

Operations Group  
Internet Draft  
Document: [draft-singh-capwap-ctp-01.txt](#)

I. Singh  
P. Francisco  
K. Pakulski  
Chantry Networks  
F. Backes  
AutoCell Laboratories  
April 2005

Expires: October 2005

## **CAPWAP Tunneling Protocol (CTP)**

### Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 3 of RFC3667](#). By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with [RFC 3668](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on October 4, 2005.

### Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

### Abstract

With the overwhelming choice of proprietary implementations of centralized control and management of wireless access points and access controllers there is a great demand for a standard protocol



and architecture that enables the deployment of large scale wireless networks.

This document describes the CAPWAP Tunneling Protocol, a protocol that allows for the centralized control and provisioning of a large number of wireless access points from access controllers. It is supported by an architecture where the MAC layer of the RF technology is terminated within the AP. This allows for the protocol to be extensible to multiple radio technologies. It assumes an IP connection between the access points and access controllers and has signaling primitives to enable wireless station mobility between access points. Therefore, seamless Layer 3 subnet mobility is seamlessly enabled by this protocol.

## Table of Contents

<a href="#">1.</a>	<a href="#">Definitions.....</a>	<a href="#">4</a>
<a href="#">1.1</a>	<a href="#">Conventions used in this document.....</a>	<a href="#">4</a>
<a href="#">1.2</a>	<a href="#">Terminology.....</a>	<a href="#">4</a>
<a href="#">2.</a>	<a href="#">Introduction.....</a>	<a href="#">4</a>
<a href="#">2.1</a>	<a href="#">Out of scope.....</a>	<a href="#">6</a>
<a href="#">2.1.1</a>	<a href="#">Secure discovery of AP and AC.....</a>	<a href="#">6</a>
<a href="#">2.1.2</a>	<a href="#">AP image management.....</a>	<a href="#">6</a>
<a href="#">2.1.3</a>	<a href="#">Multiple AC mobility.....</a>	<a href="#">7</a>
<a href="#">3.</a>	<a href="#">Protocol Overview.....</a>	<a href="#">7</a>
<a href="#">3.1</a>	<a href="#">Control and Status Messages.....</a>	<a href="#">7</a>
<a href="#">3.2</a>	<a href="#">Configuration and Statistics messages.....</a>	<a href="#">7</a>
<a href="#">3.3</a>	<a href="#">Data Messages.....</a>	<a href="#">8</a>
<a href="#">4.</a>	<a href="#">CTP Packets.....</a>	<a href="#">8</a>
<a href="#">4.1</a>	<a href="#">CTP Header format.....</a>	<a href="#">8</a>
<a href="#">4.2</a>	<a href="#">Messages.....</a>	<a href="#">9</a>
<a href="#">4.3</a>	<a href="#">Message Payloads.....</a>	<a href="#">10</a>
<a href="#">5.</a>	<a href="#">Message descriptions.....</a>	<a href="#">13</a>
<a href="#">5.1</a>	<a href="#">Message State Control.....</a>	<a href="#">13</a>
<a href="#">5.2</a>	<a href="#">Control and Status messages.....</a>	<a href="#">13</a>
<a href="#">5.2.1</a>	<a href="#">CTP_Reg-Req.....</a>	<a href="#">13</a>
<a href="#">5.2.2</a>	<a href="#">CTP_Reg-Rsp.....</a>	<a href="#">14</a>
<a href="#">5.2.3</a>	<a href="#">CTP_Auth-Req.....</a>	<a href="#">14</a>
<a href="#">5.2.4</a>	<a href="#">CTP_Auth-Rsp.....</a>	<a href="#">15</a>
<a href="#">5.2.5</a>	<a href="#">CTP_SW-Update-Req.....</a>	<a href="#">15</a>
<a href="#">5.2.6</a>	<a href="#">CTP_SW-Update-Rsp.....</a>	<a href="#">16</a>
<a href="#">5.2.7</a>	<a href="#">CTP_Set-State-Req.....</a>	<a href="#">16</a>
<a href="#">5.2.8</a>	<a href="#">CTP_Set-State-Rsp.....</a>	<a href="#">17</a>
<a href="#">5.2.9</a>	<a href="#">CTP_Poll-Req.....</a>	<a href="#">17</a>
<a href="#">5.2.10</a>	<a href="#">CTP_Poll-Rsp.....</a>	<a href="#">18</a>
<a href="#">5.2.11</a>	<a href="#">CTP_MU-Connect-Req.....</a>	<a href="#">18</a>
<a href="#">5.2.12</a>	<a href="#">CTP_MU-Connect-Rsp.....</a>	<a href="#">18</a>

[5.2.13](#) CTP\_MU-Disconnect-Req.....[19](#)

<a href="#">5.2.14</a>	<a href="#">CTP_MU-Disconnect-Rsp</a>	<a href="#">19</a>
<a href="#">5.2.15</a>	<a href="#">CTP_MU-Disconnect-Nfy</a>	<a href="#">20</a>
<a href="#">5.2.16</a>	<a href="#">CTP MU-Authenticate-Req</a>	<a href="#">20</a>
<a href="#">5.2.17</a>	<a href="#">CTP MU-Authenticate-Rsp</a>	<a href="#">20</a>
<a href="#">5.3</a>	<a href="#">Configuration and Statistics messages</a>	<a href="#">21</a>
<a href="#">5.3.1</a>	<a href="#">CTP Cap-Req</a>	<a href="#">21</a>
<a href="#">5.3.2</a>	<a href="#">CTP Cap-Rsp</a>	<a href="#">24</a>
<a href="#">5.3.3</a>	<a href="#">CTP Config-Req</a>	<a href="#">25</a>
<a href="#">5.3.4</a>	<a href="#">CTP Config-Rsp</a>	<a href="#">25</a>
<a href="#">5.3.5</a>	<a href="#">CTP Config-Ack</a>	<a href="#">25</a>
<a href="#">5.3.6</a>	<a href="#">CTP_Config-Status-Notify</a>	<a href="#">26</a>
<a href="#">5.3.7</a>	<a href="#">CTP_Stats-Notify</a>	<a href="#">26</a>
<a href="#">5.3.8</a>	<a href="#">CTP Stats-Req</a>	<a href="#">26</a>
<a href="#">5.3.9</a>	<a href="#">CTP Stats-Rsp</a>	<a href="#">27</a>
<a href="#">5.3.10</a>	<a href="#">Configuration and Statistics</a>	<a href="#">27</a>
<a href="#">5.4</a>	<a href="#">CTP_Data Messages</a>	<a href="#">27</a>
<a href="#">5.4.1</a>	<a href="#">CTP_Data</a>	<a href="#">28</a>
<a href="#">6</a>	<a href="#">State Machines</a>	<a href="#">29</a>
<a href="#">6.1</a>	<a href="#">Init</a>	<a href="#">29</a>
<a href="#">6.2</a>	<a href="#">Control Channel Establishment</a>	<a href="#">29</a>
<a href="#">6.3</a>	<a href="#">Active State</a>	<a href="#">30</a>
<a href="#">6.4</a>	<a href="#">Standby State</a>	<a href="#">30</a>
<a href="#">7</a>	<a href="#">Authentication, Encryption and Session Key generation</a>	<a href="#">30</a>
<a href="#">7.1</a>	<a href="#">Authentication</a>	<a href="#">30</a>
<a href="#">7.2</a>	<a href="#">Encryption</a>	<a href="#">33</a>
<a href="#">7.3</a>	<a href="#">Session Key refresh and generation</a>	<a href="#">35</a>
<a href="#">8</a>	<a href="#">Security considerations</a>	<a href="#">36</a>
<a href="#">9</a>	<a href="#">References</a>	<a href="#">36</a>
<a href="#">10</a>	<a href="#">Author's Addresses</a>	<a href="#">37</a>
	<a href="#">Intellectual Property and Copyright Statements</a>	<a href="#">37</a>



## **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]

### **1.2 Terminology**

AP ; Access Point - The network device that includes both the wireless termination point as well as the implementation of a specific radio technology management layer.

