A Configuration Protocol for Embedded Networked Devices on Secure Wireless Networks

Larry M. Sanders, Joseph B. Evans
Info. & Telecom. Tech. Center
University of Kansas
Lawrence, Kansas 66045
{lsanders,evans}@ittc.ku.edu
www.ittc.ku.edu

Benjamin J. Ewy
Ambient Computing, Inc.
Lawrence, Kansas 66047
bewy@ambientcomputing.com
www.ambientcomputing.com

Seventh Annual Workshop on High Performance Embedded Computing
September 2003

University of Kansas

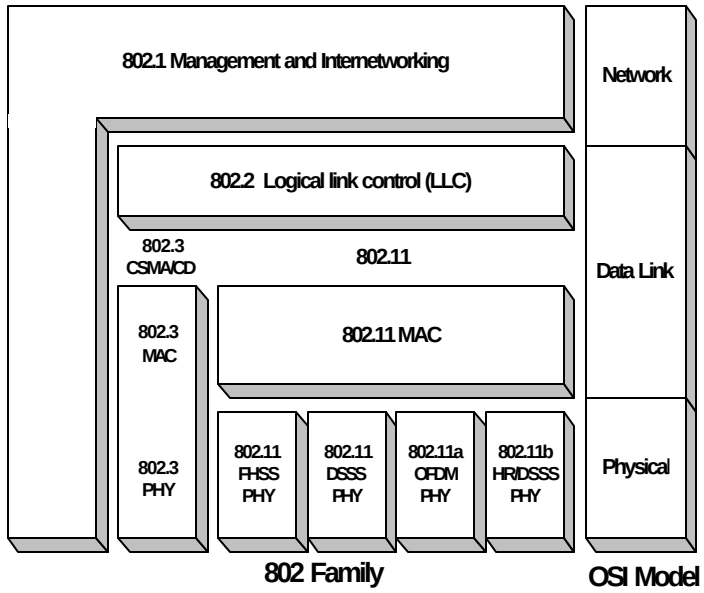
Information and Telecommunication Technology Center

Motivation

Wireless networks based on the IEEE 802.11 standard require lengthy layer two configuration parameters to be set

SSID (Network Name)
WEP Encryption Keys

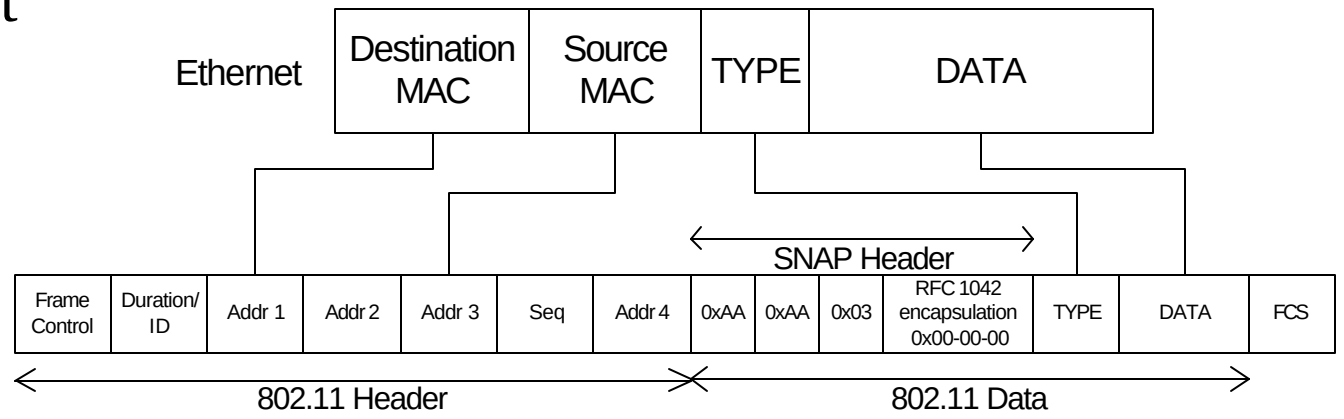
Embedded devices with limited input capabilities are unable to join the wireless network until properly configured



Traditional layer three configurations protocols like DHCP can be utilized once data layer communication is established

