Operations Group
Internet Draft
Expires: December 2005

I. Singh
P. Francisco
M. Montemurro
Chantry Networks
June 2005

Evaluation of CAPWAP Tunneling Protocol (CTP)
draft-francisco-capwap-ctp-evaluation-01.txt

Status of this Memo

Copyright Notice

Abstract

This document presents a self evaluation of the CAPWAP Tunneling Protocol (CTP) with respect to the requirements presented in the CAPWAP Objectives draft. This work is to aid in the official working group evaluation of the candidate protocols for CAPWAP.

Table of Contents

1. Definitions

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. Introduction

The authors of the CAPWAP Tunneling Protocol(CTP) [2] believe that CTP provides a robust solution in the form of a protocol that addresses the issues raised in the CAPWAP Problem Statement draft [3]. CTP can be run over an L2 or an L3 network and it is extensible to support WTPs which terminate other radio technologies than IEEE 802.11.

Given below is a brief analysis of the protocol with respect to the objectives draft [4] that has been presented and discussed in the WG.

3. Objectives Responses

3.1 Mandatory and Accepted Objectives

3.1.1 Logical Groups

The ability to control and manage physical WTPs in terms of logical groups.

3.1.1.1 Protocol Evaluation

The CTP protocol allows the AP and WTP to exchange information on logical groups as part of the capabilities exchange (CTP_CAP_REQ/RESP). The AC uses this information to provision logical groups on the WTP as part of the configuration transaction.
The CTP header in the control and data messages provides a mechanism to segment traffic between logical groups.

3.1.1.2 Compliance

CTP is compliant with this objective.

3.1.2 Support for Traffic Separation

This objective pertains to the need to maintain separation of control and data traffic in the operation of the protocol.

3.1.2.1

Protocol Evaluation

CTP provides specific message types control and data traffic. CTP data traffic can either be tunneled to the AC or bridged locally at the WTP. Control traffic will always travel between the AC and the WTP.

3.1.2.2
Compliance
CTP is compliant with this objective.

3.1.3
Wireless Terminal Transparency
This objective specifies the need for the protocol to be client agnostic. That is, the wireless terminals need not be aware of the existence of the CAPWAP protocol running underneath.

3.1.3.1
Protocol Evaluation
CTP defines a protocol for the provisioning and control of WTPs. The protocol is agnostic to wireless MAC technology and entirely transparent to a wireless terminal. Shipping products using CTP demonstrate that this protocol does not have any adverse effects, interoperability or otherwise, on the wireless terminals.

3.1.3.2
Compliance
CTP is compliant with this objective.

3.1.4
Configuration Consistency
This objectives pertains to the protocolÆs ability to provide consistent configuration state information of the WTPs at the AC.

3.1.4.1
Protocol Evaluation
CTP defines a configuration transaction where the AC can exchange configuration with the WTP. The mechanism uses an SNMP data payload encapsulated inside a CTP frame. The WTP must acknowledge the configuration update to confirm that the configuration state on the WTP is synchronized with the AC.

The protocol makes use of the SNMP MIB that is defined in the IEEE 802.11 standard and its amendments. This provides a generic mechanism for configuration which is agnostic to wireless technologies and updates to wireless standards.

3.1.4.2
Compliance
CTP is compliant with this objective.

3.1.5
Firmware Trigger
This objective states that the protocol must have the ability to trigger WTP firmware updates. It does not necessarily state the need for the protocol to integrate a software update mechanism within the

protocol itself.

3.1.5.1 Protocol Evaluation

After the device capability exchange phase (CTP-CAP_REQ/RESP) which allows for the identification of the type of WTP connecting, CTP protocol specifies a phase of firmware image validation (CTP-Software-upgrade-req/resp, section 5.1.5) where the WTP indicates the

version of its firmware to the Controller. The controller can evaluate the version of the WTP software and signal the WTP to update its image. CTP does not specify the actual method for firmware upgrade, but rather assumes the application of standardized binary transport protocols (FTP/TFTP).

3.1.5.2 Compliance

CTP is compliant with this objective.

3.1.6 Monitoring and Exchange of System-wide Resource State

This objective states that the protocol must incorporate the ability for the WTP to send statistics, congestion indications and other pertinent wireless state information to the AC.

3.1.6.1 Protocol Evaluation

CTP protocol defines frames for the periodic exchange of a WTPÆs operational statistics (CTP-Stats-req/resp, CTP-Stats-Notify, Section 5.2.7-9). The protocol uses an SNMP format for the statistics based on MIB definitions from the 802.11 standard and its amendments. This protocol mechanism is agnostic to wireless technology and updates to existing wireless standards.

3.1.6.2 Compliance

CTP is compliant with this objective.