AC - Access Controller - A centralized network entity that controls, configures and manages one or more than one APs.

MU - Mobile Unit - A wireless device which is also an IP node capable of dynamic change in its association with an Access Point.

## **2. Introduction**

The rapid pace with which wireless networks are being deployed in the home, enterprise and carrier industries has led to the proliferation of proprietary solutions which attempt to address problems associated with large scale wireless installations. The main issues plaguing 802.11 wireless networks, for example, are described in [2] and can be summarized as: the manageability of large numbers of APs (Access Points); the secure and bulk provisioning, monitoring, and control of APs; and policy control and enforcement of MU (Mobile Units) data flows and policies.

One of the key problems with deploying large scale wireless networks is that the infrastructure needs to scale to meet both geographic coverage as well as client density requirements. CAPWAP Tunneling Protocol (CTP) addresses these challenges by minimizing configuration of the wired infrastructure to accommodate the wireless network.

CTP provides both centralized configuration and operational control for wireless networks, and in doing so, provides centralized security and policy management.

This solution has been currently focused towards 802.11 networks. However, CTP is independent of the layer 2 wireless standard because it assumes that the MAC layer of the wireless technology is fully implemented in the AP. The control channel binding between the AP and AC provides for all the necessary signaling to facilitate MU connection, mobility, and even RF resource management. Thus, it is





possible to use CTP to offer IP network services to wireless users independent of the underlying wireless technology (e.g. 802.11, 802.15, or 802.16).

CTP involves one or more Access Points (APs) connected to one or more Access Controllers (ACs). The network connectivity between the APs and ACs is primarily through a Layer 3 routed network. However, switched Layer 2 or directly connected network topologies are also supported. Figure 1 shows the typical network topology of AP and AC placement in a CTP network. However, since it is assumed that the AP and AC are IP addressable direct connect or L2 connect is also supported.

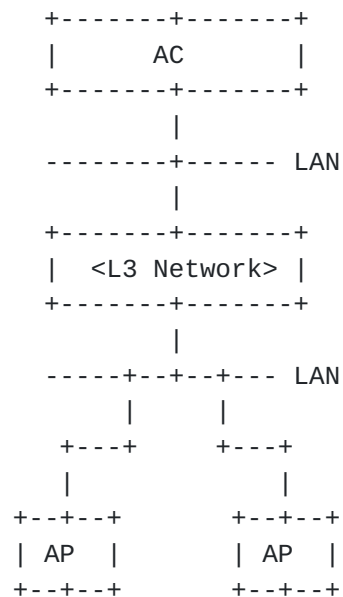


Figure 1 - Topology of AP and AC placement

CTP interacts directly with the MAC management entity to monitor and control configuration and wireless connections. CTP tunnels data traffic as 802.3 traffic to the AP and uses the L2 Bridge to pass data to the MAC. Optionally, data traffic can be passed directly to the AP, independent of a CTP data connection. This mode of operation is fully controlled by the AC rather than being an inherent property of the AP. There has been wide interest in this deployment model in the case where the link between the AC and the AP is a slow WAN link, for example. By bridging the MU data traffic locally at the AP's network, and still controlling the authentication centrally via the AC, the user is able to forgo the possibility of the data traffic having to traverse the slow WAN link upstream and then again downstream to access, for example, a local printer. In this



centralized architecture solution of CTP, the layer 2 wireless termination point and the MAC layer are fully implemented in the AP as shown in Figure 2, which enables this type of feature.

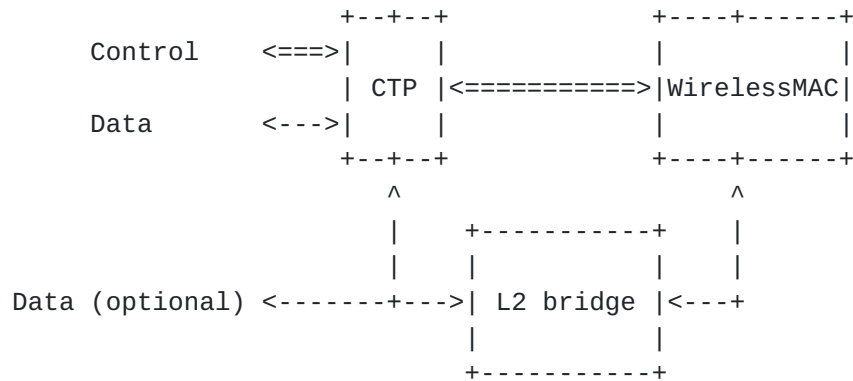


Figure 2 - CTP and MAC interaction in an AP

## 2.1 Out of scope

The following areas are out of scope for this version of the protocol.

### 2.1.1 Secure discovery of AP and AC.

Rather than specify a brand new secure discovery mechanism for APs and ACs within this protocol, CTP specifies the context and security credentials that are required to register APs into ACs. All AP implementations of CTP MUST provide a method to statically configure the IP address(es) of the AC to be stored in the non-volatile RAM of the AP.

Other methods for automatic discovery that MAY be used by implementations of CTP are: SLP, DNS name resolution, and DHCP options for AC IP address(es). The mechanism by which these methods are incorporated into CTP is out of scope for this document but is a worthwhile task for the working group that takes on this work.

### 2.1.2 AP image management.

A conscious decision in the design of this protocol excluded the implementation of an AP image management system. However, CTP provides triggers for software upgrade, ie. a message to indicate software version and a message to command the AP to initiate software upgrade. The actual protocol and mechanism for secure software download has been deemed out of scope for the protocol and beyond what the protocol was intended for.



### **2.1.3 Multiple AC mobility**

This version of CTP does not include the details of support for multi-AC control over APs for the purposes of multi-AC MU mobility. However, the reserved message types and the capability exchange phase may be used to facilitate the setting up of intra-AC tunnels.

## **3. Protocol Overview**

CTP is a generic protocol that defines a mechanism for the control and provisioning of wireless APs through centralized ACs. In addition, it provides a mechanism to optionally tunnel the mobile client data between the AP and AC.

