Network Working Group
Request for Comments: 4565
Category: Informational

D. Loher
Envysion, Inc.
D. Nelson
Enterasys Networks, Inc.
O. Volinsky
Colubris Networks, Inc.
B. Sarikaya
Huawei USA

July 2006

Evaluation of Candidate Control and Provisioning of Wireless Access Points (CAPWAP) Protocols

Status of This Memo

Copyright Notice

Abstract

This document is a record of the process and findings of the Control and Provisioning of Wireless Access Points Working Group (CAPWAP WG) evaluation team. The evaluation team reviewed the 4 candidate protocols as they were submitted to the working group on June 26, 2005.

Table of Contents

1. Introduction

This document is a record of the process and findings of the Control and Provisioning of Wireless Access Points Working Group (CAPWAP WG) evaluation team. The evaluation team reviewed the 4 candidate protocols as they were submitted to the working group on June 26, 2005.

1.1. Conventions Used in This Document

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 RFC 2119 [RFC2119].

1.2. Terminology

This document uses terminology defined in RFC 4118 [ARCH], RFC 4564 [OBJ], and IEEE 802.11i [802.11i].

2. Process Description

The process to be described here has been adopted from a previous evaluation in IETF [RFC3127]. The CAPWAP objectives in RFC 4564 [OBJ] were used to set the scope and direction for the evaluators and was the primary source of requirements. However, the evaluation team also used their expert knowledge and professional experience to consider how well a candidate protocol met the working group objectives.

For each of the 4 candidate protocols, the evaluation document editor assigned 2 team members to write evaluation briefs. One member was assigned to write a "Pro" brief and could take a generous interpretation of the proposal; this evaluator could grant benefit of doubt. A second evaluator was assigned to write a "Con" brief and was required to use strict criteria when performing the evaluation.

2.1. Ratings

The "Pro" and "Con" members independently evaluated how well the candidate protocol met each objective. Each objective was scored as an ’F’ for failure, ’P’ for partial, or ’C’ for completely meeting the objective.

F - Failure to Comply

The evaluation team believes the proposal does not meet the objective. This could be due to the proposal completely missing any functionality towards the objective. A proposal could also receive an ’F’ for improperly implementing the objective.

P - Partial Compliance

The proposal has some functionality that addresses the objective, but it is incomplete or ambiguous.

C - Compliant

The proposal fully specifies functionality meeting the objective. The specification must be detailed enough that interoperable implementations are likely from reading the proposal alone. If the method is ambiguous or particularly complex, an explanation, use cases, or even diagrams may need to be supplied in order to receive a compliant rating.

The 4-person evaluation team held a teleconference for each candidate to discuss the briefs. One of the working group chairs was also present at the meeting in an advisory capacity. Each evaluator presented a brief with supporting details. The team discussed the issues and delivered a team rating for each objective. These discussions are documented in the meeting minutes. The team ratings are used for the compliance evaluation.

The candidate protocols were scored only on the information written in their draft. This means that a particular protocol might actually meet the specifics of a requirement, but if the proposal did not state, describe, or reference how that requirement was met, it might be scored lower.

3. Member Statements

Darren Loher, Roving Planet

I am employed as the senior architect at Roving Planet, which writes network and security management software for wireless networks. I have over 11 years of commercial experience designing and operating networks. I have implemented and operated networks and network management systems for a university, large enterprises, and a major Internet service provider for over 4 years. I also have software development experience and have written web-based network and systems management tools including a system for managing a very large distributed DNS system. I have witnessed the IETF standards process for several years, my first event being IETF 28. I have rarely directly participated in any working group activities before this point. To my knowledge, my company has no direct relationship with any companies that have authored the CAPWAP protocol submissions.

David Nelson, Enterasys

I am currently cochair of the RADEXT WG, AAA Doctor in O&M Area, and employed in the core router engineering group of my company. I have previously served on a protocol evaluation team in the AAA WG, and am a coauthor of RFC 3127 [RFC3127]. I was an active contributor in the IEEE 802.11i task group, and previously employed in the WLAN

engineering group of my company. I have had no participation in any of the submitted protocols. My company does have an OEM relationship with at least one company whose employees have coauthored one of the submissions, but I have no direct involvement with our WLAN product at this time.

Oleg Volinsky, Colubris Networks

I am a member of the Enterprise group of Colubris Networks, a WLAN vendor. I have over 10 years of experience in design and development of network products from core routers to home networking equipment. Over years I have participated in various IETF groups. I have been a member of CAPWAP WG for over a year. In my current position I have been monitoring the developments of CAPWAP standards and potential integration of the resulting protocol into the company's products. I have not participated in any of the candidate protocol drafts. I have not worked for any of the companies whose staff authored any of the candidate protocols.

