Network Working Group
Internet-Draft
Expires: October 2005

S. Govindan
S. Iino
H. Cheng
M. Sugiura
Panasonic
May 2005

Evaluation of Wireless LAN Control Protocol (WiCoP)
draft-govindan-capwap-wicop-evaluation-00.txt

Status of this Memo

Copyright Notice

Abstract

The Wireless LAN Control Protocol (WiCoP) enables control of WLANs made of different types of wireless termination points. It addresses an immediate concern for WLAN deployments. This draft presents an evaluation of WiCoP with respect to the CAPWAP Objectives. It also highlights WiCoP's advantges over other CAPWAP candidate protocols.

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Terminology

This draft follows the terminologies of [I-D.ietf-capwap-arch] and [I-D.ietf-capwap-objectives].

3. Introduction

The Wireless LAN Control Protocol (WiCoP) [I-D.iino-capwap-wicop] addresses the most important issue for current WLANs - the ability to control and manage systems made up of different types of WTPs. WiCoP provides this ability and enables administrators to manage WLANs with a mix of local-MAC and split-MAC WTPs.

This document evaluates WiCoP with respect to the CAPWAP Objectives [I-D.ietf-capwap-objectives] and indicates how the protocol realizes those requirements.

4. WiCoP Evaluation

The CAPWAP Objectives are being devised by the CAPWAP WG as the core set of requirements needed to control and provision large-scale WLANs. The following sections describe how WiCoP realizes all those requirements.

4.1 Mandatory and Accepted Objectives

The Mandatory and Accepted Objectives represent those requirements that have been deemed of highest importance. WiCoP realizes all these requirements and in doing so, delivers an effective solution for managing large-scale WLANs.

4.1.1 Logical Groups

The CAPWAP protocol MUST be capable of controlling and managing physical WTPs in terms of logical groups including BSSID-based groups.

4.1.1.1 Protocol Evaluation

WiCoP establishes logical groups using BSSIDs for the wireless medium segment and VLANs for the switching segment [WiCoP Section 6.4.1]. The protocol maps the two logical groups using the BSSID-TunnelID item of the Conf WTP Data message element [WiCoP Section 5.2.2].

4.1.1.2 Comparison

The authors believe that CTP [I-D.singh-capwap-ctp] provides a feature that would enhance the realization of the Logical Groups objective in terms of QoS policy. For example, the CTP 'Policy' field may be integrated with WiCoP's logical BSSID-TunnelID configuration parameter to specify QoS attributes for the logical groups.

4.1.1.3 Compliance

WiCoP completely satisfies this objective.

4.1.2 Support for Traffic Separation

The CAPWAP Protocol MUST define transport control messages such that the transport of control messages is separate from the transport of data messages.

4.1.2.1 Protocol Evaluation

WiCoP uses separate tunnels for data and control traffic. Additionally, the protocol uses distinct VLAN tunnels for traffic from different logical groups [WiCoP Section 6.4.1]. This ensures that traffic flows are separated between WTPs and WLAN controller.

Furthermore, WiCoP uses distinct messages for control and data traffic. The two are never combined.

4.1.2.2 Compliance

WiCoP completely satisfies this objective.

4.1.3 Wireless Terminal Transparency

Wireless terminals MUST NOT be required to recognize or be aware of the CAPWAP protocol.

4.1.3.1 Protocol Evaluation

WiCoP does not mandate any changes to wireless terminals. The specifications only address the interface between WTPs and their WLAN controller.

4.1.3.2 Compliance

WiCoP completely satisfies this objective.

4.1.4 Configuration Consistency

The CAPWAP protocol MUST include support for regular exchanges of state information between WTPs and WLAN controller. Examples of state information include WTP processing load and memory utilization.

4.1.4.1 Protocol Evaluation

WiCoP uses the Feedback Interval timer [WiCoP Section 5.4.2] to maintain regular exchanges of Feedback messages [WiCoP Section 5.2.3], which contain information on the configuration state of WTPs and WLAN controller. This helps the WLAN controller in effecting consistent configuration changes to all WTPs.

4.1.4.2 Compliance

WiCoP completely satisfies this objective.

