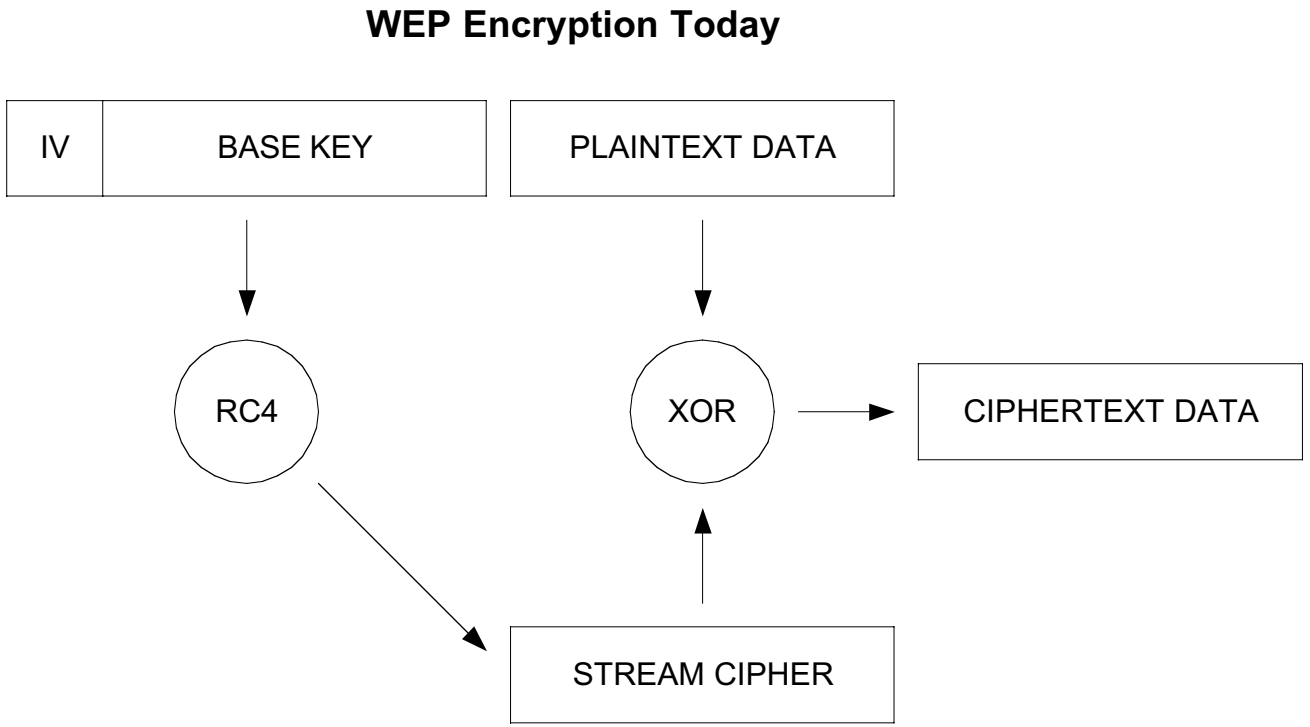
WEP Frame - MIC



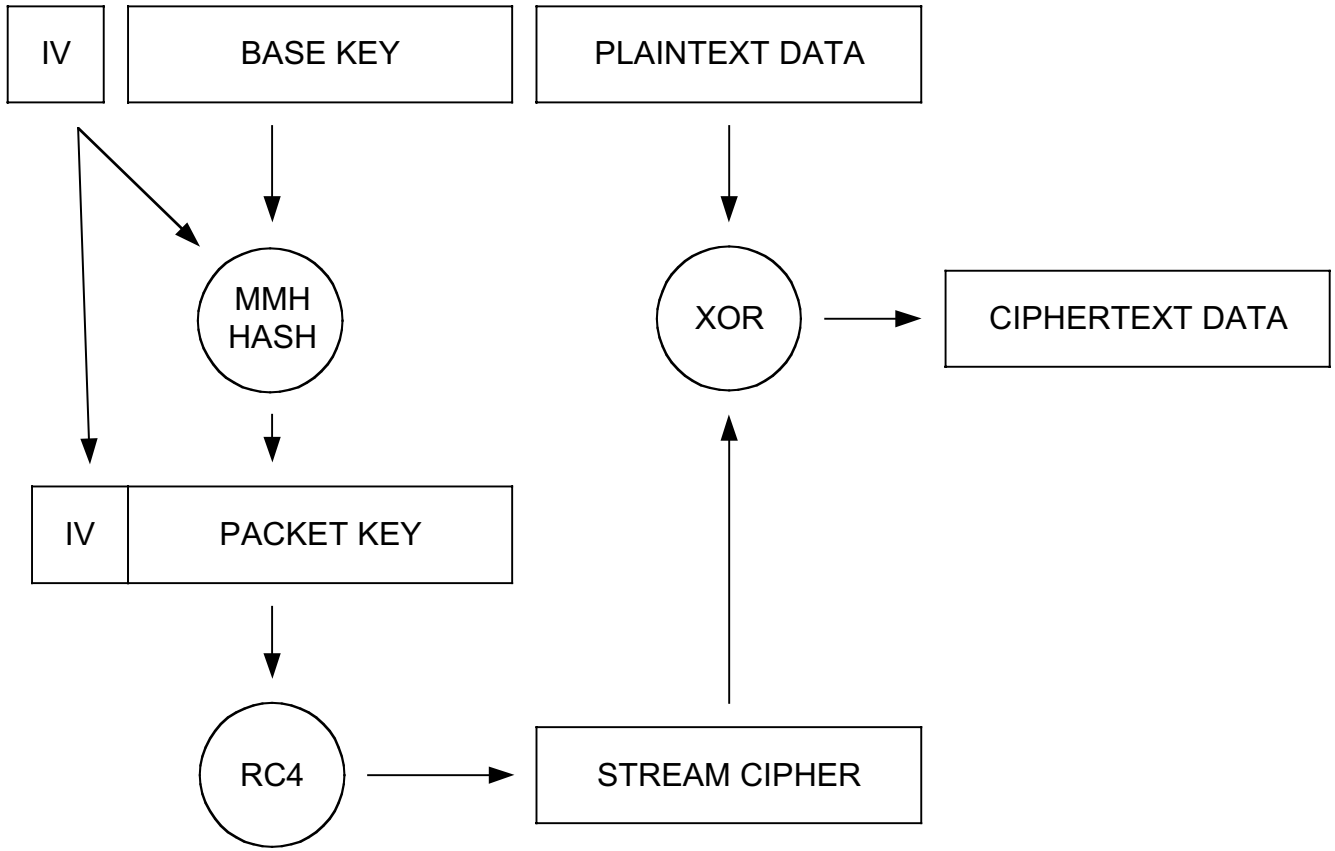
WEP Key Hashing

- **Base key and IV hashed**
  - **Transmit WEP Key changes as IV changes**
- **Cisco Proprietary**

WEP Key Hashing



WEP Key Hashing



WEP Key Hashing

- Hash function includes the AID (association ID) in the generation of the hash key.
- Ensures that the key generated is different for each connection to avoid IV collisions.
- The uplink (packets to AP) will use even IV and downlink (packets from AP) will use odd IV.
- IV will increment on transmits. An anti-replay measure will verify that any receive packets with an old IV will be dropped

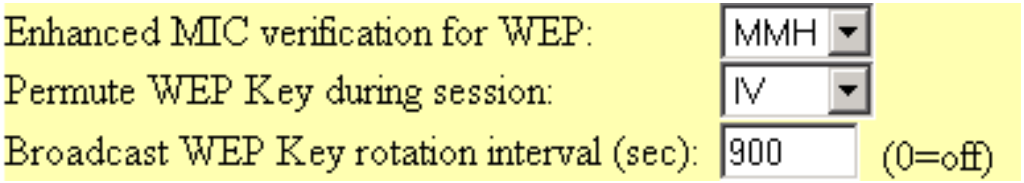
Broadcast Key Rotation

- Pre 11.10T Broadcast Key is static
- Static Broadcast Key is vulnerable to the Weak IV attack over time
  - Similar to Pre-11.10T WEP Keys