Behcet Sarikaya, University of Northern British Columbia

I am currently Professor of Computer Science at UNBC. I have so far 5 years of experience in IETF as a member of mobile networking-related working groups. I have made numerous I-D contributions and am a coauthor of one RFC. I have submitted an evaluation draft (with Andy Lee) that evaluated LWAPP, CTP, and WiCoP. Also I submitted another draft (on CAPWAPHP) that used LWAPP, CTP, WiCoP, and SLAPP as transport. I also have research interests on next-generation access point/controller architectures. I have no involvement in any of the candidate protocol drafts, have not contributed any of the drafts. I have not worked in any of the companies whose staff has produced any of the candidate protocols.

4. Protocol Proposals and Highlights

The following proposals were submitted as proposals to the CAPWAP working group.

4.1. LWAPP

The "Light Weight Access Point Protocol" [LWAPP] was the first CAPWAP protocol originally submitted to Seamoby Working Group. LWAPP proposes original solutions for authentication and user data encapsulation as well as management and configuration information elements. LWAPP originated as a "split MAC" protocol, but recent changes have added local MAC support as well. LWAPP has received a security review from Charles Clancy of the University of Maryland Information Systems Security Lab.

LWAPP is the most detailed CAPWAP proposal. It provides a thorough specification of the discovery, security, and system management methods. LWAPP focuses on the 802.11 WLAN-specific monitoring and configuration. A key feature of LWAPP is its use of raw 802.11 frames that are tunneled back to the Access Controller (AC) for processing. In both local- and split-MAC modes, raw 802.11 frames are forwarded to the AC for management and control. In addition, in split-MAC mode, user data is tunneled in raw 802.11 form to the AC. While in concept, LWAPP could be used for other wireless technologies, LWAPP defines very few primitives that are independent of the 802.11 layer.

4.2. SLAPP

"Secure Light Access Point Protocol" [SLAPP] distinguishes itself with the use of well-known, established technologies such as Generic Routing Encapsulation (GRE) for user data tunneling between the AC and Wireless Termination Point (WTP) and the proposed standard Datagram Transport Layer Security [DTLS] for the control channel transport.

4 modes of operation are supported, 2 local-MAC modes and 2 split-MAC modes. STA control may be performed by the AC using native 802.11 frames that are encapsulated in SLAPP control packets across all modes. (STA refers to a wireless station, typically a laptop.)

In SLAPP local-MAC modes, user data frames may be bridged or tunneled back using GRE to the AC as 802.3 frames. In the split-MAC modes, user data is always tunneled back to the AC as native 802.11 frames. Encryption of user data may be performed at either the AC or the WTP in split-MAC mode.

4.3. CTP

"CAPWAP Tunneling Protocol" [CTP] distinguishes itself with its use of Simple Network Management Protocol (SNMP) to define configuration and management data that it then encapsulates in an encrypted control channel. CTP was originally designed as a local-MAC protocol but the new version has split-MAC support as well. In addition, CTP is clearly designed from the beginning to be compatible with multiple wireless technologies.

CTP defines information elements for management and control between the AC and WTP. CTP control messages are specified for STA session state, configuration, and statistics.

In local-MAC mode, CTP does not forward any native wireless frames to the AC. CTP specifies control messages for STA session activity, mobility, and radio frequency (RF) resource management between the AC and WTP. CTP local-MAC mode specifies that the integration function from the wireless network to 802.3 Ethernet is performed at the WTP for all user data. User data may either be bridged at the WTP or encapsulated as 802.3 frames in CTP packets at the WTP and tunneled to the AC.

CTP's split-MAC mode is defined as an extension to local-MAC mode. In CTP's version of split-MAC operation, wireless management frames are forwarded in their raw format to the AC. User data frames may be bridged locally at the WTP, or they may be encapsulated in CTP packets and tunneled in their native wireless form to the AC.

CTP supplies STA control abstraction, methods for extending the forwarding of multiple types of native wireless management frames, and many options for user data tunneling. Configuration management is an extension of SNMP. This makes CTP one of the most flexible of the proposed CAPWAP protocols. However, it does define new security and data tunneling mechanisms instead of leveraging existing standards.

4.4. WiCoP

"Wireless LAN Control Protocol" [WICOP] introduces new discovery, configuration, and management of Wireless LAN (WLAN) systems. The protocol defines a distinct discovery mechanism that integrates WTP-AC capabilities negotiation.

WiCoP defines 802.11 Quality of Service (QoS) parameters. In addition, the protocol proposes to use standard security and authentication methods such as IPsec and Extensible Authentication Protocol (EAP). The protocol needs to go into detail with regards to explicit use of the above-mentioned methods. To ensure interoperable protocol implementations, it is critical to provide users with detailed unambiguous specification.

5. Security Considerations

Each of the candidate protocols has a Security Considerations section, as well as security properties. The CAPWAP objectives document [OBJ] contains security-related requirements. The evaluation team has considered if and how the candidate protocols implement the security features required by the CAPWAP objectives. However, this evaluation team is not a security team and has not

performed a thorough security evaluation or tests. Any protocol coming out of the CAPWAP working group must undergo an IETF security review in order to fully meet the objectives.

6. Mandatory Objective Compliance Evaluation

6.1. Logical Groups

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP provides a control message called "Add WLAN". This message is used by the AC to create a WLAN with a unique ID, i.e., its Service Set Identifier (SSID). The WTPs in this WLAN have their own Basic Service Set Identifiers (BSSIDs). LWAPP meets this objective.

