Network Working Group
Internet-Draft
Expires: November 2, 2005

P. Calhoun
B. O'Hara
Cisco Systems, Inc.
S. Hares
Nexthop Technologies, Inc.
May 2005

# LWAPP Self Evaluation
# draft-calhoun-capwap-lwapp-objectives-comparison-01

## Status of this Memo



## Copyright Notice



## Abstract

The IETF's CAPWAP working group has requested that all candidate protocols submitted must provide a document which evaluates how each protocol meets the objectives. This document describes in detail how the LWAPP protocol meets the CAPWAP objectives.

Table of Contents

## 1. Introduction

The CAPWAP working group has identified a set of objectives [2] that must be met for a protocol to be considered for standardization. The LWAPP protocol has been submitted to CAPWAP for consideration.

The authors of the LWAPP specification [4] feel that the working group should consider the following important facts about the LWAPP protocol:

- The LWAPP protocol has been available as a personal contribution for well over 18 months. During this time, many comments have been received by members of the Internet community, and as a consequence the specification has become much clearer and complete.

- The current document not only includes a completely working protocol for Local and Split MAC architectures, but it also includes the necessary behavioral specification that is required to guarantee interoperability.

- Local and Split MAC LWAPP enabled products have been shipping for well over 2 years, and many of the operational issues found in deployments have been addressed in the specification.

Given the above, the authors of the LWAPP specification feel that the CAPWAP Working Group would benefit tremendously by selecting the LWAPP protocol as the WG candidate. While we do not believe that the document is ready for publication, we believe that the quality of the protocol and the document would help expedite the publication of the CAPWAP protocol.

The authors of the LWAPP specification feel that providing a strong security solution to the CAPWAP list is of the utmost importance, and as a consequence recently requested a third party security review [8]. All recommendations made in this review have been addressed in the LWAPP specification.

This document describes how the LWAPP protocol complies to the objectives.

### 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 [1].

## 2. Objectives

LWAPP is a generic protocol defining how Wireless Termination Points communicate with Access Controllers. Wireless Termination Points and Access Controllers may communicate either by means of Layer 2 protocols or by means of a Layer 3 routed IP network.

### 2.1 Mandatory Objectives

This section contains all of the objectives that have been considered as being mandatory in order for a protocol to be considered.

#### 2.1.1 Logical Groups

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

This is being interpreted as stating that a protocol must allow for the WTP to provide service for multiple SSIDs (or WLANs), each with a distinct BSSID.

##### 2.1.1.1 Protocol Evaluation

The LWAPP protocol was designed to allow individual WTPs to support multiple BSSID/SSIDs, which allows for logical groups. From the AC's perspective, a logical group is created through the creation of a WLAN. A WLAN is a logical wireless network that is identified through the SSID and is advertised through the Beacon and Probe Response. Each WLAN can have a separate security policy, and has a unique BSSID, enabling the 802.11 stations to identify every WLAN as a separate network.

In order to create a WLAN, the LWAPP protocol defines a primitive called the IEEE 802.11 Add WLAN (section 11.8.1.1 of the LWAPP specification), which is used by the AC to create an SSID on the WTP. In the WLAN creation process, the AC selects an unused WLAN Identifier, which is used to refer to the WLAN in future commands. An AC could use the same WLAN Identifier to refer to a single WLAN on all of its WTPs, ensuring a consistent interface across all WTPs.

There are specific rules on the BSSID to WLAN Identifier mapping, which is detailed in section 11.4. When a WTP communicates with the AC, it specifies the maximum number of BSSIDs it has through the IEEE 802.11 WTP WLAN Radio Configuration message element (see section 11.9.1), which is used by the AC to determine the maximum number of logical groups that can be supported on the WTP.

When user data is sent from the AC to the WTP, the BSSID field in the 802.11 header is used to identify the logical network which the packet is to be sent through. The same is true for packets received by the WTP from a station, where the BSSID would be used by the AC to recognize which logical network the packet was received on. It is expected that the AC and the WTP perform policing to ensure that a station only send packets on the correct BSSID.

Furthermore, the 802.11 binding LWAPP section defines the WLANS field of the LWAPP header (in section 11.3.1 of the LWAPP specification). In this section, the specification states that data packets sent from the AC to the WTP include the WLAN Identifier that was used during the creation of the WLAN.

Note that for Local MAC WTPs, the AC MAY send a VLAN Name in the Add Mobile (see section 11.7.1.1), instructing the WTP to locally bridge the client's data frames to the specific VLAN. This function allows the WTP to be able to support logical groups in Local MAC mode.

#### 2.1.1.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.2 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.

Our personal interpretation of this objective is that there are two separate requirements. First, the data and control component of the protocol must be uniquely identified. Second, the protocol should allow for the control and data traffic to terminate on separate infrastructure devices, meaning that an AC may be split into two separate devices, one that handles the control and one that handles data.