3.1.7 Resource Control Objective

This objective pertains to the ability of the protocol to provide a mapping mechanism of the IEEE 802.11e QOS priorities across the wireless and wired infrastructure.

3.1.7.1 Protocol Evaluation

CTP defines a two tiered mechanism for QoS that addresses the switching segment as well as the wireless medium. The QoS strategy for the protocol involves mapping the QoS marking of the data frame to the CTP frame.

Across the switched segment, CTP is an IP protocol that provides several mechanisms to ensure the preservation of QoS markers within the original data packet. The protocol header (CTP Section 4.1) natively defines an 8-bit field for relaying of QoS policy related information in a transport independent manner. Alternatively, CTP could use 802.1p tagging to preserve QoS across the switched segment.

This allows the WTP and Controller to classify and guarantee the preservation of QoS across the switched network.

CTP makes use of the 802.11e standard to preserve QoS across the wireless medium. The mapping for QoS data frames to 802.11e QoS frames is defined in the 802.11e amendment to the 802.11 standard.

3.1.7.2
Compliance
CTP is compliant with this objective.

3.1.8
CAPWAP Protocol Security
This objective concerns the security of the CAPWAP protocol. The protocol must support mutual authentication of the WTP and the AC and the communication channel between the two entities must be secured. In addition, however, the protocol must not preclude the possibility of supporting asymmetric authentication mechanisms.

3.1.8.1
Protocol Evaluation
First of all, as currently defined, CTP does not support a pre-shared key mechanism for mutual authentication. It assumes the existence of digital certificates on the WTP and AC. The mutual authentication mechanism between WTP and AC using digital certificates as described in the CTP draft is very similar to the method employed in the LWAPP draft [5]. As such, some of the recent comments on the WG email list regarding the security of LWAPPÆs mutual authentication also applies to CTP. Specifically in the area of the generation of the encryption key. Currently CTP specifies that the encryption key is generated by the AC and is securely transported to the WTP. An obvious improvement would be for the WTP and the AC to mutually contribute to the generation of the encryption key by providing independently generated random material for the session keys.

Also, based on discussion on the WG list it is not clear whether the use of pre-shared key for mutual authentication is required or simply that the authentication must be mutual. Nevertheless, we believe that adding another method of mutual authentication, ie. with using pre-shared keys, will enhance the flexibility of the CTP protocol, but at the cost of increased protocol complexity.

3.1.8.2
Compliance
CTP is partially compliant with this objective.

3.1.9
System-wide Security
The protocol must not adversely affect the security of the wireless and wired networks on which it runs.

3.1.9.1
Protocol Evaluation
CTP defines that any exchanges of control based material such as PMK

is natively encrypted. All Control messages are mutually encrypted between the WTP and controller. In lieu of a thorough security and cryptographic analysis of the protocol by peers, the authors believe that the encryption/keying mechanism currently provides adequate protection against un-authorized compromise of the transported information which, in turn, would not adversely affect the security of the wireless or wired network.

3.1.9.2

Compliance

The protocol is partially compliant with this objective pending a thorough security and cryptographic review.

3.1.10

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.

3.1.10.1

Protocol Evaluation

The CTP protocol has separated the 802.11i security function into two components, EAP Authenticator and Key Management. The EAP Authenticator and Key Management functions provide a natural delineation point between 802.11i functions. The location of the components is negotiated between the AC and WTP during the capabilities exchange and registration. The components can either co-located or separate on the WTP or the AC. Any exchange of security association information between the AC and the WTP is protected either by 802.11i mechanisms or by CTP mechanisms.

3.1.10.2

Compliance

CTP is compliant with this objective.

3.1.11

Interoperability Objective

The objective specifies that the protocol must include a capabilities exchange mechanism so that different types of WTPs can be managed by ACs. That is, local-MAC and split-MAC WTPs may be recognized by the AC through protocol exchange and appropriate handling within the protocol would ensue as a result of this capability exchange.

3.1.11.1

Protocol Evaluation

The CTP protocol as specified, provides a mechanism for capabilities exchange (CTP-caps-req/resp) that allows the WTP and the Controller to negotiate their operational mode. The capabilities exchange for

control and data traffic is treated independently.

Control traffic in split-MAC mode indicates that the WTP will forward all wireless MAC management traffic (i.e. IEEE 802.11) to the AC.

Control traffic in local-MAC mode indicates that all 802.11 management frames will terminate at the WTP. CTP defines update messages to allow the WTP to signal the AC for updates to wireless client connection states.

Data traffic in split-MAC modes indicates that the WTP will forward all traffic to the AC. The format for the traffic can be either wireless MAC dependent (i.e. IEEE 802.11) or IEEE 802.3 depending whether the control channel is split-MAC or local-MAC.