4.1.5 Firmware Trigger

The CAPWAP protocol MUST support a trigger for delivery of firmware updates.

4.1.5.1 Protocol Evaluation

WiCoP activates Firmware Download message to initiate firmware check and download [WiCoP Section 5.2.3].

4.1.5.2 Compliance

WiCoP completely satisfies this objective.

4.1.6 Monitoring and Exchange of System-wide Resource State

The CAPWAP protocol MUST allow for the exchange of statistics, congestion and other WLAN state information.

4.1.6.1 Protocol Evaluation

WiCoP Feedback messages [WiCoP Section 5.2.3] together with QoS Value, Statistics, Interface Error and QoS Capability message elements to monitor configuration state of WTPs and WLAN Controller [WiCoP Section 5.2.2].

4.1.6.2 Compliance

WiCoP completely satisfies this objective.

4.1.7 Resource Control Objective

The CAPWAP protocol MUST map the IEEE 802.11e QoS priorities to equivalent QoS priorities across the switching and wireless medium segments.

4.1.7.1 Protocol Evaluation

The current specifications do not directly address this objective, however WiCoP can map IEEE 802.11e requirements to VLAN priority tags using the BSSID-TunnelID item of the Conf WTP Data message element [WiCoP Section 5.2.2].

4.1.7.2 Compliance

WiCoP partially satisfies this objective.

4.1.8 CAPWAP Protocol Security

The CAPWAP protocol MUST support mutual authentication of WTPs and the centralized controller. It must also ensure that information exchanges between them are secured.

4.1.8.1 Protocol Evaluation

WiCoP makes use of IPSec based authentication and encryption mechanisms [WiCoP Section 6.3] to secure all exchanges.

4.1.8.2 Comparison

The authors feel that the use of DTLS such as in SLAPP [I-D.narasimhan-ietf-slapp]is effective in addressing this objective. SLAPP describes an existing mechanism that can be reused in the CAPWAP context. It would be preferable for CAPWAP to use DTLS as opposed to adopting a new mechanism for key exchange and protocol security.

4.1.8.3 Compliance

WiCoP partially satisfies this objective.

4.1.9 System-wide Security

The design of the CAPWAP protocol MUST NOT allow for any compromises to the WLAN system by external entities.

4.1.9.1 Protocol Evaluation

WiCoP does not yet address the issue of potential problems due to PMK sharing.

4.1.9.2 Compliance

WiCoP does not satisfy this objective.

4.1.10 IEEE 802.11i Considerations

The CAPWAP protocol MUST determine the exact structure of the centralized WLAN architecture in which authentication needs to be supported, i.e. the location of major authentication components. This may be achieved during WTP initialization where major capabilities are distinguished.

The protocol must allow for the exchange of key information when authenticator and encryption roles are located in distinct entities.

4.1.10.1 Protocol Evaluation

This objective brings out the important architecture condition of the authenticator being located distinctly from the point of encryption. WiCoP addresses this condition with the use of the Key Config message [WiCoP Section 5.2.3]. Key Config is used to explicitly transport the 3rd message of the four-way handshake from the authenticator (WLAN controller) to the point of encryption (WTP) [WiCoP Section 6.5.6]. As a result of this feature, WiCoP allows the WTP to calculate the KeyMIC with its KeyRSC.

4.1.10.2 Comparison

The authors believe that, based on prevailing specifications of the other candidate protocols, only WiCoP explicitly addresses this objective.

4.1.10.3 Compliance

WiCoP completely satisfies this objective.

4.1.11 Interoperability Objective

The CAPWAP protocol MUST include sufficient capabilities negotiations to distinguish between major types of WTPs.

4.1.11.1 Protocol Evaluation

WiCoP realizes this objective of managing co-existence of WTPs of different MAC designs. The protocol uses the 'M' field of the WiCoP header to distinguish between local-MAC and split-MAC WTPs [WiCoP Section 5.1].

So for each WiCoP packet from a WTP, the WLAN controller simply parses the packet header and then processes it accordingly, i.e. for packets from local-MAC WTP certain MAC processing are bypassed.