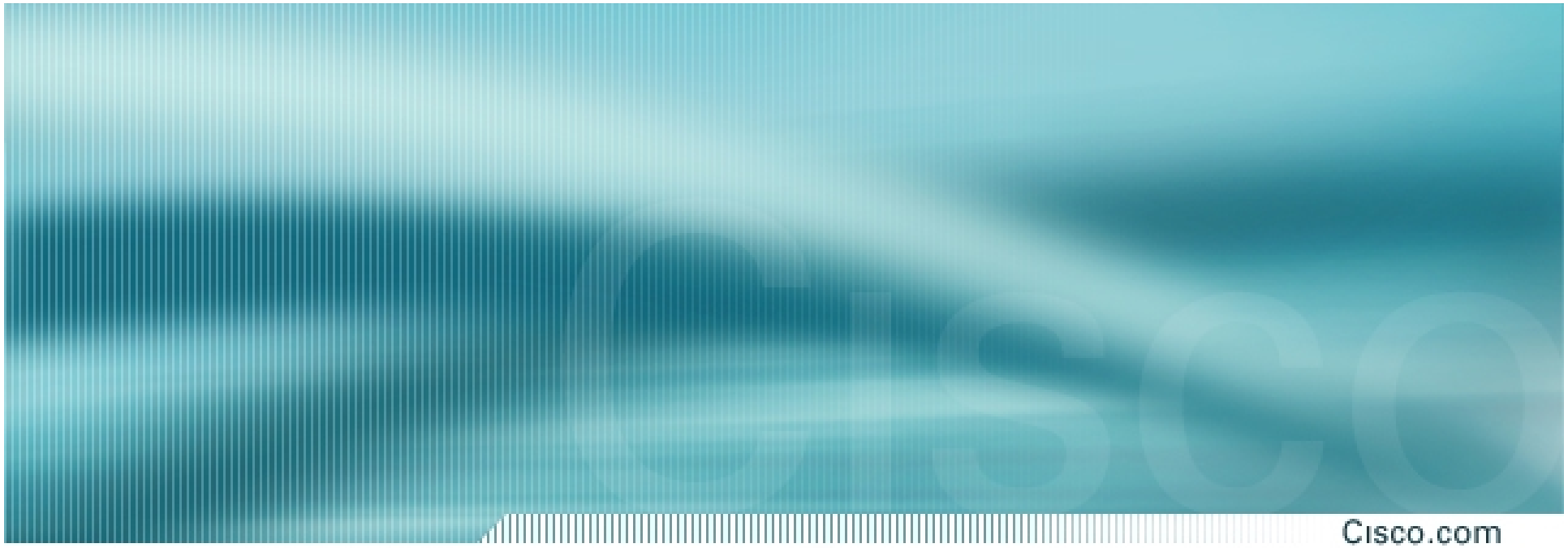
Broadcast Key Rotation

- Using Broadcast Key rotation will prevent static WEP users from functioning correctly.
- BK = Hash (seed, ap_mac_addr, nboots)
- This will be remedied in December release Phase 2 (11.10T).

Configuring Security Enhancements



- **Setup -> AP Radio Advanced Screen**
- **MIC**
  - **MMH Algorithm available for generating MIC**
- **Key Hashing**
  - **Permute WEP key using IV**
- **Broadcast Key rotation**
  - **Key timeout value, in seconds**
  - **Should match session timeout value in ACS server**
  - **Configured on a per AP basis**