Data traffic in local-MAC mode indicates that data frames will be bridged locally by the AP to its switching segment. The switching segment may be present locally at the AP or at the Controller. For Controller handled bridged access the CTP protocol provides a tunneling method for 802.3 frame encapsulation.

3.1.11.2

Compliance

CTP is compliant with this objective.

3.1.12

Protocol Specifications

This objective states that any vendor of a WTP or AC or any person may implement the CAPWAP protocol and that all such implementations should interoperate.

3.1.12.1

Protocol Evaluation

CTP specification fully specify the protocol and its operation within WTPs and ACs. It also indicates the configuration and statistics capabilities come from MIB specifications that are published by IEEE that fully describe the managed objects within an WTP. The authors believe that the work done by the IEEE will enable full interoperability as the specifications coming from IEEE will be complete and not require any knowledge of any vendor specific wireless device information.

3.1.12.2

Compliance

CTP is compliant with this objective.

3.1.13

Vendor Independence

This objective states that the CAPWAP protocol must not be reliant on any underlying vendor implementation of hardware of either the WTP or the AC.

3.1.13.1

Protocol Evaluation

CTP does not assume any underlying hardware architecture of the WTPs or the ACs. In addition any dependency on MIB definitions in its current form also does not assume any reliance on hardware specifications.

3.1.13.2
Compliance

CTP is compliant with this objective.

3.1.14
Vendor Flexibility
The protocol must not be bound to any specific MAC.

3.1.14.1
Protocol Evaluation
CTP has been completely implemented on hardware from at least two different vendors whose wireless MAC implementations are completely independent. Given this fact as well as CTPÆs inherent agnosticity of wireless implementation, CTP can be implemented without knowledge of underlying vendor hardware.

3.1.14.2
Compliance
CTP is compliant with this objective.

3.1.15
NAT Traversal
The protocol must not prevent operation across WLAN topologies which include NAT segments.

3.1.15.1
Protocol Evaluation
CTP provides an authentication mechanism which uses AC and WTP identifiers to establish a secure connection without a dependency on MAC or IP address. The CTP protocol is primarily transported as UDP payload. Typical NAT implementations are IP and TCP/UDP port based. Since CTP is transported above these layers, CTP will work properly through NAT devices. The WTP can be statically configured to discover the AC through a NAT segment.

3.1.15.2
Compliance
CTP is compliant with this objective.

3.2
Desirable Objectives

3.2.1
Multiple Authentication Mechanisms
This objective specifies the requirement that the protocol should be able to support authentication mechanisms other than IEEE 802.11i.

3.2.1.1
Protocol Evaluation
Since CTP is wireless terminal agnostic, and since the PMK key

exchange is generic (for example, does not assume any authentication mechanism in the form of an EAP type), CTP does not prevent the operation of any other authentication mechanisms.

CTP logically separates the EAP-Authentication function from the Key Management function. Different authentication or key management frameworks can be substituted without affecting the protocol behavior.

3.2.1.2
Compliance
CTP is compliant with this objective.

3.2.2
Support for Future Wireless Technologies
This objective states that the protocol should be able to be extended to future layer 2 wireless technologies and should not be limited to only supporting IEEE 802.11.

3.2.2.1
Protocol Evaluation
The current specification lists alternative layer 2 wireless technologies that and be indicated as part of the capabilities exchange phase. The protocol is sufficiently modular in that the configuration, statistics and other management functions of these wireless devices can be supported. If indeed there are layer 2 wireless specific elements that need to be added, those are easily supported by extensions to the protocol.

3.2.2.2
Compliance
CTP is compliant with this objective.

3.2.3
Support for New IEEE Requirements
The protocol must be able to accommodate defined changes or extensions to the IEEE 802.11 specifications.

3.2.3.1
Protocol Evaluation
CTP provides an abstraction layer to accommodate any type of wireless MAC technology. It provides control messages to exchange basic state information between the AC and the WTP. It provides a split MAC mechanism where all MAC frames can be forwarded and handled at the controller. It uses SNMP-based encapsulation to provide a generic mechanism for exchanging configuration and statistics data . New 802.11 amendments can be easily accommodated by the protocol. There will be work required to interpret the impact of the amendment on both the AC and the WTP to determine whether further message definition is required.

3.2.3.2
Compliance
CTP is compliant with this objective.

3.2.4
Interconnection Objective

The CAPWAP protocol must not be constrained by the underlying transport technologies of the wired medium.

3.2.4.1

Protocol Evaluation

CTP is agnostic to the underlying transport technology as it is implemented as UDP. This was done with the assumption that the transport technology can carry IP packets across its medium either L2 or L3 network. In itÆs current definition CTP is transported as UDP payload therefore directly abstracted from IPv4/v6 base.

