CAPWAP Comparative Analysis

Richard Gwee
Republic Polytechnic
(draft-gwee-capwap-comparative-analysis-00)

Agenda

- Aims & Objectives
- CAPWAP Objectives
- Summary of Recommendations
- Conclusion

Aims & Objectives

- Objectives
  - To provide a comparative analysis of the proposed CAPWAP protocols.
  - To recommend the best mechanisms among the proposals for the final CAPWAP protocol.
  - To recommend that the final CAPWAP protocol should comprise the best strengths of the current proposals.

Introduction

- Currently, four candidate protocols have been proposed.
  - CAPWAP Tunneling Protocol (CTP)
  - Light Weight Access Point Protocol (LWAPP)
  - Secure Light Access Point Protocol (SLAPP)
  - Wireless LAN Control Protocol (WiCoP)
- Comparative Analysis to focus on the CAPWAP Objectives.

CAPWAP Security

- Highlights
  - WiCoP mechanism does not address this objective directly.
  - CTP and LWAPP mechanisms uses digital certificates/pre-shared keys.
  - SLAPP mechanism uses existing DTLS scheme.
- Mechanism Recommendation
  - SLAPP mechanism (DTLS) is more appropriate for a standard.
  - It is a well-understood security mechanism and requires less security review.

Logical Group

- Highlights
  - Logical groups must be supported across both wired and wireless aspects of the network regardless of architecture.
  - WiCoP mechanism explicitly includes logical group information in WTP configuration phase.
  - WiCoP mechanism provides mapping for logical grouping, covering both wired and wireless aspects.
- Mechanism Recommendation
  - WiCoP mechanism → structured approach.

Resource Control

- Highlights
  - LWAPP mechanism allows an AC to have more control in determining the QoS policy of a MT directly.
  - CTP and SLAPP mechanism does not provide such similar control.
  - WiCoP mechanism does not address this objective directly.
- Mechanism Recommendation
  - LWAPP mechanism includes wireless and VLAN QoS metrics for configuration.
  - It meets this objective in a most effective manner.

IEEE 802.11i Considerations

- Highlights
  - Scenario where authentication and encryption point are located differently must be considered.
  - Only WiCoP specifications clearly describes this scenario in relation to IEEE 802.11i handshake mechanism.
  - This is inline with CAPWAP objective.
- Mechanism Recommendation
  - WiCoP Key Configuration exchanges address this objective.

Configuration Consistency

- Highlights
  - Proper maintenance of state information in all nodes required for effective operation.
  - Type of state information should be explicitly specified to reduce implementation issues.
- Mechanism Recommendation
  - LWAPP specifies IEEE 802.11 binding for statistic information.
  - CTP recommends use of IEEE 802.11 MIB for configuration and statistic.
  - State information is explicitly specified in these two mechanisms.

Interoperability

- Highlights
  - Both Split MAC and Local MAC architecture must be supported.
  - Protocol operations must be consistent for both types of architectures.
  - Consistent operations make for simpler protocol.
- Mechanism Recommendation
  - Final CAPWAP protocol must have similar treatment for both local MAC and split MAC WTPs.
  - WiCoP mechanism (‘M’ Field, Configuration Data) allows for consistent management of both local MAC and split MAC WTPs.

Summary of Recommendation

CAPWAP Objectives	Recommended Mechanisms
Logical Groups	WiCoP
Support Traffic Separation	LWAPP/SLAPP
Configuration Consistency	LWAPP/CTP
Firmware Trigger	WiCoP
Resource Control	LWAPP
Monitor System	WiCoP
Security	SLAPP
802.11i Considerations	WiCoP
Interoperability	WiCoP
Multiple Authentication	SLAPP/LWAPP
Future Wireless	SLAPP
New IEEE Requirements	SLAPP

Conclusion

- List of recommended mechanisms presented.
- Final CAPWAP protocol should contain the best strengths of the current proposals.