There are two types of CTP packet headers:

- a) Control: these messages allow the AC to provision and control the APs and MU session state and further contain messages that consist of configuration, statistics and state management.
- b) Data: an optional aspect of the protocol that allows MU data packets tunneled between the AP and the AC.

The CTP messages between APs and ACs are delivered by a UDP transport and the UDP port number is [TBD]. The message types of this protocol are classified into three distinct categories:

- o Control and Status messages
- o Configuration and Statistics messages
- o Data messages.

### **3.1 Control and Status Messages**

The set of control messages of CTP provides a mechanism for an AP to register itself with the AC and to interact with the MU session management operations of the AC. Primarily this set is utilized by the AP to request session association with the AC, configuration information, and to provide the mechanism and notification of MU connection to the AC. The AC uses this message set to acknowledge AP and MU session establishment and to explicitly control both AP and MU session operational state (such as AP state changes, AP and MU session disconnection, etc.)

### **3.2 Configuration and Statistics messages**

This logical set of messages exchanged between AP and AC is primarily intended for the provisioning of the AP via a capabilities exchange and configuration message set. This message set also includes a means for the AP to provide periodic status notifications of current



operational state, statistics information such as wireless and wired statistics, security alerts, etc.

### 3.3 Data Messages

The CTP-Data message is the only message in this set. Its purpose is to carry encapsulated frames associated with a registered MU. This message type utilizes the Policy field of the message header to provide user based, post authentication policy enforcement on a per packet basis. This message type applies to actual MU client data and does not include MU association, authentication and MU session management messages as those operations are explicitly represented through specific control messages.

It must be noted that the protocol allows for the data path to not have to traverse the AC. In that case, no policy can be applied on a per user basis centrally.

## 4. CTP Packets

It is assumed that the AP and AC source and destination information is available in the transport layer headers. As such, it is not indicated below.

### 4.1 CTP Header format

Figure 3 describes the CTP message header format:

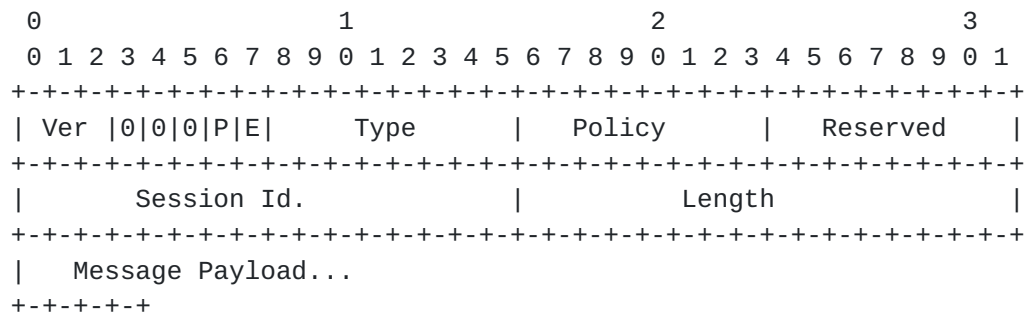


Figure 3 - CTP Header format

#### Ver Field

This field identifies the version of the protocol. It is 3 bits of data. For this specification the version field is 0.

#### Flags Field





This field is a bitmask of 5 bits that represents special CTP processing. Bits 3, 4, and 5 are undefined and MUST be zero (0). Bit #6 and #7 as follows:

Bit P ; Payload Header  
1 indicates that the CTP header is followed by a CTP payload header (see 5.3.1)  
0 indicates that there is no CTP payload header

Bit E - Data path Encryption  
1 indicates that the CTP-Data message type data is encrypted  
0 indicates that the CTP-Data message is in the clear

#### Type Field

This is a 1 byte field that identifies the message type. The message types are identified in [Section 4.2](#).

#### Policy Field

This is a 1 byte field that represents policy to be assigned and enforced. The definition of this policy field is dependent on the message type. For example, if the message type is CTP-Data (defined below) the Policy field corresponds to QoS policy for the MU data above and beyond the QoS TOS markings or DiffServ markings that may have been applied to the end-to-end user data. If the message type is not CTP-Data, then this field is not interpreted by either AP or AC and MUST be set to all zeros.

#### Reserved

Reserved for future use. MUST be set to zero (0).

#### Session ID Field

This is a 2 byte field that includes a unique session identifier provisioned by the AC after successful authentication.

#### Length Field

This is a 2 byte field that indicates the length of payload (excludes the header length).

## [4.2](#) Messages





|

Value...

Singh

Expires - October 2005

[Page 10]





AP_REG_RESPONSE	5	16	A 16 byte AP calculated response to AP_REG_CHALLENGE
AC_IPADDR_LIST	6	Variable	List of AC IP addresses with which said AP should attempt to connect
CONFIG	7	variable	Value contains a [SNMP] set of OIDs of encoded configuration elements
AC_REG_CHALLENGE	8	16	A 16 byte random challenge generated by the AP, to be used by AC upon registration request.
AC_REG_RESPONSE	9	16	A 16 byte AC calculated response to AC_REG_CHALLENGE
NETWORK_ID	10	4	Network ID with which a given radio in the AP is associated. This value is unique as it is calculated by the AC upon the provisioning phase of the AP and provided to it in the Config-Rsp message. In the case of 802.11 radio technology, this is the Extended Service Set (ESS) to which the AP belongs. This is a 32 bit integer representation of the ESS. For other radio technologies, this is a unique value representing the network that the radio is a member of.
AP_STATE	11	4	Value contains indication of AP state: 0=Standby 1=Active 2=Reset
SESSION_KEY	12	19	Encrypted session encryption key to secure AP to/from AC communications.





STATS	13	Variable	Value contains a [SNMP] set of OIDs of encoded statistics elements
RADIO ID	15	1	Index number of the radio as learnt during the Capabilities exchange.
REQ ID	16	1	Message identification to match request and response messages.
AUTH_PAYLOAD	17	Variable	Payload TLV to include Encapsulation of MU Authentication/Authorization Messages. Typically EAP frames.
CERTIFICATE	18	Variable	Digital certificate credentials of the AP or AC

## **5. Message descriptions**

### **5.1 Message State Control**

Unless otherwise stated, every message that is a "request" type includes a REQ ID payload inserted by the sender of the message. This is sent so as to aid in the match of messages that are received as "responses". After the transmission of each request, the source will wait up to 2 seconds for the reception of the response. If a response is not received, the source will retransmit the packet up to 3 times. If after 3 attempts a response is still not received the source aborts the session and resets its state machine. If the source is the AP, the AP shall resume registration operations. Correspondingly the AC will simply delete the AP session from its database and drop all packets which are from unregistered APs.

### **5.2 Control and Status messages**

#### **5.2.1 CTP\_Reg-Req**

This message is used by the AP to request registration with the AC.

This message is initiated by the AP after successful secure discovery and following the hardware and software initialization sequence of the AP. The Session ID of this message is set to 0x0000 because the AC will subsequently assign a Session ID upon successful



authentication. This message requires a mandatory payload, namely "AP Serial Number".