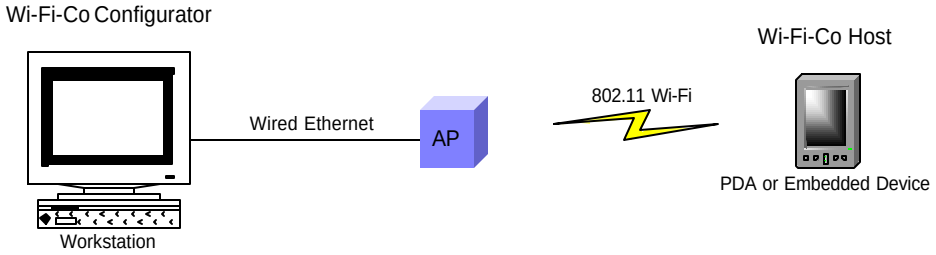
802.11 Encapsulation

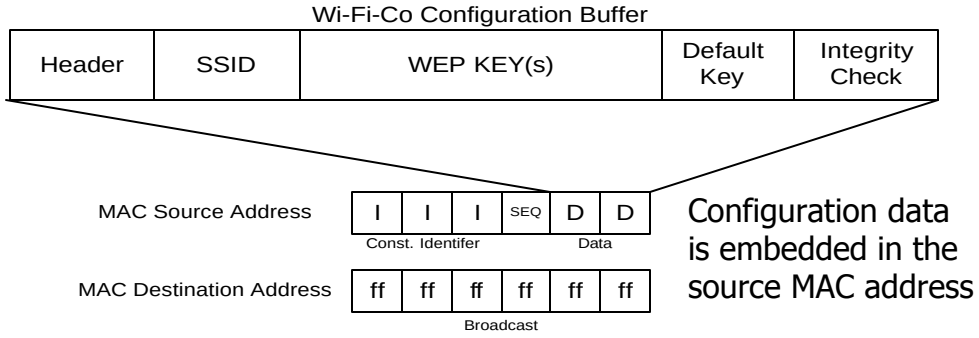
- 802.11 headers are unencrypted
- Access Points copy MAC addresses during the bridging process
- Data portion encrypted
  - No use to a station without keys
- Source address - 6 octets of data
- Broadcast



Wi-Fi-Co Protocol

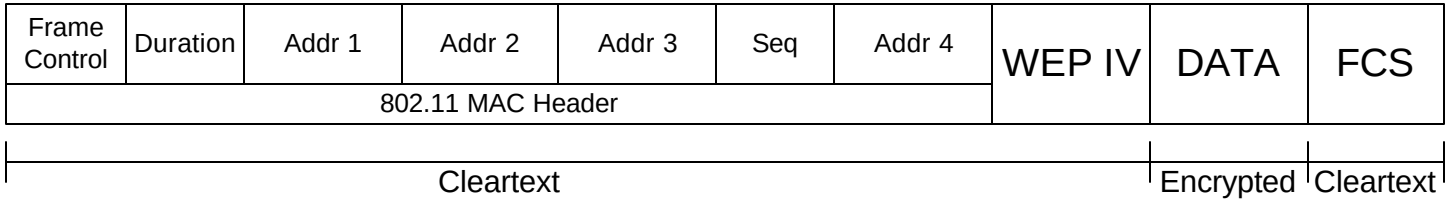
The Configurator host sends wireless network parameters to an embedded device via broadcast packets





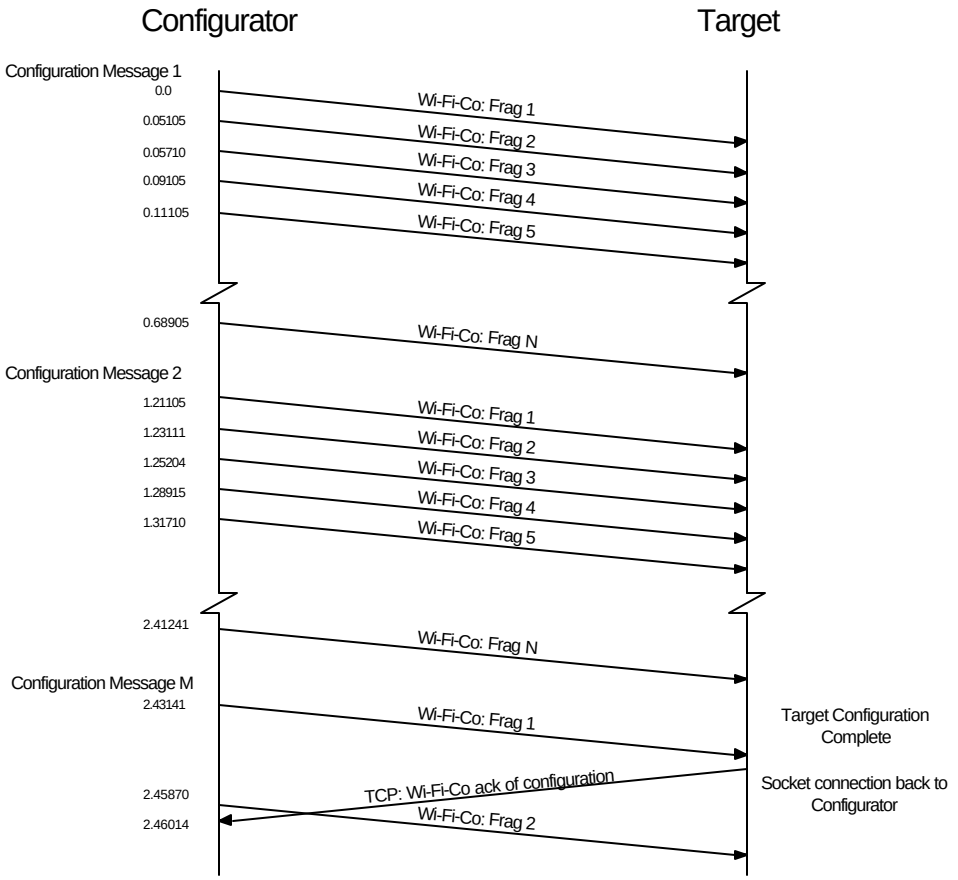
Configuration data is embedded in the source MAC address