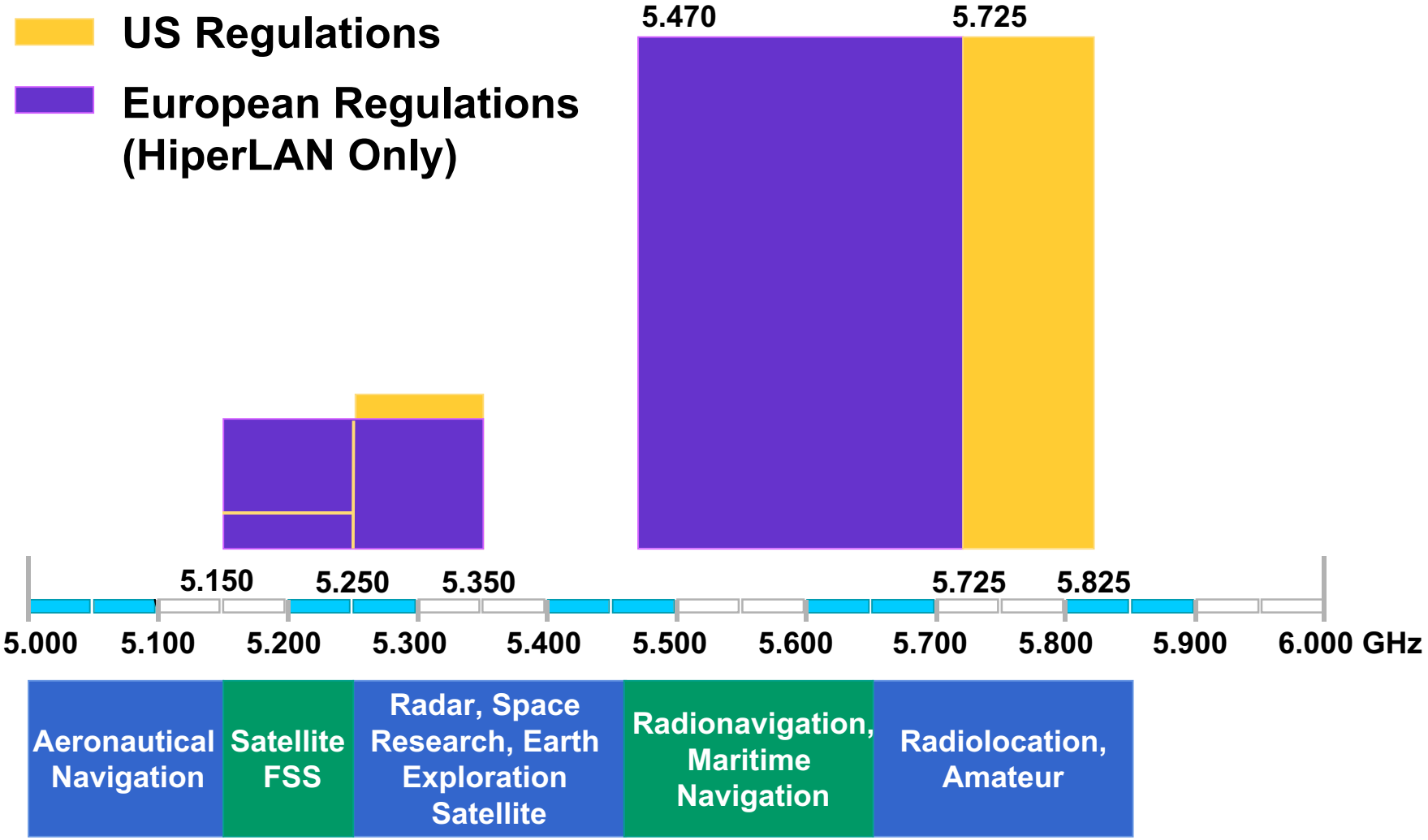


Standard Update

IEEE 802.11 Standard Activities

- 802.11a - 5GHz- ratified in 1999
- 802.11b - 11 Mbps, 2.4 GHz, ratified in 1999
- 802.11d - World Mode and additional regulatory domains - ratified
- 802.11e - Quality of Service
- 802.11f - Inter-Access Point Protocol (IAPP)
- 802.11g - Higher Data rate (>20 Mbps) 2.4GHz
- 802.11h - Dynamic Frequency Selection and Transmit Power Control mechanisms
- 802.11i - Authentication and security

Implementation Differences
5 GHz Spectrum Harmonization



802.11h- Spectrum Managed 802.11a

- Still in Draft mode
- Dynamic Frequency Selection (DFS)

  Enables transmitter to move to another channel when is encounters other RF on its channel
- Transmit Power Control (TPC)