**HEADER**

Type = 2  
SessionID = 0x0000

**PAYLOAD**

REQ ID  
AP SERIAL NUMBER

### **5.2.2 CTP Reg-Rsp**

This message is sent by the AC to an AP to indicate that it has conditionally accepted the AP's registration request based on knowing who the AP is and based on the provided serial number. If the STATUS = Success, then this message will also contain an AP REG CHALLENGE payload. This is a randomly generated 16 byte challenge to the AP.

**HEADER**

Type = 3  
SessionID = 0x0

**PAYLOAD**

REQ ID = from the corresponding Reg-Req message  
STATUS = Success (1) or Failure (2) based on the known AP database in the AC  
AP REG CHALLENGE

### **5.2.3 CTP Auth-Req**

This message is sent by the AP to begin the authentication phase of the connection establishment with the AC. It contains the AP serial number, an AP REG RESPONSE payload, the AP's digital certificate (which contains the AP's public key) and a 16 byte random challenge to the AC. Note that the SessionID field in the packet header is still zero.

**HEADER**

Type = 4  
SessionID = 0x0

**PAYLOAD**

REQ ID  
AP\_SERIAL\_NUMBER  
CERTIFICATE  
AP REG RESPONSE = Digital Signature of the concatenation of the AP SERIAL NUMBER and the AP REG CHALLENGE (from the Reg-Rsp message)



AC\_REG\_CHALLENGE = 16 byte random number challenge sent to authenticate the AC.

The response is calculated by the AP and is verified by the AC. For details on the calculation of challenge and response, see [Section 7](#)

#### **[5.2.4](#) CTP Auth-Rsp**

This message is sent by the AC to the AP as an indication of the success or failure of the authentication phase. The AP is only considered to have successfully associated with the AC if both registration and authentication phases complete successfully.

##### **HEADER**

Type = 5

SessionID = 16 byte unsigned value generated by the AC. This is set appropriately in this message if the authentication phase was successful. After this message, the AP should use this Session ID in all subsequent messages.

##### **PAYLOAD**

REQ ID = from the corresponding Auth-Req message

STATUS = Success (1) if the AP's digital certificate was successfully verified and the AP REG RESPONSE was verified.

##### **CERTIFICATE**

AC REG RESPONSE = Digital Signature of the concatenation of the AP SERIAL NUMBER and the AC REG CHALLENGE (from the Auth-Req message)

SESSION KEY = An encrypted payload of the AC generated CTP session key. This is encrypted using the public key of the AP as received in the AP's digital certificate from the Auth-Req message.

The STATUS payload indicates whether authentication and registration was processed correctly. If so, Session ID for registration is explicitly provided in the message header.

#### **[5.2.5](#) CTP SW-Update-Req**

This message is sent by the AP to ask the AC whether it should upgrade its own software or not. It simply needs to provide its current software version to the AC.

This message MAY also be sent by the AC to the AP which is a command indication for the AP to stop operations and upgrade its software.

##### **HEADER**

Type = 6

SessionID = the assigned ID as received in the Auth-Rsp message.

##### **PAYLOAD**



REQ ID

SWVersion = Variable length ASCII text specifying the current running software on the AP.

#### **5.2.6 CTP SW-Update-Rsp**

This message is sent by the AC to signal the AP to upgrade its software or by the AP to the AC to indicate to confirm that it has received the upgrade request. When the corresponding request is issued by the AP, the AC will check the SWVersion payload received in the Software-Upgrade-Req for the AP and send a response based on a match. The interpretation of the SWVersion payload is implementation specific. The response by the AC is either "Yes" or "No" which is interpreted through the STATUS payload. If the response by the AC indicates a failure the AP must abandon the registration stage, upgrade its software to the version indicated by the AC. The method by which the software image is exchanged is outside of the scope of this protocol.

When the corresponding request is issued by the AC, the AP will simply confirm the reception of the request and abandon its connected state in order to perform the upgrade.

HEADER

Type = 7

SessionID = the assigned ID as received in the Auth-Rsp message.

PAYLOAD

REQ ID = from the corresponding SW-Update-Req message

STATUS = [Success/Don't Upgrade (1) | Failure/Upgrade (2)]

SWVersion [On Failure] = Variable length ASCII text specifying the correct software version the AP should have in order to complete the session registration with the AC.

#### **5.2.7 CTP\_Set-State-Req**

This message is sent by the AC to modify the operational state of the AP. For example, at some point during an established connection it may be necessary to instruct an AP to go to STANDBY state or initiate a reboot/reset of its state machine. These states are usually entered upon user request

The following states are defined and apply to the AP:

ACTIVE

Indication to the AP that it should exit standby state and should resume full active network state including enabling its RF





interfaces. This is the default state of the AP after successful configuration phase.

#### STANDBY

This signifies a state where the AP, although connected to the AC, is in a state whereby no RF connection is allowed. It may be sent to the AP upon user request.

#### RESET

This is used as a command to the AP to change state to initialization state. This may be sent to the AP upon user request or upon failure of any of the phases of the control channel establishment.

#### HEADER

Type = 12  
SessionID = AP session id from registration

#### PAYLOAD

REQ ID  
AP\_STATE = [STANDBY(0) | ACTIVE(1) | RESET(2)]

### [5.2.8 CTP\\_Set-State-Rsp](#)

This message is sent by the AP to indicate to the AC that it has changed its operational state as requested.

#### HEADER

Type = 13  
SessionID = AP session id from registration

#### PAYLOAD

REQUEST ID = Same ID that was received in the Set-State-Req message.

STATUS = [Success (1) | Failure (2)]  
AP\_STATE = [STANDBY(0) | ACTIVE(1) | RESET(2)]

The RESET(2) state assumes that the AP would have reset its operations after sending out this message.

### [5.2.9 CTP Poll-Req](#)

This message is the keepalive mechanism for the CTP control channel. This is sent by the AP to the AC. The default send frequency for this message is 5 seconds. If no response is received from the AC after sending this message 6 times in a row, then the AP should tear down its CTP control channel state and reattempt to connect to the AC. These values are considered to be defaults. An AP



implementation MAY choose to change these values for suitability to network deployment conditions.

**HEADER**

Type = 16

SessionID = AP session id from registration

**PAYLOAD**

REQ ID = ID representing the Poll-Req. Incremented until a corresponding Poll-Rsp is received.

**5.2.10 CTP Poll-Rsp**

This message is the keepalive mechanism for the CTP control channel. This is sent by the AC in response to a CTP Poll-Req message received from the AP. The AC SHOULD detect the loss of connectivity with the AP based on the receipt of a Poll-Req message.

**HEADER**

Type = 17

SessionID = AP session id from registration

**PAYLOAD**

REQ ID = ID corresponding to the Poll-Req received.

**5.2.11 CTP\_MU-Connect-Req**

This message is sent by the AP to relay an association request received from an MU to the AC.

**HEADER**

Type = 51

SessionID = AP session id from registration

**PAYLOAD**

REQ ID

MU-MAC-Address = MAC Address corresponding to the associating MU

NETWORK ID = Network identification where association is taking place

RADIO ID = Radio ID where association is taking place

**5.2.12 CTP\_MU-Connect-Rsp**

This message is sent by the AC to authorize the access point to relay an association response to the MU requesting service. If the association is successful, then the AC MAY also include optional payloads such as Policy which can be enforced at the AP.