#### 2.1.2.1 Protocol Evaluation

The LWAPP header, described in section 3.1 of the LWAPP specification, defines the 'C' bit, which when set indicates that the LWAPP frame contains a control frame. When the bit is cleared, the payload contains an LWAPP data frame.

During the join phase, the AC may optionally include the WTP Manager Data IP Address (in section 6.2.4 and 6.2.5 of the LWAPP Specification), which is used to inform the WTP of the IP address to which it is to forward the LWAPP data frames.

The LWAPP protocol also supports Local MAC, which allows the user's data to be locally bridge at the WTP instead of being tunneled to the AC. This is an additional mechanism of keeping the data and control traffic separated. Further information on Local MAC can be found in section 11.1.2 of the LWAPP specification. Whether a WTP wishes to operate in Local vs. Split MAC is advertised in the IEEE 802.11 WTP Mode and Type message element, which can be found in section 11.9.12.

#### 2.1.2.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.3 Wireless Terminal Transparency

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

Our interpretation is that the introduction of the LWAPP protocol, and therefore the new CAPWAP architecture, MUST be transparent to the 802.11 stations. Interoperability MUST be guaranteed without any additional or new functionality on the station.

#### 2.1.3.1 Protocol Evaluation

The LWAPP protocol was designed specifically to allow for centralized control and management of WTPs without any impact on the stations. Once a WTP has joined an AC, the latter will push down 802.11 and antenna configuration to the WTP, allowing it to provide service.

Section 11.1 of the LWAPP specification defines the distribution of 802.11 functions, ensuring that all of the functions currently provided by an autonomous access point is preserved.

Lastly, the proof is in the pudding. There are hundreds of thousands of Local and Split MAC LWAPP enabled WTPs, and tens of thousands of LWAPP enabled ACs, deployed in the field today, and these have been proven to work seamlessly with all 802.11 stations on the market. Furthermore, LWAPP AC and WTPs have been certified by the WiFi Alliance as being interoperable for 802.11b, 802.11a, 802.11g, WPA and WPA2 [10]. Certification testing performed by the WiFi Alliance is focused primarily on protocol compliance and interoperability between 802.11 stations and infrastructure (APs). In the LWAPP model, the combination of the WTP and the AC comprises the AP.

#### 2.1.3.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.4 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.

Our interpretation of this requirements is that there are two separate underlying requirements. First, there must be a mechanism by which the AC can propagate configuration information to the WTP, ensuring an AC is capable of easily maintaining the consistent configuration of every WTP associated with it. Second, there is a requirement stating that the WTP MUST periodically send utilization information to the AC, allowing the latter to make real-time configuration decisions to optimize the WLANs performance.

#### 2.1.4.1 Protocol Evaluation

The LWAPP protocol provides flexibility in how WTP configuration is managed. To put it simply, a WTP has one of two options:

1. WTP retain no configuration and simply abides by the configuration provided by the AC.

2. WTP retain the configuration of parameters provided by the AC that are non-default values.

If the WTP opts to save configuration locally, the LWAPP protocol state machine defines the "configure" state, which is used during the initial binding WTP-AC phase, which allows for configuration exchange. During this period, the WTP sends its current configuration overrides to the AC via the Configure Request message. A configuration override is a parameter that is non-default. One example is that in the LWAPP protocol the default antenna configuration is internal omni antenna. However, a WTP that either has no internal antennas, or has been explicitly configured by the AC to use external antennas, would send its antenna configuration during the configure phase, allowing the AC to become aware of the WTP's current configuration.

Once the WTP has provided its configuration to the AC, the AC sends down its own configuration. This allows the WTP to inherit the configuration and policies on the AC.

An LWAPP AC maintains a copy of each active WTP's configuration. There is no need for versioning or other means to identify configuration changes. If a WTP becomes inactive, the AC MAY delete the configuration associated with it. If a WTP were to fail, and connect to a new AC, it would provide its overridden configuration

parameters, allowing the new AC to be aware of the WTP's configuration.

As a consequence, this model allows for resiliency, whereby in light of an AC failure, another AC could provide service to the WTP. In this scenario, the new AC would be automatically updated on any possible WTP configuration changes - eliminating the need for inter-AC communication or the need for all ACs to be aware of the configuration of all WTPs in the network.

Once the LWAPP protocol enters the Run state, the WTPs begin to provide service. However, it is quite common for administrators to require that configuration changes be made while the network is operational. Therefore, the Configuration Update Request is sent by the AC to the WTP in order to make these changes at run-time.

The LWAPP protocol defines various commands that allow a WTP to inform the AC of real-time events. Including:

Decryption Errors: When encryption is performed in the WTP, there is a configurable timer sent to the WTP requesting a periodic decryption error report. When sent by the WTP, the decryption error report includes the MAC address(es) of the offending stations.