SLAPP

SLAPP explicitly supports 0-255 BSSIDs.

CTP

CTP implements a NETWORK_ID attribute that allows a wireless-technology-independent way of creating logical groups. CTP meets this objective.

WiCoP

WiCoP provides control tunnels to manage logical groups. There is one control tunnel for each logical group. WiCoP meets this objective.

6.2. Traffic Separation

LWAPP:C, SLAPP:C, CTP:P, WiCoP:P

If a protocol distinguishes a data message from a control message, then it meets this objective.

LWAPP

LWAPP separates control messages from data messages using "C-bit". "C-bit" is defined in the LWAPP transport header. When C-bit is equal to zero, the message is a data message. When C-bit is equal to one, the message is a control message. So, LWAPP meets this objective.

SLAPP

The SLAPP protocol encapsulates control using DTLS and optionally, user data with GRE. Of particular note, SLAPP defines 4 "architecture modes" that define how user data is handled in relation to the AC. SLAPP is compliant with this objective.

CTP

CTP defines separate packet frame types for control and data. However, the evaluation team could not find a way to configure the tunneling of user data, so it opted to rate CTP as only partially compliant. It appears that CTP would rely on SNMP MIB Object Identifiers (OIDs) for this function, but none were defined in the specification. Defining the necessary OIDs would make CTP fully compliant.

WiCoP

WiCoP provides for separation between control and data channels. However, tunneling methods are not explicitly described. Because of this, WiCoP partially meets this objective.

6.3. STA Transparency

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

If a protocol does not indicate that STA needs to know about the protocol, then this objective is met.

The protocol must not define any message formats between STA and WTP/AC.

LWAPP

LWAPP does not require a STA to be aware of LWAPP. No messages or protocol primitives are defined that the STA must interact with beyond the 802.11 standard. LWAPP is fully compliant.

SLAPP

SLAPP places no requirements on STA network elements. No messages or protocol primitives are defined that the STA must interact with beyond the 802.11 standard.

CTP

CTP does not require a terminal to know CTP. So, CTP meets this objective.

WiCoP

WiCoP does not require a terminal to know WiCoP. So, WiCoP meets this objective.

6.4. Configuration Consistency

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

Given the objective of maintaining configurations for a large number of network elements involved in 802.11 wireless networks, the evaluation team would like to recommend that a token, key, or serial number for configuration be implemented for configuration verification.

LWAPP

It is possible to obtain and verify all configurable values through LWAPP. Notably, LWAPP takes an approach that only "non-default" settings (defaults are specified by LWAPP) are necessary for transmission when performing configuration consistency checks. This behavior is explicitly specified in LWAPP. LWAPP is compliant with this objective.

SLAPP

Numerous events and statistics are available to report configuration changes and WTP state. SLAPP does not have any built-in abilities to minimize or optimize configuration consistency verification, but it is compliant with the objective.

CTP

CTP’s use of SNMP makes configuration consistency checking straightforward. Where specified in a MIB, one could take advantage of default values.

WICOP

The WiCoP configuration starts with exchange of capability messages between the WTP and AC. Next, configuration control data is sent to the WTP.

WiCoP defines configuration values in groups of configuration data messages. In addition, the protocol supports configuration using MIB objects. To maintain data consistency, each configuration message from the AC is acknowledged by the WTP.

6.5. Firmware Trigger

LWAPP:P, SLAPP:P, CTP:P, WiCoP:C

The evaluation team considered the objective and determined that for full compliance, the protocol state machine must support the ability to initiate the process for checking and performing a firmware update independently of other functions.

Many protocols perform a firmware check and update procedure only on system startup time. This method received a partial compliance. The team believed that performing the firmware check only at startup time was unnecessarily limiting and that allowing it to occur at any time in the state machine did not increase complexity of the protocol. Allowing the firmware update process to be initiated during the running state allows more possibilities for minimizing downtime of the WTP during the firmware update process.

For example, the firmware check and download of the image over the network could potentially occur while the WTP was in a running state. After the file transfer was complete, the WTP could be rebooted just once and begin running the new firmware image. This could pose a meaningful reduction in downtime when the firmware image is large, the link for loading the file is very slow, or the WTP reboot time is long.

A protocol would only fail compliance if no method was specified for updating of firmware.

LWAPP

Firmware download is initiated by the WTP only at the Join phase (when a WTP is first associating with an AC) and not at any other time. The firmware check and update could be "triggered" indirectly by the AC by sending a reset message to the WTP. The resulting reboot would cause a firmware check and update to be performed. LWAPP is partially compliant because its firmware trigger can only be used in the startup phases of the state machine.

SLAPP

SLAP includes a firmware check and update procedure that is performed when a WTP is first connecting to an AC. The firmware check and update can only be "triggered" indirectly by the AC by sending a reset message to the WTP. SLAPP is partially compliant because its firmware trigger can only be used in the startup phases of the state machine.