If the association is rejected by the AC, the AP must disallow association of the MU.

**HEADER**

Type = 52  
SessionID = AP session id from registration

**PAYLOAD**

REQ ID = from the corresponding MU-Connect-Req message  
MU-MAC-Address = MAC Address corresponding to the associating MU  
STATUS = [Success (1) | Failure internal error (2) | Failure user deny (3)]

**5.2.13 CTP\_MU-Disconnect-Req**

This message is sent by the AC to request that a specific Mobile Unit session be removed from the AP list of currently connected devices. This operation may be the result of Mobile Unit roaming to a different AP or the result of Mobile Unit session timeout, or administrator request.

The MU-MAC-Address identifies the device in question.

**HEADER**

Type = 53  
SessionID = AP session id from registration

**PAYLOAD**

REQ ID = ID for the request. Must increment after every retransmission of this message.  
MU-MAC-Address = MAC Address corresponding to the MU that is to be disconnected.  
RADIO ID = Radio ID where disconnection is required.

**5.2.14 CTP\_MU-Disconnect-Rsp**

This message is sent by the AP to indicate that it has successfully processed a disconnect request by the AC. At this point the MU should no longer be associated with the AP.

**HEADER**

Type = 54  
SessionID = AP session id from registration

**PAYLOAD**

REQ ID = Same ID that was received in the MU-Disconnect-Req message.  
MU-MAC-ADDRESS = MAC Address corresponding to the MU that was disconnected



STATUS = [Success (1) | Failure (2)]

#### **5.2.15 CTP\_MU-Disconnect-Nfy**

This message is sent by the AP to the AC to indicate that it has received an explicit disconnection message from the MU. The transmission of this message from the AP is dependent on the MAC layer of the radio technology implemented on the AP as well as the capability of the MU. For example, the radio MAC layer may or may not support an explicit "disconnect" trigger when an MU goes away. Rather, the disconnection is based on a timer. In cases where the disconnection is timer based, the AC may be the appropriate entity to handle idle timer management. However, in the case where there may be a disconnect indication, then the AP must send this message to the AC when and MU disconnects.

**HEADER:**

Type = 57

SessionID = AP session ID negotiated at registration

**PAYLOAD**

MU-MAC-Address = MAC address of Mobile unit that was disconnected

NETWORK ID =

RADIO ID =

#### **5.2.16 CTP MU-Authenticate-Req**

This message is sent by the AP to forward an authentication request to the AC. In the case of 802.1x/EAP authentication, the payload of this packet will include information that the AC will forward to a RADIUS Server

**HEADER**

Type = 55

SessionID = AP session id from registration

**PAYLOAD**

REQ ID

AUTH\_PAYLOAD = The authentication request payload between the AP and the AC carries the request of the MU for authentication. In typical cases this will be the EAP packets from an 802.1x supplicant.

#### **5.2.17 CTP MU-Authenticate-Rsp**

This message is sent by the AC to forward an authentication response to the AP. In the case of 802.1x/EAP authentication, the payload of this packet will include the response from the RADIUS server which will be forwarded to the AP.





## HEADER

Type = 56

SessionID ; AP session id from registration

## PAYLOAD

REQ ID = from the MU-Authenticate-Req message

AUTH\_PAYLOAD = The Authentication response payload between the AP and the AC carries the response from the authentication server. In typical cases this will be the EAP packets from the Authentication server.

STATUS = [Success (1) | Failure (2)] - Note that the authenticator to authentication server interface resides in the AC so the AC does know the state of the authentication.

Note: There may be multiple transitions of this message set.

### 5.3 Configuration and Statistics messages

These messages correspond to information and command exchanges between AP and AC only after successful authentication and setup of the secure channel between AP and AC.

### 5.3.1 CTP Cap-Req

This message is sent by the AP to indicate to the AC the capabilities of this AP in regards to the number of radios and the types of RF technologies that it supports. The AP will encode its capabilities per each RADIO (or interface) that it supports. These are encoded in a variable length embedded attribute format called `capabilities control frames`. A type-length-value encoding scheme, similar to the format of payloads of regular control messages, is used to encode the capabilities attributes (ATTs) in the capability control frames.

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-
Type										Length										Value...																			
+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-

The available capability attributes are defined as follows:

- 1) ATT-NUM-RADIOS - number of radios that the AP supports.

Type= 1

Length= 1 byte

Value= 1 through 255







Type= 3  
 Length= 2 bytes  
 Value= MAC layer information as defined below:

```

0                               1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+--+--+--+--+--+--+--+--+--+
| RADIO-INDEX  |  MAC-TYPE      |
+-+--+--+--+--+--+--+--+--+--+

```

where

RADIO-INDEX is a unique index of the enumeration of the number of radios that the AP supports

MAC-TYPE is defined as

- o Local MAC           = 1
- o Split MAC           = 2

- 4) ATT-NETWORK-INFO - This attribute consists of the unique information that identifies each network per RADIO-INDEX and consists of RADIO-INDEX, NETWORK-INDEX and NETWORK-ID. Each Cap-Req payload MUST contain exactly NUM-NETWORKS worth of unique ATT-NETWORK-INFO attributes.

Type= 4  
 Length= 8 bytes  
 Value= network information type as defined below:

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| RADIO-INDEX  | NETWORK-INDEX |          NETWORK ID          |
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                     NETWORK ID                                     |
+-+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

where

RADIO-INDEX is a unique index of the enumeration of the number of radios that the AP supports

NETWORK-INDEX is a unique index of the enumeration of the networks that each RADIO supports



NETWORD-ID is the unique identifier for the network. This 6 byte value MAY be the MAC address for the given network within the radio. In the case of 802.11 radios, this value SHOULD be the BSS ID.

5) ATT-VENDOR-ID - name of vendor or manufacturer of AP.

Type= 5  
 Length= 4 bytes  
 Value = a 32-bit value containing the IANA assigned "SMI Network Management Private Enterprise Codes" [3].

6) ATT-PRODUCT-ID - name of product.

Type= 6  
 Length= variable length value of string  
 Value= ASCII string for the name of the product, non-Null terminated.

#### HEADER

Type = 20  
 SessionID = AP session id from registration

#### PAYLOAD

REQ ID = increments with each retransmission.  
 The capabilities attributes encoded as TLVs and as defined above.

### 5.3.2 CTP Cap-Rsp

This message is sent by the AC to acknowledge the capabilities of the AP. The AC must ack or nak the capabilities for each RADIO-INFO element that it received in the Cap-Req message. This is accomplished by sending back exactly ATT-NUM-RADIOS worth of ATT-RADIO-INFO-ACK for each RADIO-INFO sub-attribute that this AC supports.

The ATT-RADIO-INFO-ACK is an attribute that contains the RADIO-INDEX and CAP-STATUS sub-attribute. For each Radio type that the AC supports, the CAP-STATUS must be set to 1. For each radio type that the AC does not support, the CAP-STATUS must be set to 0.

Type= 7  
 Length= 2 bytes  
 Value= as defined below.