Duplicate IP Address: Given that WTPs are commonly installed in hard to reach places, it is necessary to know when the WTP detects network related errors without access to a console. Therefore, the LWAPP protocol defines a primitive that allows the WTP to report when it detects another host that has a duplicate IP address.

Statistics: During the configuration phase, the AC transmits the statistics interval period, which is used by the WTP to send statistics reports to the AC. The LWAPP protocol defines an 802.11 binding specific statistics report message (see section 11.4.2.1 in the LWAPP specification), which is used to communicate load information to the AC. It is important to note that since all valid 802.11 data frames are tunneled to the AC, the AC may also calculate load statistics. New wireless technologies wishing to make use of LWAPP will need to define a technology binding statistics report format.

802.11 MIC Countermeasures: The 802.11i specification [7] describes countermeasures that must be taken when a MIC error is detected. This event is sent by the WTP to the AC when such an event occurs, allowing the AC to take appropriate action (e.g., disabling the WLAN for a period of 60 seconds).

Radio Fail Indication: As previously mentioned, since the WTP is not within easy physical access, assuming that observing LEDs to ensure the health of the WTP is not sufficient. Therefore, when a WTP detects a radio error, it issues a radio fail indication error.

WTP Failure: A WTP failure may require the AC to take some specific action, which is not defined in the LWAPP specification. However, the LWAPP protocol does define the Echo Request command, which is used to detect network failures.

Should the working group define additional information elements they feel would be useful to send from the WTP to the AC, the LWAPP protocol defines extensible mechanisms to issue event related information.

#### 2.1.4.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.5 Firmware Trigger

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

#### 2.1.5.1 Protocol Evaluation

The LWAPP state machine states that during the join phase, the AC and WTP exchange version numbers, including the hardware type and configuration. This information is used by the WTP to detect whether a firmware upgrade is required. The WTP specifies the filename it wishes to have downloaded through the Image Download message element (see section 8.1.1).

Note that the LWAPP protocol also defines the actual primitives required to download the firmware to the WTP. It is not clear whether the working group has decided whether this function of the protocol is in or out of scope, but the authors feel that being able to piggyback off the security association already established with the AC provides for secure firmware download, minimizing vulneratibilities and possible confusion or errors that could occur by attempting to integrate multiple protocols within a single state machine in a secure fashion.

#### 2.1.5.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.6 Monitoring and Exchange of System-wide Resource State

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

#### 2.1.6.1 Protocol Evaluation

The objective describes two separate set of segments; switched and wireless.

On the switched segment, the LWAPP protocol provides a rich set of message elements to allow for the WTP and AC to exchange information, including, but not limited to, the WTP's firmware version and number of radios (see WTP Descriptor in section 5.1.2), radio failures (see IEEE 802.11 WTP Radio Fail Alarm Indication in section 11.8.3.2) and duplicate IP Address detection (see Duplicate IP Address in section 8.5.2 and 8.5.3). The WTP also has the ability to provide the reboot statistics, and the reason for a previous failure (see WTP Reboot Statistics in section 7.2.7).

On the wireless side, the WTP will sent statistics to the AC based on the AC's policy, which is dictated through the Statistics Timer (see section 7.2.5). In Split MAC architectures, the AC also receives the user's traffic in a tunnel form, and may maintain additional local state as it sees fit, including signal strength information, as specified in section 11.3.1 of the LWAPP specification.

There are various tools available in the LWAPP protocol to allow for either the AC to request information from the WTP, or for the WTP to send unsolicited statistics (of various form) to the AC. The authors feel that if the working group has identified additional information they would like the AC to gain access to, we believe this can be done within the confines of the protocol.

#### 2.1.6.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.7 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.

Author comment: There are several requirements defined in the Resource Control Objective such as the ability to provide quality of service based on the 802.11e standard, as well as allow for the use of 802.11k or 802.11v. The objective also mentions 802.11u, which

deals with inter-technology roaming, and since the authors do not understand how 802.11u relates to resource control, this specific standard will not be mentioned in this section.

#### 2.1.7.1 Protocol Evaluation

The LWAPP protocol defines the IEEE 802.11 WTP Quality of Service message element in section 11.9.14, which is used by the AC to push global 802.11e policies to the WTPs, ensuring that they are providing consistent service to the stations. This message element contains policies for the WTP for every access class defined in the 802.11e specification. It contains the CwMin, CwMax and AIFS fields which dictate how the individual transmit queues are to behave. The data structure also includes a CBR fields, which when present, dictates the amount of air time the access class is allowed to have, per beacon period (in %). The message element also specifies whether data frames are to be tagged, and if so, the tagging method, in terms of 802.1P or DSCP. When tagging is to be performed, there is a separate 802.1P and/or DSCP value for every access class. Note that although one could conceive there being a single QoS policy for a given network, there are no restrictions on having an AC sending a separate configuration to a given WTP.