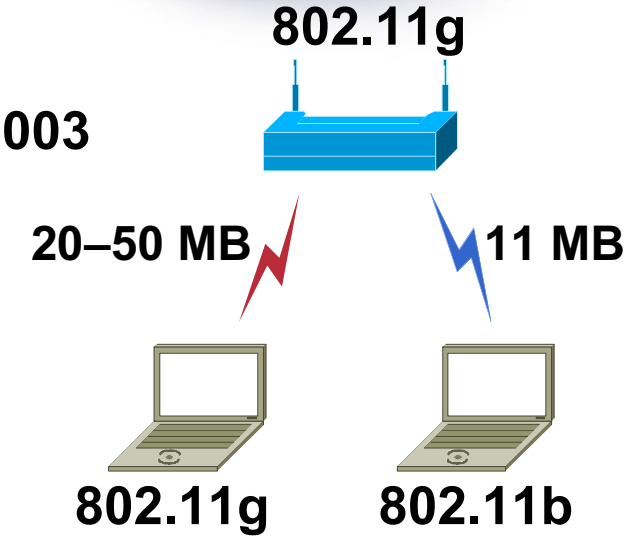
  Provides minimum required transmitter power for EACH user

  Provides minimal interference to any other users or system
- ETSI Requirement for 5 GHz

IEEE 802.11g

Standard for Higher Rate (20+ Mbps) Extensions in the 2.4 GHz Band

- Working on Draft for Letter ballot passed the task group committee in Nov.
- Provides higher data rates @ 2.4 GHz
- Similar speeds as 802.11a
- Backward compatible with 11 Mbps (802.11b
- Same modulation as 802.11a—OFDM
- Estimated to complete specification in Jan 2003



Standards Update

- **802.1X Current Status**

  draft: http://grouper.ieee.org/groups/802/1/pages/802.1x.html

  last update March 27, 2001

- **802.11 Security**

  TG e (Task Group E and I) Working on security and QoS extensions to the MAC 802.11 layer

  TG-e Security sub-group chair : Dave Halasz (Cisco- Aironet Engineering)

  joint multi-vendor 802.1X for 802.11 proposal accepted as baseline security document.

IEEE 802.11i Security

- **Passed 1st letter ballot (Draft currently at version 1.6)**
  - **Fixes to WEP (Software)**
  - **New AES proposals (Requires Hardware Changes)**
    - **All MIC/IV Hash/IV Sequencing/Rapid Rekey to informative text:** passed
    - **Replace WEP2 with TKIP :** passed
  - **TKIP (Temporal Key Integrity Protocol)**
    - **Text/hash function/MIC etc is Work in Progress.**
    - **11.10T is an early implementation**

Summary

- 802.11 security doesn't meet any of its security objectives today
- 802.11 TGi is working to replace
  - authentication scheme using 802.1X and Kerberos
  - encryption scheme using AES in OCB mode
- Cisco Aironet Solution already implemented 802.1X draft to provide enhanced WLAN security services
- Always possible to setup IPSec/VPN !!!

Reference Papers

- **IEEE 802.1X**
  http://grouper.ieee.org/groups/802/1/pages/802.1x.html
- **IEEE Wireless Standards**
  http://standards.ieee.org/wireless/
- **EAP**
  http://www.ietf.org/rfc/rfc2284.txt - http://www.ietf.org/rfc/rfc2716.txt
- **Microsoft EAP-TLS Support**
  http://www.microsoft.com/HWDEV/TECH/network/wireless/IEEE802Net.asp
  http://www.microsoft.com/HWDEV/TECH/network/802x/default.asp
- **Whitepaper : Security for Next Generation Wireless LANs**
  http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm
- **Unsafe at any key size**
  http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip
- **The insecurity of 802.11**
  http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- **Your 802.11 network has no clothes**
  http://www.cs.umd.edu/~waa/wireless.pdf
- **FMS Attack**
  http://www.crypto.com/papers/others/rc4_ksaproc.ps
  -http://www.cs.rice.edu/~astubble/wep/wep_attack.html
- **SAFE Wireless**
  –http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm
  –http://www.cisco.com/go/safe

The End…

- Thanks!
- Questions ?

- Thomas Latzer - tlatzer@cisco.com


Cisco Systems
Empowering the
Internet Generation℠