

TRAPEZE NETWORKS
A BELDEN BRAND

Security & Management Improvements for Wireless LANs

Matthew Gast
Office of the CTO
March 31, 2009

TRAPEZE NETWORKS
A BELDEN BRAND

About Me

- Principal Engineer at Trapeze Networks
 - Product architecture & design
 - Long range planning and evolution of wireless LAN technology
- Chair of 802.11 revision task group (TGmb)
- Chair of Wi-Fi Alliance Wireless Network Management and Security Technical task groups
- Author of 802.11 Wireless Networks: The Definitive Guide (O'Reilly, 2005)
- Founder and board member at the OpenSEA Alliance

TRAPEZE NETWORKS
A BELDEN BRAND

Agenda

- Increasing the security of wireless LANs with 802.11w
- Updating the 802.11 protocol for manageability and new services

TRAPEZE NETWORKS
A BELDEN BRAND

802.11w introduction

- Attacks based on lack of protection of management frames
 - Disconnection attacks (e.g. airjack, void11)
 - Password/PSK recovery attacks (e.g. aircrack) often force disconnections to gather data
- Action frames are becoming more important: used by 11k/r/s
 - New AP connections, roaming, & mesh formation
- 802.11w provides protection for these frames, and therefore, against many common attacks

TRAPEZE NETWORKS
A BELDEN BRAND

Protection for management frames

- Only protected after 4-Way Handshake (class 3)
- Protection depends on type of frame

Provides:
Confidentiality, Source Auth., Integrity, Replay Protection

Provides:
Integrity, Replay Protection

TRAPEZE NETWORKS
A BELDEN BRAND

How Protection Happens

- Protecting unicast management frames
 - Uses CCMP (sometimes referred to as "WPA2") to provide encryption
 - Both privacy & integrity – frame contents cannot be sniffed or tampered with
 - Very small specification changes: a few pages out of 50 in the CCMP specification
- Broadcast management frames
 - New protocol: Broadcast/Multicast Integrity Protocol (BIP)
 - Provides integrity only – frame contents are "in the clear," but are authenticated

TRAPEZE NETWORKS
A BELDEN BRAND

Status of 802.11w

- Standard progressing through IEEE sponsor ballot
- Wi-Fi Alliance developing a certification program
 - Launch date to be determined
- Open source implemented by wpa_supplicant, planned for Open1x

TRAPEZE NETWORKS
A BELDEN BRAND

New Management Standards

- Largely based on work in IEEE 802.11v
 - Purpose: enable better station management, such as monitoring, configuring, updating, and troubleshooting
- Timeline
 - Study group formed in January 2004, task group formed in November 2004
 - Call for papers in September 2005, work begins on draft in January 2006
 - Initial ballot on draft 1.0 in July 2007
 - Further letter ballots through present time
 - Currently anticipating work complete in June 2010

TRAPEZE NETWORKS
A BELDEN BRAND

Broad functional categories in 802.11v

- Power saving
- Station management (troubleshooting, diagnostics, & reporting)
- Location
- Timing
- Coexistence

TRAPEZE NETWORKS
A BELDEN BRAND

Power Management Features

- WNM (wireless network management) Sleep Mode
 - Further extension to base 802.11 power saving allows for longer power-off times for 802.11 radios
 - Used in conjunction with new Traffic Filtering Service to enable AP to deliver only specified frame types
- Enables "wake on WLAN"
- Proxy ARP
 - AP responds to ARP requests to enable stations to power down for longer periods
- TIM Broadcast
 - Distributes traffic indication map (TIM) so that stations do not need to receive every Beacon frame (~100 ms interval)
- Flexible Broadcast/Multicast service (FBMS)
 - Sends broadcast/multicast frames at highest data rate for the group of receivers; reduces power-on time for radio interfaces
 - Higher data rates improve performance of multicast apps

TRAPEZE NETWORKS
A BELDEN BRAND

Station Management Features

- Event reporting
 - Stations can send information on events (e.g. syslog) for troubleshooting purposes
- Diagnostic reporting
 - APs can gather station statistics to improve application performance
- BSS transition management
 - APs direct stations to less loaded APs (load balancing)
 - Reports on transitions for management purposes
- Interference reporting
 - Allows network managers to mitigate effects of localized interference
- Authentication troubleshooting
- Enables large-scale network management

TRAPEZE NETWORKS
A BELDEN BRAND

New Services

- Multiple BSSID operation
 - Reduces Beacon and Probe traffic to save power and increase airtime utilization efficiency
- Timing synchronization
 - Enables more accurate location capabilities
 - Supports audio synchronization (e.g. Wi-Fi speakers)
- Location format reporting
 - Enables Wi-Fi RFID tags and emergency location for Wi-Fi phones