When the AC creates a WLAN on the WTP, through the IEEE 802.11 Add WLAN command, defined in section 11.8.1.1, the AC may set a default policy for all users assigned to the WLAN. In this case, the AC may include the WMM [9] and 802.11e Information Elements that are to be included in the Beacon and Probe Requests, as well as the default QoS value. The default value is to be used in determining the access class queue to use for all packets for the given user, unless a specific override was received when the user's context was created on the WTP.

When an AC pushes a mobile's policy to the WTP, through the Add Mobile command, which is defined in section 11.7.1.1, it can specify the QoS policy for the station. For instance, the AC specifies whether the station supports either the WMM or the 802.11e protocol. The Add Mobile command also allows the AC to dictate how the user's data packets are to be treated from a QoS perspective. For instance, if the AC determines that a given station is to be provided either WMM or 802.11e service, it would set the appropriate bits, and ensure that the 802.11e UP field is set accordingly within the encapsulated 802.11 data packet to the user. The quality of service field is to be used by the WTP on any packets sent over the air for which no UP information is available (default value for non QoS marked packets).

The Station QoS Profile defined in section 11.7.1.3 of the LWAPP specification is included in an Add Mobile command and is used by the

AC to set the upper limit for incoming WMM or 802.11e packets from a given user. The 802.1P precedence value is to be considered to be the maximum value allowed by the station. The WTP is expected to perform policing of incoming data from the station, and remark any packets as it deems necessary.

The IEEE 802.11 Update Mobile QoS message element (see section 11.7.1.4) may be sent at any time by the AC to the WTP in order to modify the quality of service properties associated with the station. The 802.1P and DSCP fields have two purposes. For WMM or 802.11e stations, this value is intended to be the maximum value that can be set for a given station. However, for non-WMM or non-802.11e stations, these values are intended to be the default value for all packets received from the station. Although not related to QoS per-se, if the VLAN identifier field in the message element is intended to represents the VLAN on which the station is to be assigned when the LWAPP protocol is used in the local MAC mode.

The LWAPP protocol defines Quality of Service recommendations for both LWAPP control frames (see section 4.2.3), and 802.11 MAC management frames (see section 11.5).

In terms of support of 802.11e (or 802.11k), the WTP is expected to forward any received Action frames received on behalf of the station. This allows the AC to set the QoS policy for the user, including admission control. For 802.11k, the various Radio Management messages would be exchanged transparently through the WTP. The applicable QoS for these management frames, and all future 802.11 extensions, are described in section 11.5.

Unfortunately, the 802.11u task group is still to early in its infancy to determine what functionality it will provide, but should standard management frames be used, the LWAPP protocol could tunnel them transparently through the WTP.

#### 2.1.7.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.8 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.

Our interpretation of this objective is that it states that some cryptographic exchange must be defined in the specification in order to protect the contents of the control protocol. Further, this

requirement states that mutual authentication is required. The requirement states the key exchange protocol must be designed in such a way where once a security association has been established, there is no possible compromises. Lastly, while the requirements do not specifically state how the WTP and the AC are to authenticate each other, it does state that the protocol should allow for either symmetric or asymmetric cryptography.

#### 2.1.8.1 Protocol Evaluation

The LWAPP protocol defines two different types of methods by which authentication occurs between the AC and the WTP. The first is based on asymmetric cryptography and relies on the presence of X.509 certificates on both the AC and the WTP. The second method is symmetric in nature and relies on pre-shared keys, which must be configured a priori on both the AC and the WTP.

The LWAPP state machine defines the Join phase, which is used to create a secure binding between the WTP and the AC. During the join phase, session keys, as well as an IV which is used for the purposes of encrypting the control traffic, are mutually derived. The Join Reply and Join ACK messages provide mutual authentication between the peers, while the Join ACK and Join Confirm provide explicit key confirmation. The authenticated key exchange, which supports either X.509 certificates or pre-shared keys, can be found in section 10.3.2 of the LWAPP specification.

Once session keys have been exchanged between the WTP and the AC, the LWAPP protocol defines how the control frames are to be encrypted in section 10.2. The encryption algorithm used is AES-CCM, and this section also discussed how the initialization vectors are derived.

The LWAPP state machine also defines a key update mechanism, which allows for the session keys to be refreshed over time, minimizing the amount of data that is encrypted with the same session key. The key update process is very straightforward, and uses a separate derivation key that was originally derived either during the phase or the last key update messages. Similar to the Join messages, the key update process also includes explicit key confirmation and mutual authentication. The details of this process can be found in section 10.3.3.

