

Independent Submission
Request for Comments: 5412
Category: Historic
ISSN: 2070-1721

P. Calhoun
R. Suri
N. Cam-Winget
Cisco Systems, Inc.
M. Williams
GWhiz Arts & Sciences
S. Hares
B. O'Hara
S.Kelly
February 2010

Lightweight Access Point Protocol

Abstract

In recent years, there has been a shift in wireless LAN (WLAN) product architectures from autonomous access points to centralized control of lightweight access points. The general goal has been to move most of the traditional wireless functionality such as access control (user authentication and authorization), mobility, and radio management out of the access point into a centralized controller.

The IETF's CAPWAP (Control and Provisioning of Wireless Access Points) WG has identified that a standards-based protocol is necessary between a wireless Access Controller and Wireless Termination Points (the latter are also commonly referred to as Lightweight Access Points). This specification defines the Lightweight Access Point Protocol (LWAPP), which addresses the CAPWAP's (Control and Provisioning of Wireless Access Points) protocol requirements. Although the LWAPP protocol is designed to be flexible enough to be used for a variety of wireless technologies, this specific document describes the base protocol and an extension that allows it to be used with the IEEE's 802.11 wireless LAN protocol.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for the historical record.

This document defines a Historic Document for the Internet community. This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc5412>.

IESG Note

This RFC documents the LWAPP protocol as it was when submitted to the IETF as a basis for further work in the CAPWAP Working Group, and therefore it may resemble the CAPWAP protocol specification in RFC 5415 as well as other IETF work. This RFC is being published solely for the historical record. The protocol described in this RFC has not been thoroughly reviewed and may contain errors and omissions.

RFC 5415 documents the standards track solution for the CAPWAP Working Group and obsoletes any and all mechanisms defined in this RFC. This RFC is not a candidate for any level of Internet Standard and should not be used as a basis for any sort of Internet deployment.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction	8
1.1. Conventions Used in This Document	9
2. Protocol Overview	10
2.1. Wireless Binding Definition	11
2.2. LWAPP State Machine Definition	12
3. LWAPP Transport Layers	20
3.1. LWAPP Transport Header	21
3.1.1. VER Field	21
3.1.2. RID Field	21
3.1.3. C Bit	21
3.1.4. F Bit	21
3.1.5. L Bit	22
3.1.6. Fragment ID	22
3.1.7. Length	22
3.1.8. Status and WLANS	22
3.1.9. Payload	22
3.2. Using IEEE 802.3 MAC as LWAPP Transport	22
3.2.1. Framing	23
3.2.2. AC Discovery	23
3.2.3. LWAPP Message Header Format over IEEE 802.3 MAC Transport	23
3.2.4. Fragmentation/Reassembly	24
3.2.5. Multiplexing	24
3.3. Using IP/UDP as LWAPP Transport	24
3.3.1. Framing	24
3.3.2. AC Discovery	25
3.3.3. LWAPP Message Header Format over IP/UDP Transport ..	25
3.3.4. Fragmentation/Reassembly for IPv4	26
3.3.5. Fragmentation/Reassembly for IPv6	26
3.3.6. Multiplexing	26
4. LWAPP Packet Definitions	26
4.1. LWAPP Data Messages	27
4.2. LWAPP Control Messages Overview	27
4.2.1. Control Message Format	28
4.2.2. Message Element Format	29
4.2.3. Quality of Service	31
5. LWAPP Discovery Operations	31
5.1. Discovery Request	31
5.1.1. Discovery Type	32
5.1.2. WTP Descriptor	33
5.1.3. WTP Radio Information	34
5.2. Discovery Response	34
5.2.1. AC Address	35
5.2.2. AC Descriptor	35
5.2.3. AC Name	36
5.2.4. WTP Manager Control IPv4 Address	37

5.2.5.	WTP Manager Control IPv6 Address	37
5.3.	Primary Discovery Request	38
5.3.1.	Discovery Type	38
5.3.2.	WTP Descriptor	38
5.3.3.	WTP Radio Information	38
5.4.	Primary Discovery Response	38
5.4.1.	AC Descriptor	39
5.4.2.	AC Name	39
5.4.3.	WTP Manager Control IPv4 Address	39
5.4.4.	WTP Manager Control IPv6 Address	39
6.	Control Channel Management	39
6.1.	Join Request	39
6.1.1.	WTP Descriptor	40
6.1.2.	AC Address	40
6.1.3.	WTP Name	40
6.1.4.	Location Data	41
6.1.5.	WTP Radio Information	41
6.1.6.	Certificate	41
6.1.7.	Session ID	42
6.1.8.	Test	42
6.1.9.	XNonce	42
6.2.	Join Response	43
6.2.1.	Result Code	44
6.2.2.	Status	44
6.2.3.	Certificate	45
6.2.4.	WTP Manager Data IPv4 Address	45
6.2.5.	WTP Manager Data IPv6 Address	45
6.2.6.	AC IPv4 List	46
6.2.7.	AC IPv6 List	46
6.2.8.	ANonce	47
6.2.9.	PSK-MIC	48
6.3.	Join ACK	48
6.3.1.	Session ID	49
6.3.2.	WNonce	49
6.3.3.	PSK-MIC	49
6.4.	Join Confirm	49
6.4.1.	Session ID	50
6.4.2.	PSK-MIC	50
6.5.	Echo Request	50
6.6.	Echo Response	50
6.7.	Key Update Request	51
6.7.1.	Session ID	51
6.7.2.	XNonce	51
6.8.	Key Update Response	51
6.8.1.	Session ID	51
6.8.2.	ANonce	51
6.8.3.	PSK-MIC	52
6.9.	Key Update ACK	52

6.9.1.	WNonce	52
6.9.2.	PSK-MIC	52
6.10.	Key Update Confirm	52
6.10.1.	PSK-MIC	52
6.11.	Key Update Trigger	52
6.11.1.	Session ID	53
7.	WTP Configuration Management	53
7.1.	Configuration Consistency	53
7.2.	Configure Request	54
7.2.1.	Administrative State	54
7.2.2.	AC Name	55
7.2.3.	AC Name with Index	55
7.2.4.	WTP Board Data	56
7.2.5.	Statistics Timer	56
7.2.6.	WTP Static IP Address Information	57
7.2.7.	WTP Reboot Statistics	58
7.3.	Configure Response	58
7.3.1.	Decryption Error Report Period	59
7.3.2.	Change State Event	59
7.3.3.	LWAPP Timers	60
7.3.4.	AC IPv4 List	60
7.3.5.	AC IPv6 List	61
7.3.6.	WTP Fallback	61
7.3.7.	Idle Timeout	61
7.4.	Configuration Update Request	62
7.4.1.	WTP Name	62
7.4.2.	Change State Event	62
7.4.3.	Administrative State	62
7.4.4.	Statistics Timer	62
7.4.5.	Location Data	62
7.4.6.	Decryption Error Report Period	62
7.4.7.	AC IPv4 List	62
7.4.8.	AC IPv6 List	62
7.4.9.	Add Blacklist Entry	63
7.4.10.	Delete Blacklist Entry	63
7.4.11.	Add Static Blacklist Entry	64
7.4.12.	Delete Static Blacklist Entry	64
7.4.13.	LWAPP Timers	65
7.4.14.	AC Name with Index	65
7.4.15.	WTP Fallback	65
7.4.16.	Idle Timeout	65
7.5.	Configuration Update Response	65
7.5.1.	Result Code	65
7.6.	Change State Event Request	65
7.6.1.	Change State Event	66
7.7.	Change State Event Response	66
7.8.	Clear Config Indication	66
8.	Device Management Operations	66

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.