CTP

The CTP state machine specifies that the firmware upgrade procedure must be performed immediately after the authentication exchange as defined in section 6.2 of [CTP]. However, section 5.2.5 of [CTP] states that the SW-Update-Req message MAY be sent by the AC. This indirectly implies that CTP could support an AC-triggered software update during the regular running state of the WTP. So it seems that CTP might be fully compliant, but the proposal should be clarified for full compliance.

WiCoP

In WiCoP, firmware update may be triggered any time in the active state, so WiCoP is fully compliant.

6.6. Monitor and Exchange of System-wide Resource State

LWAPP:C, SLAPP:C, CTP:P, WiCoP:C

The evaluation team focused on the protocols supplying 3 methods relevant to statistics from WTPs: The ability to transport statistics, a minimum set of standard data, and the ability to extend what data could be reported or collected.

LWAPP

Statistics are sent by the WTP using an "Event Request" message. LWAPP defines an 802.11 statistics message that covers 802.11 MAC layer properties. LWAPP is compliant.

SLAPP

WLAN statistics transport is supplied via the control channel and encoded in SLAPP-defined TLVs called information elements. 802.11 configuration and statistics information elements are supplied in [SLAPP] 6.1.3.1. These are extendable and include vendor-specific extensions.

CTP

CTP defines a control message called "CTP Stats-Notify". This control message contains statistics in the form of SNMP OIDs and is sent from the WTP to AC. This approach is novel because it leverages the use of standard SNMP.

Section 5.3.10 of [CTP] recommends the use of 802.11 MIBs where applicable. However, the proposal acknowledges that additional configuration and statistics information is required, but does not specify these MIB extensions. CTP needs to add these extensions to the proposal. Also, this minimum set of statistics and configuration OIDs must become requirements in order to fully meet the objective.

WiCoP

The feedback control message sent by the WTP contains many statistics. WiCoP specifies 15 statistics that the WTP needs to send to the AC. New versions of WiCoP can address any new statistics that the AC needs to monitor the WTP. WiCoP meets this objective.

6.7. Resource Control

LWAPP:C, SLAPP:P, CTP:P, WiCoP:P

The evaluation team interpreted the resource control objective to mean that the CAPWAP protocol must map 802.11e QoS markings to the wired network. This mapping must include any encapsulation or tunneling of user data defined by the CAPWAP protocol. Of particular note, the evaluation team agreed that the CAPWAP protocol should supply an explicit capability to configure this mapping. Since most of the protocols relied only on the 802.11e statically defined mapping, most received a partial compliance.

LWAPP

LWAPP defines its own custom TLV structure, which consists of an 8-bit type or class of information value and an additional 8-bit value that indexes to a specific variable.

LWAPP allows the mobile station-based QoS configuration in each Add Mobile Request sent by AC to WTP for each new mobile station that is attached. Packet prioritization is left to individual WTPs. 4 different QoS policies for each station to enforce can be configured. Update Mobile QoS message element can be used to change QoS policy at the WTP for a given mobile station. LWAPP should support 8 QoS policies as this matches 802.11e 802.1p and IP TOS, but for this objective, 4 classes is compliant.

Overall, LWAPP conforms to the resource control objective. It enables QoS configuration and mapping. The control can be applied on a logical group basis and also enables the wireless traffic to be flexibly mapped to the wired segment.

SLAPP

Although 802.11e specifies 802.1p and Differentiated Service Code Point (DSCP) mappings, there is no explicit support for 802.11e in SLAPP. SLAPP must be updated to add 802.11e as one of the standard capabilities that a WTP could support and specify a mechanism that would allow configuration of mapping the QoS classes.

CTP

CTP requires that the WTP and AC copy the QoS marking of user data to the data message encapsulation. This mapping is accomplished by the CTP Header's 1-byte policy field. However, no configuration of QoS mapping other than copying the user data's already existing markings is defined in CTP. It seems clear that SNMP could be used to configure the mapping to occur differently, but no OIDs are defined that would enable this. Partial compliance is assigned to CTP for this objective.

WiCoP

Note: WiCoP rating for resource control objectives has been upgraded from Failed to Partial. After an additional review of the WiCoP protocol proposal, it was determined that the protocol partially meets resource control objectives.

WiCoP protocol starts its QoS configuration with 802.11e capability exchange between the WTP and AC. The QoS capabilities primitives are included in the capability messages.

WiCoP defines the QoS-Value message that contains 802.11e configuration parameters. This is sent for each group supported by the WTP. WiCoP does not provide an explicit method for configuration of DSCP tags and 802.1P precedence values. It is possible to configure these parameters through SNMP OID configuration method, but WiCoP does not explicitly identify any specific MIBs. Overall, WiCoP partially meets resource control CAPWAP objectives. In order to be fully compliant with the given objective, the protocol needs to identify a clear method to configure 802.1p and DSCP mappings.

6.8. Protocol Security

LWAPP:C, SLAPP:C, CTP:F, WiCoP:F

For the purposes of the protocol security objective, the evaluation team primarily considered whether or not the candidate protocols implement the security features required by the CAPWAP objectives. Please refer to the Security Considerations section of this document.