The Security Considerations section of the LWAPP protocol suggest that the AC provide some form of authorization when a WTP attempts to connect. This would disallow for unauthorized WTPs to connect. Further, when the certificate based approach is used, the AC should validate the identity of the WTP within the certificate itself.

The Security Considerations section also includes specific text guiding the implementer on avoiding possible Join Request replay attacks. This recommendation eliminates the possibility for the AC to prematurely disconnect LWAPP connections with trusted WTPs.

#### 2.1.8.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.9 System-wide Security

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

#### 2.1.9.1 Protocol Evaluation

An Access Controller and Wireless Termination Point that support the LWAPP protocol are no more vulnerable than any off the shelf access point, meaning that the LWAPP protocol itself does not in any way add to the compromise of the system. As previously mentioned, the control protocol is secured through a key exchange that is protected either through a pre-shared key or via an X.509 certificate.

When using X.509, section 10.4 of the LWAPP protocol defines a certificate profile that binds a certificate to a specific role. For instance, a WTP cannot impersonate an AC since its certificate clearly states it is only valid for use with a WTP. This additional level of security eliminates man-in-the-middle attacks, such as one where a compromised WTP impersonates an AC to a valid WTP, but acts as a WTP to a valid AC.

There is one specific issue that is mentioned in the objectives draft, which states that PMK sharing shall not be permitted. It is important to note that the PMK is held at the AC, whether or not the PMK is shared across multiple WTPs is implementation specific and completely outside the scope of the LWAPP protocol. It is assumed that LWAPP enabled ACs comply with the 802.11i protocol, which has strict guidelines on key usage. However, the introduction of the 802.11r protocol will allow for fast handoffs by using the original PMK for additional key derivation purposes. A centralized AC approach facilitates support for such future 802.11 extensions.

One advantage of the centralized policy enforcement architecture that is inherited from the LWAPP protocol is the fact that the AC is capable of detecting and correlating attacks across multiple WTPs, and allow the administrator to take some action. However, these types of actions are not specified in the LWAPP protocol. However, by having access to the complete 802.11 header, and associated signal

strength, and AC can make much smarter decisions than if it only had access to 802.3 frames.

If rogue clients attempt to send improperly encrypted frames, either through an SSID that mandates a static WEP key (see section 7.3.1), or by creating a MIC attack (see section 11.9.15), the AC will be notified of the failure, including the offending station's MAC address, as well as the WTP on which the attack was detected. In the case of a WEP decryption error, it is important to note this information is provided to the AC as a scheduled event, and not on each individual decryption error, ensuring that such an attack does not in turn creates a DoS attack on the AC. When a MIC error occurs, the event MUST be sent immediately to the AC in order for it to take countermeasures, such as disabling the WLAN for 60 seconds, as required by the 802.11i specification.

Although not specified in the LWAPP protocol specification, it is assumed that AC manufacturers build proper defenses into their implementation to detect and report malicious behavior, such as excessive failed authentication attempts or associations, etc. Note that these types of protections are required in any good 802.11 AP implementation, regardless of whether the infrastructure is of the autonomous form, or uses a hierarchical architecture.

The LWAPP protocol, through section 11.2, provides explicit guidance to the implementers on how to make use of the protocol to handle an 802.11i roaming station, ensuring that there are no possibilities for denial of service or other session highjacking vulnerabilities.

The LWAPP protocol also provides a statement in the security considerations section discouraging the use of WEP, but the authors of the LWAPP protocol wish to reinforce that they do not believe that the introduction of LWAPP (or any centralization protocol) increases the risks already present with the use of WEP.

#### 2.1.9.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.10 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.

#### 2.1.10.1 Protocol Evaluation

The LWAPP protocol is capable of supporting both local and split MAC approaches. Section 11.1.1 defines the Split MAC mode, where authentication is centralized but encryption can be performed either on the WTP or the AC. Section 11.1.2 defines Local MAC mode, where the authenticator resides in the AC, but since the WTP performs local bridging of user traffic, encryption occurs on the WTP. In either case, the PMK is maintained in the AC.

During the LWAPP join phase, which creates the binding between the WTP and the AC, the WTP specifies its encryption capabilities, through the WTP Descriptor message element (described in section 5.1.2). This message element allows the WTP to specify whether it is capable of providing encryption capabilities, and if so, which algorithms are supported. For Split MAC mode, it is the AC's policy that dictates where encryption will be provided, through the encrypt policy field of the Add Mobile message element. For Local MAC mode, this information element is used by the AC to ensure that the WTP is capable of providing secure services (and may restrict the mode of operation based on this information).

When a WLAN has been configured for 802.1X authentication, once a station has associated, the AC would send down an Add Mobile message element that specifies that the policy requires that only 802.1X frames are to be permitted (see section 11.1 for more details on the use of the Add Mobile message element). Optionally, the AC may specify a session key should the EAP frames require encryption. The WTP then simply forwards all 802.1X frames either to the station or the AC (depending upon the direction of the frame). The WTP does not participate in the 802.1X authentication exchange.