0	1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5	
+--+--+--+--+--+--+--+--+--+	
RADIO-INDEX	CAP-STATUS





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

#### HEADER

Type = 21

SessionID = AP session id from registration

#### PAYLOAD

REQ ID = ID corresponding to the Cap-Req message.

The AC capabilities attribute response encoded as TLVs and as defined above.

### **5.3.3 CTP Config-Req**

This message is sent by the AP to request configuration from its master AC. This message must be sent only after a receipt of a successful Auth-Rsp message from the AC and the verification of the AC's AC REG RESPONSE payload.

#### HEADER

Type = 8

SessionID ; the assigned ID as received in the Auth-Rsp message.

#### PAYLOAD

REQ ID

No specific information is required on this message.

### **5.3.4 CTP Config-Rsp**

This message is sent by the AC as a response to a Config-Req message to provide the configuration parameters for the registered AP.

#### HEADER

Type = 9

SessionID = AP session id from registration

Sequence Number = Sequence number of current packet.

#### PAYLOAD

REQ ID = from Config-Req message

STATUS = [Success (1) | Failure (2)]

CONFIG = The type of the configuration payload is defined in

[Section 5.3.10](#).

### **5.3.5 CTP Config-Ack**

This message is sent by the AP to indicate proper reception of an AP\_Config-Rsp message. This message is particularly important in processing multi-sequenced packets, in particular configuration



updates that require more than one payload for full receipt of configuration information.

**HEADER**

Type = 10

SessionID = AP session id from registration

**PAYLOAD**

None

**[5.3.6](#) CTP\_Config-Status-Notify**

This message is used by the AP to indicate to the AC that it has successfully completed it's configuration as per parameters indicated by the AP.

**HEADER**

Type = 11

SessionID = AP session id from registration

**PAYLOAD**

STATUS

**[5.3.7](#) CTP\_Stats-Notify**

This message is sent by the AP to provide periodic operational statistics to the AC. This message is also used following a correct configuration establishment to indicate to the AC that the AP is functionally ready to enter ACTIVE state.

**HEADER**

Type = 14

SessionID = AP session id from registration

**PAYLOAD**

STATS - The type of the statistics payload is defined in [Section 5.3.10](#).

**[5.3.8](#) CTP Stats-Req**

This message is sent by the AC to request statistics information upon request. It is intended to be used as an interface by an administrator or management application to query the AP for instantaneous statistics information.

**HEADER**

Type = 18

SessionID = AP session id from registration



**PAYLOAD**

STATS = The type of the statistics payload is defined in [Section 5.3.10](#)

**[5.3.9](#) CTP Stats-Rsp**

This message is sent by the AP to provide operational statistics to the AC as per the Stats-Req message. It is similar in format to the Stats-Notify message.

**HEADER**

Type = 19

SessionID = AP session id from registration

**PAYLOAD**

STATS = The type of the statistics payload is defined in [Section 5.3.10](#)

**[5.3.10](#) Configuration and Statistics**

Two data representations were considered for the CTP configuration and statistics payload. The first data representation considered was a TLV representation where all the variables for the statistics and configuration would be defined as groups of TLVs. Given the nature of CTP as a radio agnostic protocol and the complexity of the statistics and configuration of the 802.11 protocols with multiple networks per radio a TLV representation might be cumbersome and not extensible.

Most of today's network devices in both the enterprise and the carrier space employ the Simple Network Management Protocol. Thus, it is natural to assume that most, if not all, APs will contain an embedded SNMP agent able to decode SMI representations. Using SMI representations for configuration and statistics variables can speed up deployment of CTP without incurring additional cost for the APs. Our recommendation is to reuse the 802.11 MIBs where applicable for the CTP configuration and statistics message payload. MIB extensions should be defined where the corresponding IEEE MIBs are not sufficient. Upon reception of the message the CTP daemon should forward the configuration and statistics message payload to the SNMP daemon for further decoding and processing of the SMI O.I.D.s.

**[5.4](#) CTP Data Messages**

The CTP data messages use the same CTP header as the control and other messages. If the Type field is 15 (CTP-Data), then the Policy field of the header is used by the AC to tag the data for special handling. The interpretation of the Policy field is left up to the

implementation. An example of its use is as follows:

Singh

Expires - October 2005

[Page 27]

Data packet coming into the AC from the wired network is a voice packet as indicated by the TOS or DSCP markings in the IP header. This TOS/DSCP byte will be copied to the outer transport header for proper priority handling within the network between the AP and the AC. However, for appropriate classification at the AP, the AC sets the Policy field to a value that allows the AP to prioritize this packet over other data packets that may have a lower priority. Similarly in the reverse direction, the MU may have set the appropriate fields in the original IP header, but the AP can interpret those bits and map them to the Policy field in the CTP-Data header for special dispensation at the AC.

#### **5.4.1 CTP\_Data**

This message is utilized as the transport of MU layer data. The contents of the message body are not interpreted by the AP layer other than sending it to the MAC layer of the AP.

##### **HEADER**

Type = 15  
SessionID = AP session id from registration  
Policy = as set by the implementation

##### **PAYLOAD**

802.3 frame





## 6. State Machines

This state machine in Figure 4 indicates the logical state transitions of the CTP session establishment.

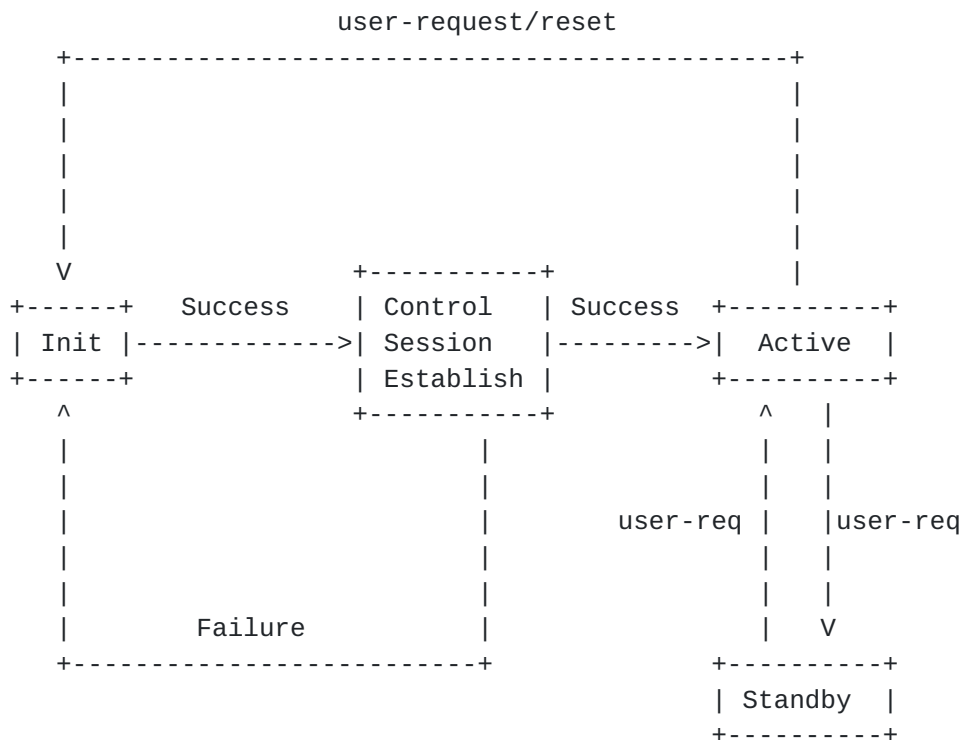


Figure 4 - Simple CTP state machine

### 6.1 Init

This state represents the boot state, and initialization of the hardware. Entry into this state is either Failure of the Control Session Establishment or user-request or reset signal from the Active state

### 6.2 Control Channel Establishment

Once Initialization completes the AP initiates the control channel establishment phase of the connection. Any phase within this state that fails because of a STATUS=FAILURE or no response from either device will result in a failure of the whole phase and go back to initialization. A successful completion of the control session establishment process will include

- Registration
- Authentication



Software Upgrade Notification  
Capability negotiation  
Configuration Request  
Configuration Response  
Configuration Ack.