LWAPP

It appears that the security mechanisms, including the key management portions in LWAPP, are correct. One third-party security review has been performed. However, further security review is warranted since a CAPWAP-specific key exchange mechanism is defined. LWAPP is compliant with the objective.

SLAPP

The SLAPP protocol implements authentication of the WTP by the AC using the DTLS protocol. This behavior is defined in both the discovery process and the 802.11 control process. SLAPP allows mutual and asymmetric authentication. SLAPP also gives informative examples of how to properly use the authentication. SLAPP should add another informative example for authentication of the AC by the WTP. SLAPP is compliant with the objective.

CTP

The original presentation at IETF63 of the preliminary findings of the evaluation team reported that CTP failed this objective. This was on the basis of asymmetric authentication not being supported by CTP. This was due to a misunderstanding of what was meant by asymmetric authentication by the evaluation team. The definitions of the terminology used in [OBJ] were clarified on the CAPWAP mailing list. CTP in fact does implement a form of asymmetric authentication through the use of public keys.

However, CTP still fails to comply with the objective for two reasons:

First, CTP does not mutually derive session keys. Second, CTP does not perform explicit mutual authentication because the 2 parties authenticating do not confirm the keys.

WiCoP

There is not enough specific information to implement WiCoP protocol security features. Although in concept EAP and IPsec make sense, there is no explicit description on how these methods would be used.

6.9. System-Wide Security

LWAPP:C, SLAPP:C, CTP:F, WiCoP:F

LWAPP

LWAPP wraps all control and management communication in its authenticated and encrypted control channel. LWAPP does not seem particularly vulnerable to Denial of Service (DoS). LWAPP should make a recommendation that the Join method be throttled to reduce the impact of DoS attacks against it. Use of an established security mechanism such as IPsec would be preferred. However, LWAPP's independent security review lent enough confidence to declare LWAPP compliant with the objective.

SLAPP

SLAPP is compliant due to wrapping all control and management communication in DTLS. SLAPP also recommends measures to protect against discovery request DoS attacks. DTLS has undergone security review and has at least one known implementation outside of SLAPP. At the time of this writing, DTLS is pending proposed standard status in the IETF.

CTP

CTP introduces a new, unestablished mechanism for AC-to-WTP authentication. For complete compliance, use of an established security mechanism with detailed specifications for its use in CTP is preferred. Alternatively, a detailed security review could be performed. CTP does not point out or recommend or specify any DoS attack mitigation requirements against Reg-Req and Auth-Req floods, such as a rate limiter. Because CTP received an 'F' on its protocol security objective, it follows that system-wide security must also be rated 'F'.

WiCoP

WiCop does not address DoS attack threats. Also, as with the protocol security objective, the protocol needs to explicitly describe its tunnel and authentication methods.

6.10. 802.11i Considerations

LWAPP:C, SLAPP:C, CTP:F, WiCoP:P

LWAPP

LWAPP explicitly defines mechanisms for handling 802.11i in its modes with encryption terminated at the WTP. In order to accomplish this, the AC sends the Pairwise Transient Key (PTK) using the encrypted control channel to the WTP using the Add Mobile message. When encryption is terminated at the AC, there are no special requirements. LWAPP is compliant.

SLAPP

SLAPP defines a control message to send the PTK and Group Temporal Key (GTK) to the WTP when the WTP is the encryption endpoint. This control message is carried on the DTLS protected control channel. SLAPP is compliant.

CTP

CTP lacks a specification for a control message to send 802.11i PTK and GTK keys to a WTP when the WTP is an encryption endpoint. Based on this, CTP fails compliance for this objective. This requirement could be addressed either by defining new control channel information elements or by simply defining SNMP OIDs. The transport of these OIDs would be contained in the secure control channel and therefore protected.

WiCoP

WiCoP lacks documentation on how to handle 4-way handshake. The case for encryption at the AC needs clarification.

6.11. Interoperability

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP supports both split- and local-MAC architectures and is therefore compliant to the letter of the objectives. LWAPP is particularly rich in its support of the split-MAC architecture. However, LWAPP’s support of local-MAC is somewhat limited and could be expanded. LWAPP is lacking a mode that allows local-MAC data

frames to be tunneled back to the AC. A discussion of possible extensions and issues is discussed in the recommendations section of this evaluation.

SLAPP

SLAPP is compliant.

CTP

CTP is compliant.

WiCoP

WiCoP is compliant.

6.12. Protocol Specifications

LWAPP:C, SLAPP:P, CTP:P, WiCoP:P

LWAPP

LWAPP is nearly fully documented. Only a few sections are noted as incomplete. Detailed descriptions are often given to explain the purpose of the protocol primitives defined that should encourage interoperable implementations.

SLAPP

SLAPP is largely implementable from its specification. It contains enough information to perform an interoperable implementation for its basic elements; however, additional informative references or examples should be provided covering use of information elements, configuring multiple logical groups, and so on.