Once the 802.11i process is completed, and the AC has computed the PTK, if the AC's policy states that encryption is to be performed on the WTP, it would issue a new Add Mobile message element, but this time without the 802.1X only bit set, and the PTK in the session key field and the encrypt policy field set to an appropriate value. If the AC's policy states that encryption is to be performed at the AC, then it would omit the session key, and set the encrypt policy field to "Clear Text". Again, this process is illustrated and documented in section 11.1.

#### 2.1.10.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.11 Interoperability Objective

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

#### 2.1.11.1 Protocol Evaluation

The LWAPP protocol is capable of supporting both local and split MAC approaches. Further, the LWAPP protocol provides specific guidance on how to make use of the protocol in order to provide either service in section 11.1. The authors wish to state that LWAPP products already exist in the market today that are capable of supporting either modes of operation. As defined in [5] also outlines both modes of operation to help identify the main differences.

The method by which a WTP advertises its mode of operation is through the WTP Mode and Type message element, which may be found in section 11.6.12. When set to zero, the mode of operation is Split MAC, while when set to two it is Local MAC.

#### 2.1.11.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.12 Protocol Specifications

Any WTP or WLAN controller 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.

#### 2.1.12.1 Protocol Evaluation

The LWAPP protocol is a fully specified protocol that is capable of ensuring that any WTP or AC vendor can gain guaranteed interoperability. Note that the authors realize that some changes will be required during the standardization phase, and that some of these changes will increase the level of interoperability by addressing areas that may be underspecified. However, the LWAPP protocol has been publicly available for well over 18 months, has been shipping in products for even longer and has undergone many external recommendations that help interoperability. Lastly, the LWAPP specification includes significant behavioral text to help guarantee interoperability.

#### 2.1.12.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.13 Vendor Independence

A WTP vendor SHOULD be able to make modifications to hardware without any WLAN controller vendor involvement.

#### 2.1.13.1 Protocol Evaluation

Because the LWAPP protocol is fully specified, it is assumed that the WTP vendors will do the actual implementation of the protocol on their hardware, providing them with the ability to make any necessary changes as they see fit without the involvement of a third party AC vendor.

#### 2.1.13.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.14 Vendor Flexibility

The CAPWAP protocol MUST NOT limit WTP vendors in their choice of local-MAC or split-MAC WTPs. It MUST be compatible with both types of WTPs.

#### 2.1.14.1 Protocol Evaluation

The authors of the LWAPP protocol have had discussions with the most popular MAC vendors to ensure that the assumptions behind the split MAC approach would work on any chipset, and have yet to find a vendor that could not support LWAPP.

Since the LWAPP protocol is fully specified, and the fact that the assumption behind having a specification that any WTP vendor may implement without the aid of any AC vendors, allows for innovation by these third party WTP vendors without requiring that they disclose any confidential information about their chip.

Finally, the LWAPP protocol supports both Local and Split MAC approaches, which are documented in section 11.1.

#### 2.1.14.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.1.15 NAT Traversal

The CAPWAP protocol MUST NOT prevent the operation of established methods of NAT traversal.

#### 2.1.15.1 Protocol Evaluation

There are two specific situations where a NAT system may be used in conjunction with LWAPP. The first consists of a configuration where the WTP is behind a NAT system. Given that all communication is initiated by the WTP, and all communication is performed over IP using a single UDP port, the protocol easily traverses NAT systems in this configuration.

The second configuration is one where the AC sits behind a NAT and there are two main issues that exist in this situation. First, an AC communicates its interfaces, and associated WTP load on these interfaces, through the WTP Manager Control IP Address (see section 5.2.4 of the LWAPP specification). This message element is currently mandatory, and if NAT compliance became an issue, it would be possible to either:

1. Make the WTP Manager Control IP Address optional, allowing the WTP to simply use the known IP Address. However, note that this approach would eliminate the ability to perform load balancing of WTP across ACs, and therefore is not the recommended approach.

2. Allow an AC to be able to configure a NAT'ed address for every associated AC that would generally be communicated in the WTP Manager Control IP Address message element.

3. Require that if a WTP determines that the AC List message element (see section 6.2.5) consists of a set of IP Addresses that are different from the AC's IP Address it is currently communicating with, then assume that NAT is being enforced, and require that the WTP communicate with the original AC's IP Address (and ignore the WTP Manager Control IP Address message element(s)).

