Network Working Group   S. Iino
Internet-Draft   S. Govindan
Expires: December 25, 2005   M. Sugiura
                                                        H. Cheng
                                                       Panasonic
                                                   June 23, 2005

Wireless LAN Control Protocol (WiCoP)
draft-iino-capwap-wicop-02.txt

Status of this Memo

Copyright Notice

Abstract

   The popularity of wireless local area networks (WLANs) has led to
   wide spread deployments across different establishments. It has also
   translated in to increasing scale of the WLANs. Large-scale
   deployments made of large numbers of wireless termination points
   (WTPs) and covering substantial areas are increasingly common.

   The Wireless LAN Control Protocol (WiCoP) described in this document
   allows for the control and provisioning of large-scale WLANs. It
   enables central management of these networks and realizes the
   objectives set forth for the control and provisioning of wireless
   access points (CAPWAP).

Table of Contents

1. Requirements notation

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 [RFC2119].

2. Terminology

   This document follows the terminologies of [I-D.ietf-capwap-arch] and
   [I-D.ietf-capwap-objectives].

3. **Introduction**

   The popularity of wireless local area networks (WLANs) has led to
   numerous but incompatible designs and solutions. The CAPWAP
   Architecture Taxonomy [I-D.ietf-capwap-arch] describes major
   variations of these designs. Among them, the local-MAC and split-MAC
   architecture designs are notable categories.

   Wireless LAN Control Protocol (WiCoP) recognizes the major
   architecture designs and presents a common platform on which WLAN
   entities of different designs can be accommodated. This enables
   interoperability among wireless termination points (WTPs) and WLAN
   access controllers (ACs) of distinct architecture designs. WiCoP
   therefore allows for cost-effective WLAN expansions. It can also
   accommodate future developments in WLAN technologies. Figure 1
   illustrates the WiCoP opertional structure in which distinct control
   elements are utilized for local-MAC and split-MAC WTPs.

   WiCoP also addresses the increasing trend of shared infrastructure
   WLANs. Here, WLAN management needs to distinguish and isolate
   control for the different logical groups sharing a single physical
   WLAN. WiCoP manages WLANs through a series of tunnels that separate
   traffic based on logical groups.

   The WiCoP operational structure in Figure 1 shows that each WTP uses
   a number of tunnels to distinguish and separate traffic for control
   and for each logical group. The protocol allows for managing WLANs
   in a manner consistent with the logical groups that share the
   physical infrastructure.

```
                           Local-MAC WTP


    +-------+                   +-------+
    |       |                   |       |   Logical Groups
    |      (=====Control Tunnel=====)   |
    |       |                   |       |      ~~~~~~~
    |       |                   |       |     /       /
    |     <=====Logical Group A====>    |    /   A   /~~~~
    |       |                   |       |   /       /   /
    |     <=====Logical Group B====>    |    ~~~~~~~     /~~~~
    |       |                   |       |        /   B  /    /
    |     <=====Logical Group C====>    |     ~~~~~~~       /
    |       |                   |       |       /   C  /
    |       |                   +-------+        ~~~~~~~
    |       |
    |       |
    |  AC   |
    |       |
    |       |              Split-MAC WTP
    |       |
    |       |              +-------+   Logical Groups
    |       |              |       |   |
    |     [=====Control Tunnel=====]       |    ~~~~~~~
    |       |                   |       |   /       /
    |       |                   |       |  /   1   /~~~~
    |     <=====Logical Group 1====>    |  /       /   /
    |       |                   |       |   ~~~~~~~     /
    |     <=====Logical Group 2====>    |      /   2  /
    |       |                   |       |       ~~~~~~~
    +-------+                   +-------+
```