CTP

As noted earlier, there are a few areas where CTP lacks a complete specification, primarily due to the lack of specific MIB definitions.

WiCoP

Due to the lack of specific tunnel specifications and authentication specifications, WiCoP is only partially compliant.

6.13. Vendor Independence

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP is compliant.

SLAPP

SLAPP is compliant.

CTP

CTP is compliant.

WiCoP

WiCoP is compliant.

6.14. Vendor Flexibility

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP is compliant.

SLAPP

SLAPP is compliant.

CTP

CTP is compliant.

WiCoP

WiCoP is compliant.

6.15. NAT Traversal

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP may require special considerations due to it carrying the IP address of the AC and data termination points in the payload of encrypted control messages. To overcome Network Address Translation (NAT), static NAT mappings may need to be created at the NAT'ing device if the AC or data termination points addresses are translated from the point of view of the WTP. A WTP should be able to function in the hidden address space of a NAT'd network.

SLAPP

SLAPP places no out-of-the-ordinary constraints regarding NAT. A WTP could function in the hidden address space of a NAT'd network without any special configuration.

CTP

CTP places no out-of-the-ordinary constraints regarding NAT. A WTP could function in the hidden address space of a NAT'd network without any special configuration.

WiCoP

WiCoP places no out-of-the-ordinary constraints regarding NAT. A WTP could function in the hidden address space of a NAT'd network without any special configuration.

7. Desirable Objective Compliance Evaluation

7.1. Multiple Authentication

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP allows for multiple STA authentication mechanisms.

SLAPP

SLAPP does not constrain other authentication techniques from being deployed.

CTP

CTP supports multiple STA authentication mechanisms.

WiCoP

WiCoP allows for multiple STA authentication mechanisms.

7.2. Future Wireless Technologies

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP could be used for other wireless technologies. However, LWAPP defines very few primitives that are independent of the 802.11 layer.

SLAPP

SLAPP could be used for other wireless technologies. However, SLAPP defines very few primitives that are independent of the 802.11 layer.

CTP

CTP supplies STA control abstraction, methods for extending the forwarding of multiple types of native wireless management frames, and many options for user data tunneling. Configuration management is an extension of SNMP, to which new MIBs could, in concept, be easily plugged in. This helps makes CTP a particularly flexible proposal for supporting future wireless technologies. In addition, CTP has already defined multiple wireless protocol types in addition to 802.11.

WiCoP

WiCoP could be used for other wireless technologies.

7.3. New IEEE Requirements

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP’s extensive use of native 802.11 frame forwarding allows it to be transparent to many 802.11 changes. It, however, shifts the burden of adapting MAC layer changes to the packet processing capabilities of the AC.

SLAPP

SLAPP's use of native 802.11 frames for control and management allows SLAPP a measure of transparency to changes in 802.11. Because SLAPP also supports a mode that tunnels user data as 802.3 frames, it has additional architectural options for adapting to changes on the wireless infrastructure.

CTP

CTP has perhaps the greatest ability to adapt to changes in IEEE requirements. Architecturally speaking, CTP has several options available for adapting to change. SNMP OIDs are easily extended for additional control and management functions. Native wireless frames can be forwarded directly to the AC if necessary. Wireless frames can be bridged to 802.3 frames and tunneled back to the AC to protect the AC from changes at the wireless MAC layer. These options allow many possible ways to adapt to change of the wireless MAC layer.

WiCoP

Because WiCoP uses 802.11 frames for the data transport, it is transparent to most IEEE changes. Any new IEEE requirements may need new configuration and new capability messages between the WTP and AC. The AC would need to be modified to handle new 802.11 control and management frames.

7.4. Interconnection (IPv6)

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP explicitly defines measures for accommodating IPv6. LWAPP is more sensitive to this in part because it carries IP addresses in two control messages.

SLAPP

SLAPP is transparent to the interconnection layer. DTLS and GRE will both operate over IPv6.

CTP

CTP is transparent to the interconnection layer. CTP should be able to operate over IPv6 without any changes.

WiCoP

WiCoP is transparent to the interconnection layer and should be able to operate over IPv6 without changes.

7.5. Access Control

LWAPP:C, SLAPP:C, CTP:C, WiCoP:C

LWAPP

LWAPP uses native 802.11 management frames forwarded to the AC for the purpose of performing STA access control. WTPs are authenticated in LWAPP's control protocol Join phase.

SLAPP

SLAPP has support for multiple authentication methods for WTPs. In addition, SLAPP can control STA access via 802.11 management frames forwarded to the AC or via SLAPP's information element primitives.

CTP

CTP specifies STA access control primitives.

WiCoP

WiCoP specifies access control in [WICOP] section 5.2.2.

8. Evaluation Summary and Conclusions

See Figure 1 (section numbers correspond to RFC 4564 [OBJ]).