3.2.4.2
Compliance
CTP is compliant with this objective in terms of not having specified IPv6 header types.

3.2.5
Access Control
This objective pertains to the ability of the protocol to exchange information required for access control of WTPs and wireless terminals.

3.2.5.1
Protocol Evaluation
CTP provides specific messages, e.g. CTP-MU-Connect/Disconnect/Authenticate messages, that control the access of wireless terminals. In addition to the actual mutual authentication of WTPs and ACs, the registration phase contains a AP-ID field that needs to be verified by the AC. This field needs to be checked by the AC and the mechanism for this check is not within the scope of any CAPWAP work. However, the CTP protocol itself provides this identification token as a means of access control of the WTP.

3.2.5.2
Compliance
CTP is compliant with this objective.

3.3
Non-objectives

The current objectives draft states this section as ôRejected Objectivesö. We have used the term ôNon-Objectivesö for this section based on the discussion on the WG email list.

3.3.1
Support for Non-CAPWAP WTPs
This objective states that the CAPWAP protocol should be capable of recognizing legacy WTPs and existing network management systems.

3.3.1.1
Protocol Evaluation
This requirement is more of a feature for centralized WLAN network applications and thus does not apply to the CAPWAP problem statement.

3.3.1.2
Compliance
CTP is compliant with this objective.

3.3.2

Technical Specifications

This objective states that WTP vendors should not have to share technical specifications for hardware and software to AC vendors in order for interoperability to be achieved.

3.3.2.1

Protocol Evaluation

As discussed earlier, CTP is hardware and vendor agnostic.

3.3.2.2

Compliance

CTP is compliant with this objective.

3.4 Operator Requirements

3.4.1 AP Fast Handoff

This objective states that the CAPWAP protocol operations must not impede or obstruct the efficiency of fast handoff procedures.

3.4.1.1 Protocol Evaluation

In the CTP protocol, the signaling of roaming events are efficiently encoded in the CTP-MU messages. Also, the 802.1x messaging is centralized allowing efficient use of CPU resources at the AC. In effect, the mere existence of the centralized architecture ensures that the efficiency of fast handoffs is improved rather than impeded.

3.4.1.2 Compliance

CTP complies with this objective.

4. Compliance Table

Given below is a table summarizing the compliance to the objectives. C = Compliant, P = Partially compliant, N = Non-compliant.

Objective Type	Compliance
Logical Groups	C
Support for Traffic Separation	C
Wireless Terminal Transparency	C
Configuration Consistency	C
Firmware Trigger	C
Monitoring & Exchange of System-wide Resource State	C
Resource Control Objective	C
CAPWAP Protocol Security	P
System-wide Security	C
IEEE 802.11i Considerations	C
Interoperability Objective	C
Protocol Specifications	C
Vendor Independence	C
Vendor Flexibility	C
NAT Traversal	C
Multiple Authentication Mechanisms	C
Support for Future Wireless Technologies	C

Support for New IEEE Requirements	C
Interconnection Objective	C
Access Control	C
Support for Non-CAPWAP WTPs	C
Technical Specifications	C
AP Fast Handoff	C

+---+------------+

5. Security considerations

This document provides a self evaluation of CTP in respect to the CAPWAP objectives. The CTP draft itself has a section that catalogues all the pertinent security concerns. Therefore, in this draft there are no new security considerations to be discussed.

6. References

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

[2] Singh, I., et. al., ôCAPWAP Tunneling Protocolö, draft-singh-capwap-ctp-01.txt (work in progress), April 2005.

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

[4] Govindan, S., et. al., ôObjectives for Control and Provisioning of Wireless Access Points (CAPWAP)ö, draft-ietf-capwap-objectives-02.txt (work in progress), April 2005

[5] Calhoun, et. al., ôLight Weight Access Point Protocol (LWAPP)ö, draft-ohara-capwap-lwapp-02.txt (work in progress), April 2005

7. Author's Addresses

Paulo Francisco
Chantry Networks Inc.
1900 Minnesota Court
Mississauga, ON L5N 3C9
Canada

Phone: +1 905-363-6410
Email: paulo.francisco@siemens.com

Inderpreet Singh
Chantry Networks Inc.
1900 Minnesota Court
Mississauga, ON L5N 3C9

Canada

Phone: +1 905-363-6412
Email: inderpreet.singh@siemens.com

Michael Montemurro
Chantry Networks Inc.
1900 Minnesota Court
Mississauga, ON L5N 3C9
Canada

Phone: +1 905-363-6413
Email: michael.montemurro@siemens.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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