If however, the 'M' field is not used, then the WLAN controller must first parse incoming packet header and then use the parsed information to perform a lookup operation to determine the type of WTP and then determine how to process the packet. This is an extended procedure which will adversely affect WLAN operational performance.

So using 'M' field, a WLAN controller can handle packets from different types of WTPs faster and with fewer processing steps.

4.1.11.2 Comparison

The authors believe that, based on prevalent specifications of alternative candidate protocols, WiCoP realizes the Interoperability Objective in the most efficient manner.

4.1.11.3 Compliance

WiCoP completely satisfies this objective.

4.1.12 Protocol Specifications

Any WTP or AC vendor or any person MUST be able to implement the CAPWAP protocol from the specification itself and by that it is required that all such implementations do interoperate.

4.1.12.1 Protocol Evaluation

WiCoP is a complete specification and does not require any additional proprietary information to implement.

4.1.12.2 Compliance

WiCoP completely satisfies this objective.

4.1.13 Vendor Independence

A WTP vendor can make modifications to hardware without any AC vendor involvement.

4.1.13.1 Protocol Evaluation

WiCoP is a complete specification and does not require any additional proprietary information to implement.

4.1.13.2 Compliance

WiCoP completely satisfies this objective.

4.1.14 Vendor Flexibility

WTP vendors must not be bound to a specific MAC.

4.1.14.1 Protocol Evaluation

WiCoP is a complete specification and does not require any additional proprietary information to implement.

4.1.14.2 Compliance

WiCoP completely satisfies this objective.

4.2 Desirable Objectives

The Desirable Objectives are those that are not crucial to a CAPWAP protocol but would be beneficial. WiCoP realizes all these requirements.

4.2.1 Multiple Authentication Mechanisms

The CAPWAP protocol MUST support different authentication mechanisms in addition to IEEE 802.11i.

4.2.1.1 Protocol Evaluation

WiCoP does not prevent the operation of any authentication mechanism. It is generic to support all types of authentication mechanisms.

4.2.1.2 Compliance

WiCoP completely satisfy this objective.

4.2.2 Support for Future Wireless Technologies

CAPWAP protocol messages MUST be designed to be extensible for specific layer 2 wireless technologies. It should not be limited to the transport of elements relating to IEEE 802.11.

4.2.2.1 Protocol Evaluation

WiCoP is generic and extensible to support future developments in wireless technologies.

4.2.2.2 Compliance

WiCoP completely satisfies this objective.

4.2.3 Support for New IEEE Requirements

The CAPWAP protocol MUST be openly designed to support new IEEE 802.11 extensions.

4.2.3.1 Protocol Evaluation

WiCoP is generic and extensible to support future developments in wireless technologies and standards.

4.2.3.2 Compliance

WiCoP completely satisfy this objective.

4.2.4 Interconnection Objective

The CAPWAP protocol MUST NOT be constrained to specific underlying transport mechanisms.

4.2.4.1 Protocol Evaluation

WiCoP does not rely of the specifics of underlying transport technologies. Although WiCoP uses UDP, it does not require any UDP-specific information for its operation.

4.2.4.2 Compliance

WiCoP completely satisfies this objective.

4.2.5 Access Control

The CAPWAP protocol MUST be capable of exchanging information required for access control of WTPs and wireless terminals.

4.2.5.1 Protocol Evaluation

WiCoP uses the Terminal Data message element [WiCoP Section 5.2.2] to exchange association and authentication information on wireless terminals. This is used by the WLAN controller to supervise access control.

4.2.5.2 Compliance

WiCoP completely satisfies this objective.

4.3 Non-objectives

These objectives have been recognized by the CAPWAP WG as having relatively lower priorities for the current phase of CAPWAP.

4.3.1 Support for Non-CAPWAP WTPs

The CAPWAP protocol SHOULD be capable of recognizing legacy WTPs and existing network management systems.

4.3.1.1 Protocol Evaluation

WiCoP can configure local-MAC WTPs, which in some cases require

limited management. This case is similar to those of legacy WTPs.

4.3.1.2 Compliance

WiCoP completely satisfies this objective.