Upon receipt of a successful Config-Ack from the AP, the AP and AC session for the AP are put into ACTIVE state.

### **6.3 Active State**

Once confirmation of successful registration is received the device now has a properly established communications/tunneling session with the AC. The Authentication response MUST have indicated a valid CTP session ID by which this tunnel is registered on the AC. So in this state, the SessionId MUST be non-zero.

This state persists until device terminates or communications with the AC are interrupted. To assist in the detection of connection termination, the device MUST implement the CTP Poll-Req and Poll-Rsp messages as described previously. Another method of exiting this state is with an explicit Set-State message that may only be initiated by the AC to the AP.

### **6.4 Standby State**

At some time during the operation, it may be necessary to instruct an AP to halt its current operation, ie. to switch off the RF interface(s) on the AP. This is done by the Set-State message. The device will remain in this state, until explicitly told by the AC to resume operation also using the Set-State message.

## **7. Authentication, Encryption and Session Key generation**

Since the AP and AC can be separated over any arbitrary L3 cloud, first and foremost there is a need for a secure binding between the AC and AP. A control channel security association is required between the AC and AP.

### **7.1 Authentication**

The AC and AP must go through a mutual authentication phase during a registration and authentication process and form a security association. A couple of assumptions are made to ensure this security association is created. First, there must be a secure mechanism to get the digital certificates onto the APs and ACs and that process must be run either at the factory or prior to device deployment. Secondly, the placement of the AP ID (in most cases the AP serial number) in a data store on the AC assumes a secure



insertion mechanism. This may be a manual process or other secure ID provisioning methods may be employed. Mutual authentication of AP and AC is done by means of digital certificates as is described below.

```

+-----+                                     +-----+
|  AP  |                                     |  AC  |
+-----+                                     +-----+

                Reg-Req(AP-ID)
                ----->

                Reg-Rsp(Status,AP-challenge)
    <-----

                Auth-Req(AP-ID,AP-cert,AP-resp,AC-challenge)
    ----->

                Auth-Rsp(Status,AC-cert,AC-rsp,Session-Key)
    <-----

```

AP-ID - AP SERIAL NUMBER attribute. This attribute is assumed to be available in a data store in the AC as well as being factory burnt-in in the AP device. The AC will respond with a STATUS=Success in the Reg-Rsp message if there is a match in its data store for the given AP-ID

AP-challenge - is a 16 byte random number generated using [4] as guidelines for the randomness of the challenge.

AP-cert - Is a digital certificate assumed to be available on the AP prior to its Registration request. The mechanism to get the certificate onto the AP is out of scope for this document.

AP-resp - Is a digital signature over the SHA-1 hash of the AP-challenge concatenated with the AP-ID.

S-ap(H-sha1(AP-challenge|AP-ID))

AP-challenge - is a 16 byte random number generated for subsequent authentication of the AC.

AC-cert - Is a digital certificate or chain of certificates of the AC that is assumed to be available on the AC prior to sending the Reg-Rsp message. The mechanism to get the certificate or chain of certificates onto the AC is out of scope for this document.

AC-resp - is a digital signature over the SHA-1 hash of the AC-challenge concatenated with the encrypted session key.

S-ac(H-sha1(AC-challenge|Enc-ac-p(SessionKey)))



Session Key - is actually the encrypted randomly generated session encryption keying material. The AC uses the public key of the AP to encrypt the session encryption key. The size of the Session Key is 19 bytes. The first 16 bytes are used as AES-CCM encryption and the remaining 3 bytes are used as a salt for a nonce which is required by the AES-CCM algorithm. See [section 7.2](#) for encryption details. The Session key is a random number generated using [4]. At the time of writing this document there are no known weak keys for AES.

The following steps describe in detail the registration and authentication process:

1. The AP sends a Reg-Req message with its AP SERIAL NUMBER. If it does not receive a Reg-Req within 3 seconds, it must resend the Reg-Req message.
2. Upon receipt of the Reg-Req message, the AC checks its data store for the AP SERIAL NUMBER. If it exists then the AC sends back a Reg-Rsp message with STATUS payload with Success (1) attribute and an AP CHALLENGE payload. If the AP SERIAL NUMBER does not exist, then a Reg-Rsp message with a STATUS payload of Failure (2) is sent back.
3. The AP will take the AP CHALLENGE payload, concatenate it with the AP SERIAL NUMBER and calculate an AP RESPONSE as shown above and send it back to the AC along with an AC CHALLENGE payload and its own digital CERTIFICATE payload in an Auth-Req message.
4. Upon receipt of the Auth-Req message the AC will
  - a. Verify the AP's digital certificate
  - b. Verify the AP RESPONSE, which was the digital signature of the AP over the hash of the AP CHALLENGE and the AP SERIAL NUMBER. This is done with the public key of the AP.
  - c. If both a) and b) are verified correctly, then the STATUS payload will contain Success (1). Otherwise it will contain Failure (2).
  - d. If Success, then the AC will add its own CERTIFICATE to the Auth-Rsp message
  - e. Encrypt the session encryption keys with the public key of the AP.
  - f. Generate a unique SessionID to be used in subsequent CTP messages.
  - g. Send back an Auth-Rsp message with STATUS, CERTIFICATE, AC RESPONSE and SESSION KEY payloads with the SessionID in the CTP header.
5. Upon receipt of the Auth-Rsp message, the AP will
  - a. Verify the AC's digital certificate
  - b. Verify the AC RESPONSE which was the digital signature of the AC over the hash of the AC CHALLENGE and the encrypted session encryption key.
  - c. Decrypt the encrypted session encryption key with its own

private key

Singh

Expires - October 2005

[Page 32]



- d. Store the SessionID which will be used in each subsequent CTP message.
6. All CTP control messages after the Auth-Rsp will be sent encrypted with AES-CCM as described in [section 7.2](#).

## 7.2 Encryption

Once the registration and authentication process has successfully completed then the control traffic is encrypted. The traffic is confined to control, configuration and management traffic between the AC and AP.