Another issue related to having an AC behind a NAT system is LWAPP's support for the CAPWAP Objective to allow the control and data plane to be separated. In order to support this requirement, the LWAPP protocol defines the WTP Manager Data IP Address message element (see section 6.2.4), which allows the AC to inform the WTP that the LWAPP data frames are to be forwarded to a separate IP Address. This feature MUST be disabled when an AC is behind a NAT. However, there is no easy way to provide some default mechanism that satisfies both the data/control separation and NAT objectives, as they directly conflict with each other. As a consequence, user intervention will be required to support such networks.

LWAPP has a feature that allows for all of the ACs identities supporting a group of WTPs to be communicated through the AC List message element. This feature must be disabled when the AC is behind

a NAT and the IP Address that is embedded would be invalid.

The LWAPP protocol has a feature that allows an AC to configure a static IP address on a WTP. The WTP Static IP Address Information message element provides such a function, however this feature SHOULD NOT be used in NAT'ed environments, unless the administrator is familiar with the internal IP addressing scheme within the WTP's private network, and does not rely on the public address seen by the AC.

When a WTP detects the duplicate address condition, it generates a message to the AC, which includes the Duplicate IP Address message element (see section 8.5.2). Once again, it is important to note that the IP Address embedded within this message element would be different from the public IP address seen by the AC.

#### 2.1.15.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.2 Desirable Objectives

#### 2.2.1 Multiple Authentication Mechanisms

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

#### 2.2.1.1 Protocol Evaluation

The LWAPP protocol allows for multiple SSIDs be to created on a WTP, and for every one of these WLANs, a separate security policy may exist. For instance, the Encryption Policy field of the IEEE 802.11 Add WLAN message element, described in section 11.8.1.1, defines static and Dynamic WEP encryption, as well as TKIP and AES. Further, the Encryption Policy may be set to Clear Text, which would be used in the case where a captive portal were to be used (or for centralized AES or TKIP encryption/decryption).

#### 2.2.1.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

#### 2.2.2 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.

#### 2.2.2.1 Protocol Evaluation

Section 2.1 of the LWAPP specification describes the process that must be followed in order to define a wireless technology binding for LWAPP. Further, section 11 defines the IEEE 802.11 binding. While no other technology bindings have been defined published, the authors have been working on other wireless technologies and feel very confident that this can be done with relative ease.

One of the reasons why it is felt that the LWAPP protocol is sufficiently flexible is the fact that the protocol simply states that all "access related" wireless control frames (e.g., Association Request for 802.11) are tunneled to the AC. While this does impose the requirement that the AC must understand the individual wireless technologies, it does simplify the WTP implementation, which is the ultimate goal. Further, the authors would argue that this would be required regardless in order for the AC to be able to provide additional services, such as centralized authentication and key distribution, quality of service access control, etc.

One alternative to the LWAPP approach would be to attempt to map individual information elements found within a wireless protocol frame to a generic protocol data set, and hide the underlying technology from the AC. However, every wireless technology have objects that are very specific and unique, and cannot be easily mapped to a generic information element. Some of these information elements could also be items that the AC would need to have access to in order to make policy decisions. The authors of the LWAPP specification therefore feel that simply tunneling the wireless technology frames to the AC allows for the most flexibility and extensibility.

#### 2.2.2.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.2.3 Support for New IEEE Requirements

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

#### 2.2.3.1 Protocol Evaluation

The LWAPP protocol was designed to be able to accommodate new IEEE extensions defined, and the authors of the specification have been involved in the 802.11 IEEE process for as many as 14 years, have acted in the role of chairs, editors and technical contributors in various task groups. Therefore, we feel that there is significant

expertise in the group to be justify our statement.

One example of extensibility is support for 802.11k. Given that the management frames are tunneled from the WTP to the AC, in order for the AC to support 802.11k, all that is needed is for the WTP to forward the related action frames. The AC may initiate an 802.11k radio measurement simply by sending a tunneled 802.11 management frame to the appropriate station, through its WTP.

Another example of extensibility is the ability to support other wireless technologies. This requirement was addressed in section Section 2.2.2.

That said, the CAPWAP WG and the authors cannot predict all of the future work that will be done by the IEEE. So it is possible that some future extensions will require some additional IETF CAPWAP standardization work. It is therefore necessary to make sure that the WG puts in place a set of guidelines for IANA numbering assignment and a process for protocol extensibility. The authors expect to create an extensive IANA considerations section to the LWAPP spec if it is selected as the basis for the working group.

#### 2.2.3.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.2.4 Interconnection Objective

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

#### 2.2.4.1 Protocol Evaluation

The LWAPP protocol was designed to be able to be transported over any link layer. The current specification defines the use of either Ethernet or UDP/IP as transports (supporting both IPv4 and IPv6). Much of the dependences on transport capabilities have been removed by including support for these within the LWAPP protocol itself (for instance fragmentation/reassembly). As a consequence, it is felt that the protocol is sufficiently flexible to handle a variety of underlying transports, with the understanding that certain guidelines would have to be specified for new transports.