CAPWAP Evaluation	LWAPP	SLAPP	CTP	WiCoP
5.1.1 Logical Groups	C	C	C	C
5.1.2 Traffic Separation	C	C	P	P
5.1.3 STA Transparency	C	C	C	C
5.1.4 Config Consistency	C	C	C	C
5.1.5 Firmware Trigger	P	P	P	C
5.1.6 Monitor System	C	C	P	C
5.1.7 Resource Control	C	P	P	P
5.1.8 Protocol Security	C	C	F	F
5.1.9 System Security	C	C	F	F
5.1.10 802.11i Consideration	C	C	F	P
5.1.11 Interoperability	C	C	C	C
5.1.12 Protocol Specifications	C	P	P	P
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	C	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

Figure 1: Summary Results

9. Protocol Recommendation

The proposals presented offer a variety of novel features that together would deliver a full-featured, flexible, and extensible CAPWAP protocol. The most novel of these features leverage existing standards where feasible. It is this evaluation team's opinion that a mix of the capabilities of the proposals will produce the best CAPWAP protocol.

The recommended features are described below. Many of these novel capabilities come from CTP and SLAPP and WiCoP. However, LWAPP has the most complete base protocol and is flexible enough to be extended or modified by the working group. We therefore recommend that LWAPP be used as the basis for the CAPWAP protocol.

The evaluation team recommends that the working group carefully consider the following issues and recommended changes. The evaluation team believes that a more complete CAPWAP protocol will be delivered by addressing these issues and changes.

9.1. High-Priority Recommendations Relevant to Mandatory Objectives

9.1.1. Information Elements

LWAPP's attribute value pair system meets the objectives as defined by the working group. However, it has only 8 bits assigned for attribute types, with an additional 8 bits for a specific element within an attribute type. The evaluation team strongly recommends that a larger number of bits be assigned for attribute types and information elements.

9.1.2. Control Channel Security

LWAPP's security mechanisms appear satisfactory and could serve CAPWAP going forward. However, the evaluation team recommends adoption of a standard security protocol for the control channel.

There are several motivations for a standards-based security protocol, but the primary disadvantage of a new security protocol is that it will take longer and be more difficult to standardize than reusing an existing IETF standard. First, a new security protocol will face a longer, slower approval processes from the Security Area Directorate and the IESG. The new CAPWAP security protocol will need to pass several tests including the following:

What is uniquely required by CAPWAP that is not available from an existing standard protocol? How will CAPWAP's security protocol meet security area requirements for extensibility, such as the ability to support future cipher suites and new key exchange methods? How does this ability compare to established security protocols that have these capabilities?

Points such as these are continually receiving more attention in the industry and in the IETF. Extensibility of key exchange methods and cipher suites are becoming industry standard best practices. These issues are important topics in the IETF Security Area Advisory Group (SAAG) and the SecMech BOF, held during the 63rd IETF meeting.

These issues could be nullified by adopting an appropriate existing standard security protocol. IPsec or DTLS could be a standards alternative to LWAPP's specification. DTLS presents a UDP variant of Transport Layer Security (TLS). Although DTLS is relatively new, TLS is a heavily used, tried-and-tested security protocol.

The evaluation team recommends that whatever security protocol is specified for CAPWAP, its use cases must be described in detail. LWAPP does a good job of this with its proposed, proprietary method. If an updated specification is developed, it should contain at least one mandatory authentication and cipher method. For example, pre-shared key and x.509 certificates could be specified as mandatory authentication methods, and Advanced Encryption Standard (AES) Counter Mode with CBC-MAC Protocol (CCMP) could be selected as a mandatory cipher.

Given the possibilities for code reuse, industry reliance on TLS, and the future for TLS, DTLS may be a wise alternative to a security method specific to CAPWAP. In addition, use of DTLS would likely expedite the approval of CAPWAP as a proposed standard over the use of CAPWAP-specific security mechanisms.

9.1.3. Data Tunneling Modes

9.1.3.1. Support for Local MAC User Data Tunneling

The issue of data encapsulation is closely related to the split- and local-MAC architectures. The split-MAC architecture requires some form of data tunneling. All the proposals except LWAPP offer a method of tunneling in local-MAC mode as well. By local-MAC data tunneling, we mean the tunneling of user data as 802.3 Ethernet frames back to the AC from a WTP that is otherwise in local-MAC mode.

Tunneling data in local-MAC mode offers the ability for implementers to innovate in several ways even while using a local-MAC architecture. For example, functions such as mobility, flexible user data encryption options, and fast handoffs can be enabled through tunneling of user data back to an AC, or as LWAPP defines, a data termination endpoint, which could be different from the AC. In addition, there are special QoS or application-aware treatments of user data packets such as voice or video. Improved transparency and compatibility with future wireless technologies are also possible when encapsulating user data in a common format, such as 802.3, between the access point and the AC or other termination point in the network.

Another possibility is when a native wireless MAC changes in the future, if a new WTP that supports this MAC change can also support a wireless MAC -> 802.3 integration function, then the wireless MAC layer change may remain transparent to an AC and still maintain many of the benefits that data tunneling can bring.