It is believed that for security sensitive applications and deployments there will always be an end to end encrypted tunnel for MU data traffic. Therefore, a data path encryption mechanism is not provided by CTP.

All control messages except of CTP\_Reg-Req, CTP\_Reg-Rsp, CTP\_Auth-Req and CTP\_Auth-Rsp, which are used to establish a trust relationship between the AP and AC, must be encrypted. If a non-encrypted CTP control packet with type other than CTP\_Reg-Req, CTP\_Reg-Rsp, CTP\_Auth-Req and CTP\_Auth-Rsp is received, it MUST be dropped by a receiver and no notification is sent to the sender.

Encrypted packets MUST be sent in the following format:

[illegible]

The first 8 bytes is general CTP header described in [section 4.1](#). E bit MUST be equal to 1.

The additional fields have the following meaning:



IV ; Initialization Vector used by AES-CCM as described in [section 7.2](#).

Sequence Number ; 32 bits value used for anti-replay protection.

Encrypted Data ; data of variable length encrypted with AES-CCM. Typically the encrypted data corresponds to the specified message payloads.

Authentication Data ; MAC of CTP header, IV, Sequence Number and encrypted data.

CTP uses AES-CCM encryption as defined in [5] with value  $L = 4$  and value  $M = 8$ . The Nonce length is 11 bytes. The Nonce is formed by concatenation of 3 bytes of the salt send by AC to the AP during Session Key exchange and 8 bytes of Initialization Vector. The sender of a packets MUST NOT send two packets with the same IV, as it immediately leads to plain-text revealing.

The Sequence Number field MUST start from zero for the first encrypted packet and is incremented each time a packet is encrypted. The receiver MUST use the sequence number field to protect against replay-attack and MAY use it to accept reordered or late packets. The sender MUST negotiate a new session key before reaching maximum value for the Sequence Number.

The sender of an encrypted packet MUST perform the following steps during the packet encryption:

- IV and the Sequence Number are inserted into the packet after CTP header.
- E bit in CTP header is set to 1.
- The first 20 bytes including CTP header, IV and the Sequence Number are passed to AES-CCM for authentication only.
- The CTP payload is encrypted with AES-CCM.
- After encryption, a MAC value received from AES-CCM is copied to the output packet after encrypted data.
- The Sequence Number MUST be incremented
- IV value must be changed to another value which has not been used so far with the current encryption key.

The receiver of the encrypted packet MUST perform the following steps during the packet decryption:

- E bit in CTP header is checked. If it is not 1, the packet is silently dropped.
- Type of the packet is checked. All control packets except CTP\_Reg-Req, CTP\_Reg-Rsp, CTP\_Auth-Req and CTP\_Auth-Rsp must be encrypted.
- The Sequence Number is compared to the sequence number of the last received packet, which MUST be stored by the receiver. If the

Sequence Number is larger than the one stored by the receiver the

Singh

Expires - October 2005

[Page 34]

packet MUST be accepted for further processing. If the sequence number is equal to the one stored by the receiver the packet MUST be silently dropped. If the sequence number is lower than stored by the receiver, packet MAY be accepted if the receiver implements sliding window algorithm.

- Payload of the packet is passed for decryption to AES-CCM algorithm.
- The first 20 bytes of the packet starting with CTP header are passed to AES-CCM for authentication.
- Data payload is passed to AES-CCM for decryption
- After decryption, MAC value received from AES-CCM decryption process is compared to the MAC value received in the packet. If locally calculated MAC does not match the MAC value from the received packet, the packet MUST be silently dropped. If MAC values are equal, the packet is passed for further processing.
- IV, the Sequence Number and MAC values are stripped from the packet.
- If the Sequence Number from the received packet is larger than stored by the receiver, the receiver must update the stored sequence number with the received one.

### **7.3 Session Key refresh and generation**

One session key is used to encrypt control packets exchanged in both directions between the AP and the AC. The Session Key is always generated by the AC and is sent to AP during the CTP registration and authentication phase as described in [section 7.1](#).

The Session Key must be refreshed before either one of the following happens:

- key lifetime expires
- sequence numbers are exhausted

The Session Key's lifetime is not negotiated in-band and is set to 24 hours.

If the Session Key's lifetime has expired or the sequence numbers have been exhausted and the new Session Key has not been negotiated, the receiver MUST silently drop any received packet and the sender MUST NOT encrypt CTP packet.

The Key refresh is always initiated by the AP. The packet exchange between the AP and the AC for new key is TBD.

The AC MAY request the AP to start the key refresh process by sending TBD packet.

After the Session Key refresh, the AC must use the old key until it receives a packet encrypted with the new Session Key, what is an

indication that the AP received and accepted the new Session Key.

Singh

Expires - October 2005

[Page 35]

## 8. Security considerations

CTP provides mutual authentication of the AP and the AC. The trust is achieved by digital certificates. The trust hierarchy leading to successful certificate or certificates chain validation is out of scope of this document.

Certificates issued for the AP and the AC are bound to the serial number of the AP and the AC respectively.

During the authentication exchange, the receiver cannot verify that the sender of the certificate really has the serial number presented in the certificate. An attacker may steal the legitimate credentials and send a valid certificate from a device with different serial number.

During the authentication phase the receiver MAY verify whether the presented certificate has not been revoked. The mechanism of accessing CRL is not defined by CTP.

CTP encryption and authentication is sufficient for control packets only. It MUST NOT be used for data encryption, because the exchange between the AP and the AC does not use ephemeral keys. Compromise of AP's private key enables an attacker to decrypt all session keys used in the past between the AP and AC and decrypt all data packets exchanged between AP and AC.

Control packets exchanged between the AP and the AC are encrypted and authenticated. Both, confidentiality and authentication is provided by AES-CCM as described in [5].

## 9. References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997
- [2] O'Hara, B., et. al, "CAPWAP Problem Statement", [RFC 3990](#), February 2005
- [3] "Assigned Numbers: [RFC 1700](#) is Replaced by an On-line Database", January 2002, <ftp://ftp.isi.edu/in-notes/rfc3232>
- [4] Eastlake, D., et. al., "Randomness Recommendations for Security", December 1994, [RFC 1750](#)





[5] Whiting, et al., "Counter with CBC-MAC (CCM)", September 2003,  
[RFC 3610](#)

#### **10. Author's Addresses**

Paulo Francisco  
Chantry Networks  
1900 Minnesota Court  
Mississauga, ON M8V 1E5  
Canada

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

Inderpreet Singh  
Chantry Networks  
1900 Minnesota Court  
Mississauga, ON M8V 1E5  
Canada

Phone: +1 905-363-6412  
Email: isingh@chantrynetworks.com

Krzysztof Pakulski  
Chantry Networks  
1900 Minnesota Court  
Mississauga, ON M8V 1E5  
Canada

Phone: +1 905-363-6400 (ext. 6449)  
Email: kpakulski@chantrynetworks.com

Floyd Backes  
AutoCell Laboratories  
125 Nagog Park  
Acton, MA 01720  
USA

Phone: +1 978-264-4884  
Email: fbackes@autocell.com

#### **Intellectual Property Statement**

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in



this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

#### Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

#### Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

#### Acknowledgment

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