A Wi-Fi station is able to capture the configuration frames and assemble the data from the cleartext 802.11 headers



Wi-Fi-Co Timing Diagram

- *Configurator* constantly broadcasts configuration data in fragmented packets
- The *target* assembles configuration data and decodes link level parameters
- Must “hop” Wi-Fi channels to guarantee that configuration data will be received



University of Kansas

Information and Telecommunication Technology Center

Protecting WEP Keys

- Broadcast packets easily intercepted
  - On wired Ethernet network portion
  - On wireless network portion

- Configuration data Encrypted
  - Shared key symmetric cipher
  - Embedded devices ship with unique, pre-programmed key
    - Certificate with product code
    - Additional input required on the *Configuration* host where it is much easier than input to embedded device

Wi-Fi Toaster 9000

Congratulations, you've have purchased the most advanced toaster on the planet! In moments you'll be tagged on to best tasting toast you've ever pinged. Be sure to check out our other fine products such as the ***Wi-Fi Can Opener 3000.***

Please Keep this certificate in a safe place

Serial Number: 0129831321332

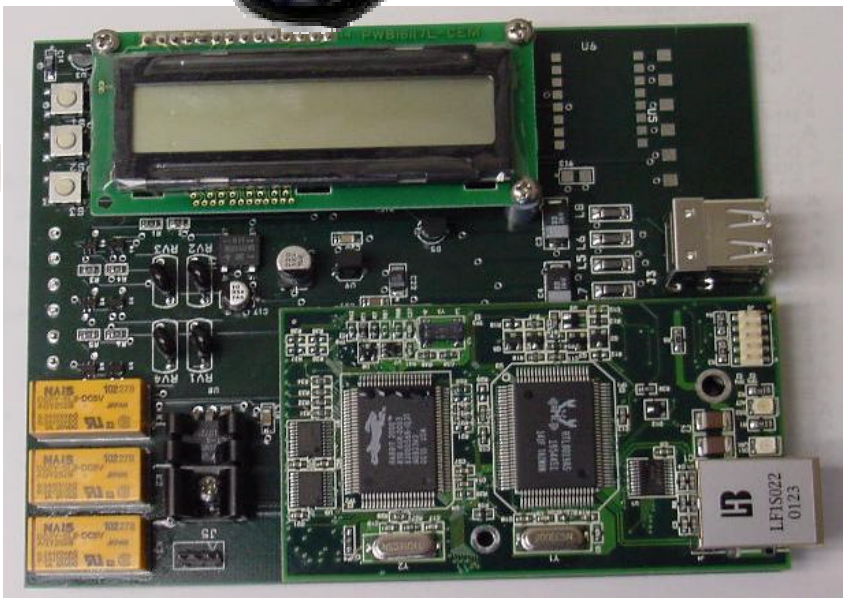
Product Code: 90FA-C387-8712-7AC9

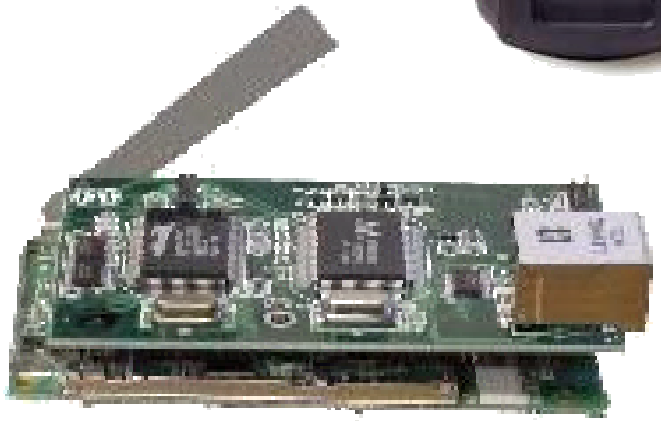
Limited Warranty

IN NO EVENT SHALL THE DIRECT VENDOR'S LIABILITY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT OR ITS DOCUMENTATION EXCEED THE PRICE PAID FOR THE PRODUCT.

The manufacturer is **not** responsible of loss of toast and/or bagels due to network stability problems due to, but not limited to, fiber cut, worms, DDoS attacks, hackers, viruses, or user stupidity.

Applications





University of Kansas

Information and Telecommunication Technology Center