LWAPP does support a header for tunneled user data that contains layer 1 wireless information (Received Signal Strength Indication (RSSI) and Signal-to-Noise Ratio (SNR)) that is independent of the wireless layer 2 MAC. Innovations related to the use of RSSI and SNR at the AC may be retained even when tunneling 802.3 user data across different wireless MACs.

It is likely that many other features could be created by innovative implementers using this method. However, LWAPP narrowly defines the local-MAC architecture to exclude an option of tunneling data frames back to the AC. Given the broad support for tunneling 802.3 data frames between the WTP and AC across all the proposals and existing proprietary industry implementations, the evaluation team strongly recommends that the working group consider a data tunneling mode for local-MAC be added to the LWAPP proposal and become part of the standard CAPWAP protocol.

9.1.3.2. Mandatory and Optional Tunneling Modes

If more than one tunneling mode is part of the CAPWAP protocol, the evaluation team recommends that the working group choose one method as mandatory and other methods as optional. In addition, the CAPWAP protocol must implement the ability to negotiate which tunneling methods are supported through a capabilities exchange. This allows ACs and WTPs freedom to implement a variety of modes but always have the option of falling back to a common mode.

The choice of which mode(s) should be mandatory is an important decision and may impact many decisions implementers have to make with their hardware and software choices for both WTPs and ACs. The evaluation team believes that the working group should address this issue of local-MAC data tunneling and carefully choose which mode(s) should be mandatory.

9.2. Additional Recommendations Relevant to Desirable Objectives

9.2.1. Access Control

Abstraction of STA access control, such as that implemented in CTP and WiCoP, stands out as a valuable feature as it is fundamental to the operational capabilities of many types of wireless networks, not just 802.11. LWAPP implements station access control as an 802.11-

specific function via forwarding of 802.11 control frames to the access controller. LWAPP has abstracted the STA Delete function out of the 802.11 binding. However, the Add STA function is part of the 802.11 binding. It would be useful to implement the wireless MAC independent functions for adding a STA outside of the 802.11 binding.

9.2.2. Removal of Layer 2 Encapsulation for Data Tunneling

LWAPP currently specifies layer 2 and layer 3 methods for data tunneling. The evaluation team believes that the layer 2 method is redundant to the layer 3 method. The team recommends that the layer 2 method encapsulation be removed from the LWAPP protocol.

9.2.3. Data Encapsulation Standard

LWAPP’s layer 3 data encapsulation meets the working group objectives. However, the evaluation team recommends the use of a standards-based protocol for encapsulation of user data between the WTP and AC. GRE or Layer 2 Tunneling Protocol (L2TP) could make good candidates as standards-based encapsulation protocols for data tunneling.

Using a standard gives the opportunity for code reuse, whether it is off-the-shelf microcode for processors, code modules that can be purchased for real-time operating systems, or open-source implementations for Unix-based systems. In addition, L2TP and GRE are designed to encapsulate multiple data types, increasing flexibility for supporting future wireless technologies.

10. Normative References

[802.11i] IEEE Standard 802.11i, "Medium Access Control (MAC) Security Enhancements", July 2004.

[ARCH] Yang, L., Zerfos, P., and E. Sadot, "Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 4118, June 2005.

[OBJ] Govindan, S., Ed., Cheng, H., Yao, ZH., Zhou, WH., and L. Yang, "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 4564, July 2006.

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

11. Informative References

[CTP] Singh , I., Francisco, P., Pakulski , K., and F. Backes, "CAPWAP Tunneling Protocol (CTP)", Work in Progress, April 2005.

[DTLS] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[LWAPP] Calhoun, P., O'Hara, B., Kelly, S., Suri, R., Williams, M., Hares, S., and N. Cam Winget, "Light Weight Access Point Protocol (LWAPP)", Work in Progress, March 2005.

[RFC3127] Mitton, D., St.Johns, M., Barkley, S., Nelson, D., Patil, B., Stevens, M., and B. Wolff, "Authentication, Authorization, and Accounting: Protocol Evaluation", RFC 3127, June 2001.

[SLAPP] Narasimhan, P., Harkins, D., and S. Ponnuswamy, "SLAPP : Secure Light Access Point Protocol", Work in Progress, May 2005.

[WICOP] Iino, S., Govindan, S., Sugiura, M., and H. Cheng, "Wireless LAN Control Protocol (WiCoP)", Work in Progress, March 2005.

Authors' Addresses

Darren P. Loher
Envysion, Inc.
2010 S. 8th Street
Boulder, CO 80302
USA

Phone: +1.303.667.8761
EMail: dplore@gmail.com

David B. Nelson
Enterasys Networks, Inc.
50 Minuteman Road
Anover, MA 01810-1008
USA

Phone: +1.978.684.1330
EMail: dnelson@enterasys.com

Oleg Volinsky
Colubris Networks, Inc.
200 West Street
Waltham, MA 02451
USA

Phone: +1.781.547.0329
EMail: ovolinsky@colubris.com

Behcet Sarikaya
Huawei USA
1700 Alma Dr. Suite 100
Plano, TX 75075
USA

Phone: +1.972.509.5599
EMail: sarikaya@ieee.org

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).