#### 2.2.4.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

#### 2.2.5 Access Control

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

##### 2.2.5.1 Protocol Evaluation

Given the LWAPP protocol requires that the 802.11 MAC management frames be tunneled to the AC, the AC has complete control over the behavior of the network, and can implement certain strategies such as load balancing. Further, as previously described since 802.11e simply builds on top of management frames, these would be sent to the AC, which would then have the ability to perform admission control, etc.

The security considerations section of the LWAPP specification states that an AC SHOULD perform authorization of WTPs prior to allowing them to join. This function is outside the scope of the LWAPP protocol, and could be performed through a function such as RADIUS or LDAP. However, the authors recognize that authorization of WTPs is necessary in order to eliminate the possibility of grey market APs from connecting to the CAPWAP infrastructure.

##### 2.2.5.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.3 Rejected Objectives

#### 2.3.1 Support for Non-CAPWAP WTPs

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

##### 2.3.1.1 Protocol Evaluation

As mentioned in the objectives document, whether an AC is capable of supporting non-CAPWAP WTPs is an implementation issue, and is not required as part of a candidate protocol.

##### 2.3.1.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

#### 2.3.2 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.

#### 2.3.2.1 Protocol Evaluation

Although the working group opted to reject this objective, the authors of the LWAPP specification wish to re-inforce that they believe that any specification adopted by the working group must be sufficiently specified to ensure that any third party WTP is capable of providing 802.11 access to stations in an interoperable manner.

#### 2.3.2.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

### 2.4 Operator Requirements

#### 2.4.1 AP Fast Handoff

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

#### 2.4.1.1 Protocol Evaluation

The authors of the LWAPP specification believe that the protocol as specified is capable of handling fast AP handoffs. The fact that the WTP only needs to tunnel any management frames, as opposed to perform some packet manipulation significantly increases the ability for the WTPs to handle low latency handoffs, especially in the face of network load.

Further, the centralization of the 802.1X function allows for an authenticator to have quick access to information which will could crucial for new initiatives such as the 802.11r fast roaming group.

Using the terminology defined by 802.11r, whereby a handoff starts as of the last packet on the old AP to the first packet on the new AP. Existing LWAPP products shipping in the field are capable of performing this function in less than 30 ms.

#### 2.4.1.2 Compliance

The LWAPP protocol satisfies this CAPWAP objective.

## 3. Compliance Table

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

## 4. Security Considerations

This document simply lists how the LWAPP protocol conforms to the requirements listed in the CAPWAP objectives document. The LWAPP specification has an extensive security considerations section which applies to the protocol itself. There is nothing specific about this document that introduces new security considerations.

## 5. IANA Considerations

This document requires no action by IANA.

## 6. Acknowledgements

The authors would like to thanks Russ Housley and Charles Clancy for their assistance in provide a security review of the LWAPP specification.

## 7. IPR Statement

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

Please refer to http://www.ietf.org/ietf/IPR for more information.

# 8. References

## 8.1 Normative References

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

[2] Govindan, S., "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)", draft-ietf-capwap-objectives-03 (work in progress), June 2005.

[3] 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.

[4] Calhoun, P., "Light Weight Access Point Protocol (LWAPP)", draft-ohara-capwap-lwapp-02 (work in progress), April 2005.

[5] Calhoun, P., "CAPWAP Taxonomy Recommendations", draft-calhoun-capwap-taxonomy-recommendation-00 (work in progress), June 2005.

[6] "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", IEEE Standard 802.11, 1999, <http://standards.ieee.org/getieee802/download/802.11-1999.pdf>.

[7] "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements", IEEE Standard 802.11i, July 2004, <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>.

[8] Clancy, C., "Security Review of the Light Weight Access Point Protocol", May 2005, <http://www.cs.umd.edu/~clancy/docs/lwapp-review.pdf>.

[9] "Wi-Fi Certified for WMM - Support for Multimedia Applications with Quality of Service in WiFi Networks", September 2004, <http://www.weca.net/opensection/pdf/WMM_QoS_whitepaper.pdf>.

[10] "Wi-Fi Protected Access (WPA)", March 2005, <http://www.wi-fi.org/OpenSection/pdf/

Wi-Fi_Protected_Access_Overview.pdf>.

## 8.2 Informational References

Authors' Addresses

Pat R. Calhoun
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134

Phone: +1 408-853-5269
Email: pcalhoun@cisco.com

Bob O'Hara
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134

Phone: +1 408-853-5513
Email: bob.ohara@cisco.com

Sue Hares
Nexthop Technologies, Inc.
825 Victors Way, Suite 100
Ann Arbor, MI 48108

Phone: +1 734 222 1610
Email: shares@nexthop.com

## Intellectual Property Statement



## Disclaimer of Validity



## Copyright Statement



## Acknowledgment

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