4.3.2 Technical Specifications

WTP vendors SHOULD NOT have to share technical specifications for hardware and software to AC vendors in order for interoperability to be achieved.

4.3.2.1 Protocol Evaluation

WiCoP is a complete specification and does not require any additional proprietary information to implement.

4.3.2.2 Compliance

WiCoP completely satisfies this objective.

4.4 Operator Requirements

The following objective addresses the concerns of WLAN service providers.

4.4.1 AP Fast Handoff

The CAPWAP protocol operations MUST NOT impede or obstruct the efficacy of AP fast handoff procedures.

4.4.1.1 Protocol Evaluation

Since WiCoP addresses the centralized WLAN architecture in which information can be managed across WTPs. Consequently, the protocol would only serve to enhance AP fast handoff procedures instead of impeding it.

4.4.1.2 Compliance

WiCoP completely satisfies this objective.

5. Summary

The evaluation presented in this document indicates that WiCoP satisfies most of the crucial objectives. The authors also believe that WiCoP addresses some objectives in highly efficient and effective ways.

Objective	Compliance
Logical Groups	C
Support for Traffic Separation	C
Wireless Terminal Transparency	C
Configuration Consistency	C
Firmware Trigger	C
Monitoring and Exchange of System-wide Resource State	C
Resource Control Objective	P
CAPWAP Protocol Security	P
System-wide Security	N
IEEE 802.11i Considerations	C
Interoperability Objective	C
Protocol Specifications	C
Vendor Independence	C
Vendor Flexibility	C
Multiple Authentication Mechanisms	C
Support for Future Wireless Technologies	C
Support for New IEEE Requirements	C
Interconnection Objective	C
Access Control	C
Support for Non-CAPWAP WTPs	C
Technical Specifications	C
AP Fast Handoff	C

6. Security Considerations

The WiCoP evaluation does not constitue any new security considerations other than those addressed in the WiCoP specifications.

7. References

[I-D.ietf-capwap-arch]
Yang, L., Zerfos, P., and E. Sadot, "Architecture Taxonomy for Control and Provisioning of Wireless Access Points(CAPWAP)", draft-ietf-capwap-arch-06 (work in progress), November 2004.

[I-D.ietf-capwap-objectives]
Govindan, S., "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)", draft-ietf-capwap-objectives-02 (work in progress), April 2005.

[I-D.ietf-capwap-problem-statement]
Calhoun, P., "CAPWAP Problem Statement", draft-ietf-capwap-problem-statement-02 (work in progress), September 2004.

[I-D.iino-capwap-wicop]
Iino, S., "Wireless LAN Control Protocol (WiCoP)", draft-iino-capwap-wicop-00 (work in progress), March 2005.

[I-D.narasimhan-ietf-slapp]
Narasimhan, P., "SLAPP : Secure Light Access Point Protocol", draft-narasimhan-ietf-slapp-01 (work in progress), June 2005.

[I-D.singh-capwap-ctp]
Singh, I., "CAPWAP Tunneling Protocol (CTP)", draft-singh-capwap-ctp-01 (work in progress), April 2005.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

Saravanan Govindan
Panasonic Singapore Laboratories
Block 1022, Tai Seng Industrial Estate
#06-3530, Tai Seng Avenue
Singapore 534 415
Singapore

Phone: +65 6550 5441
Email: saravanan.govindan@sg.panasonic.com

Satoshi Iino
Panasonic Mobile Communications
600, Saedo-cho
Tsuzuki-ku
Yokohama 224 8539
Japan

Phone: +81 45 938 3789
Email: iino.satoshi@jp.panasonic.com

Hong Cheng
Panasonic Singapore Laboratories
Block 1022, Tai Seng Industrial Estate
#06-3530, Tai Seng Avenue
Singapore 534 415
Singapore

Phone: +65 6550 5447
Email: hong.cheng@sg.panasonic.com

Mikihito Sugiura
Panasonic Mobile Communications
600, Saedo-cho
Tsuzuki-ku
Yokohama 224 8539
Japan

Phone: +81 45 938 3789
Email: sugiura.mikihito@jp.panasonic.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.