# CAPWAP Evaluation Team Summary Report

IETF63

1 August 2005

# Evaluation Team Details

- Team Members
  - – David Nelson <dnelson@enterasys.com>
  - – Oleg Volinsky <ovolinsky@colubris.com>
  - – Behcet Sarikaya <sarikaya@unbc.ca>
  - – Darren Loher – Editor <dloher@rovingplanet.com>
- Team Meetings
  - – Team formed June 8th
  - – Weekly meetings June 15 – July 29
  - – Observed by WG Chairs

# Evaluation Process

- Used RFC 3217 as guideline
  - AAA WG Protocol Evaluation
  - Complete Compliance, Partial, Fail to comply
  - 2 primary evaluators per protocol
    - One “Pro” and one “Con” viewpoint
  - Two secondary evaluators, Neutral viewpoints
- Each protocol received a two hour conference call review
- Validated self-evaluation assertions against objectives and the draft
- Used copies of drafts available as of 25th June 2005

# Notes on Objectives

- Resource Control
  - Interpreted to require configuration of QoS mapping
- Configuration Consistency
  - Recommend a token, key or serial number for configuration to verify configuration on large scale
- Security Considerations
  - Rated on basis of meeting features in security objective
  - Any protocol will require review though the IESG security process
  - Old issue of PMK sharing when encryption terminated at WTP still exists
- NAT Traversal
  - Only looking for obvious constraints of IP carried in payload
- Firmware Trigger
  - Full compliance granted only if trigger can be executed at any time in state machine (without multiple resets/reboots of WTP)

# Summary Results

| CAPWAP Evaluation | SLAPP | WiCoP | CTP | LWAPP |
|---|---|---|---|---|
| **Mandatory** | | | | |
| 5.1.1 Logical Groups | C | C | C | C |
| 5.1.2 Traffic Separation | C | P | P | C |
| 5.1.3 STA Transparency | C | C | C | C |
| 5.1.4 Config Consistency | C | C | C | C |
| 5.1.5 Firmware Trigger | P | C | P | P |
| 5.1.6 Monitor System | C | C | P | C |
| 5.1.7 Resource Control | P | F | P | C |
| 5.1.8 Protocol Security | C | F | F | C |
| 5.1.9 System Security | C | F | F | C |
| 5.1.10 802.11i Consideration | C | P | C | C |
| 5.1.11 Interoperability | C | C | C | C |
| 5.1.12 Protocol Specifications | P | P | P | C |
| 5.1.13 Vendor Independence | C | C | C | C |
| 5.1.14 Vendor Flexibility | C | C | C | C |
| 5.1.15 NAT Traversal | C | C | C | C |
| **Desirable** | | | | |
| 5.2.1 Multiple Authentication | C | C | P | C |
| 5.2.2 Future Wireless | C | C | C | C |
| 5.2.3 New IEEE Requirements | C | C | C | C |
| 5.2.4 Interconnection (IPv6) | C | C | C | C |
| 5.2.5 Access Control | C | C | C | C |

C = Complete Compliance
P = Partial Compliance
F = Failed Compliance

# SLAPP Evaluation Summary

- Highlights
  - Version 01 of draft defines control protocol, encapsulation and TLV’s
  - Use of GRE for user data encapsulation and DTLS for control channel encapsulation
  - Ability to forward raw 802.11 frames from WTP To AC on secure control channel
- Compliance notes
  - Missing configuration of QoS mappings
  - Firmware trigger should be usable at any time in state machine
- Recommendations
  - Should define a local MAC mode with local bridging of user data
  - The discovery mechanism could recommend that the WTP allow multiple FQDN's or IP addresses in each of it's discovery modes
- Additional information requested
  - Missing explicit definition for authentication of AC by a WTP
  - Some ambiguity regarding 802.11 information elements, indexing and defining multiple BSSID’s
  - Method to handle re-association requests in 802.11 control protocol?
  - IANA considerations for extending TLV’s

# WiCoP Highlights

- Highlights
  - Novel combination of capabilities exchange during discovery stage
  - Proposes standard authentication and security methods
  - Explicit group definition and clear association between groups and tunnels
- Compliance notes
  - Missing configuration of QoS mappings
  - Must describe details regarding IPSec authentication and key management of the control channel
  - Missing necessary details for WTP-AC authentication
- Recommendations
  - Modify protocol specification to adhere to standard RFC protocol format
- Additional information requested
  - Discuss protocol security issues, specifically DoS attacks on discovery phase
  - Explicitly discuss how protocol can be extended to support future wireless technologies

# CTP Evaluation Summary

- Highlights
  - Encapsulates SNMP in CTP control channel
  - Defines new authentication mechanism
- Compliance notes
  - Only one authentication and encryption method without ability to extend methods
  - Precludes ability to perform asymmetric authentication
  - Must define standard set of CAPWAP specific SNMP OID’s to address all objectives
    - Method to configure tunneling of user data
    - QoS mapping
    - System resources
  - Firmware trigger should be usable at any time in state machine
- Recommendations
  - Use of an established security method for control channel
- Additional information requested
  - Define usage and configuration of QoS policy field in control channel

# LWAPP Highlights

- Highlights
  - Most detailed proposal
  - New security and authentication methods for control channel
  - Forwards raw 802.11 management frames on control channel
- Compliance Notes
  - LWAPP does support multiple authentication methods for STA via EAP, but does not support multiple types for AC – WTP authentication
  - Firmware trigger should be usable at any time in state machine
- Recommendations
  - Standards based security and authentication methods would be preferred
  - 8 bit length Message type ID may be a limitation
- Additional Information
  - Additional security review is required
  - Some TBD areas still exist
  - IANA considerations and considerations for future definition and registration of codes points needs detail