                          Figure 1

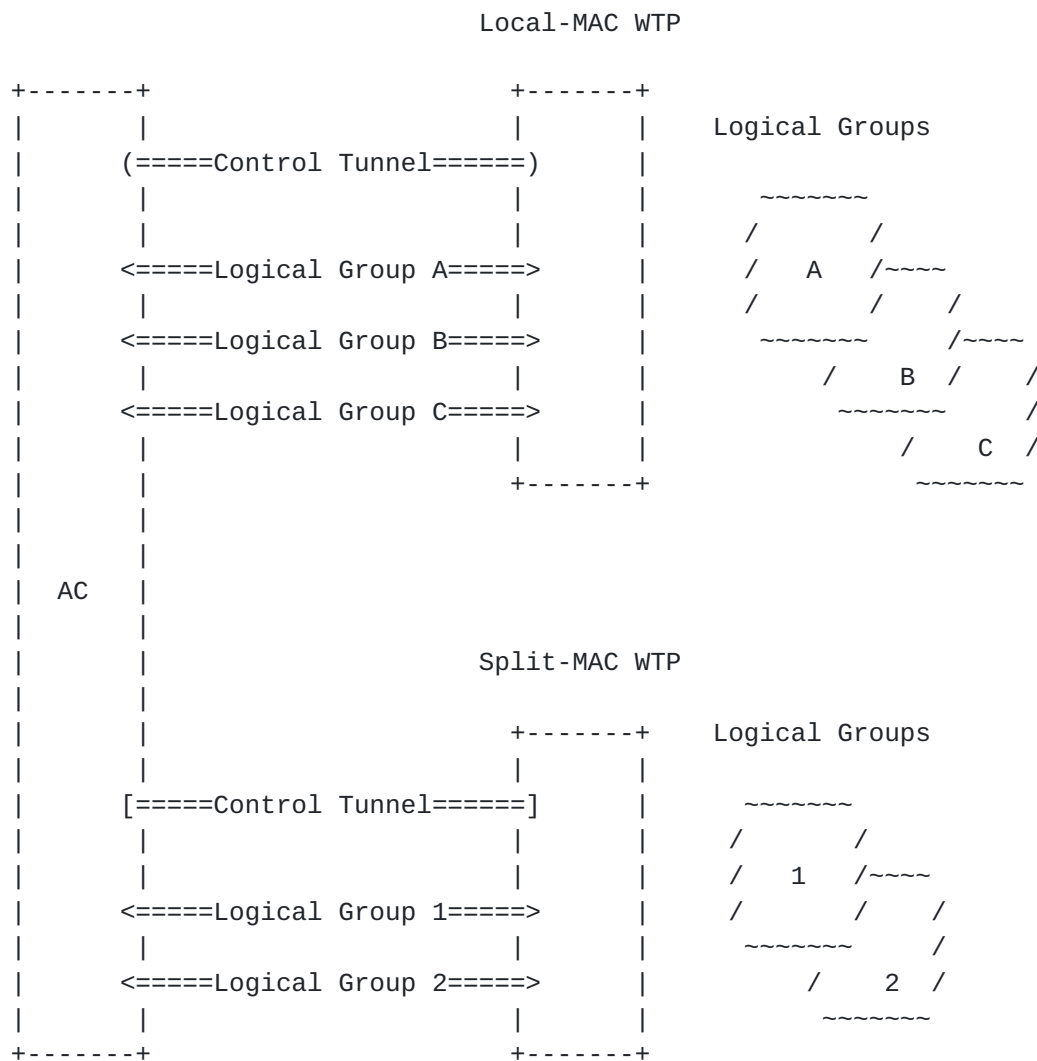   From Figure Figure 1 WiCoP establishes and operates control tunnels
   and logical group tunnels between the AC and two types of WTPs. The
   control tunnels are used to transport WiCoP messages dealing with the
   configuration, monitoring and management of WTPs as a physical whole.
   The logical group tunnels serve to separate traffic among each of the
   logical groups constituting a physical WTP.

4. **Protocol Overview**

   The Wireless LAN Control Protocol (WiCoP) focuses on enabling
   interoperability in shared infrastructure WLANs. It is designed for
   use with different wireless technologies. This document provides
   both the general operations of WiCoP and also specific use-cases with
   respect to IEEE 802.11 based systems.

   The state machine for WiCoP is illustrated in Figure 2.

```
                                 +--------------------------------+
                                 |                                |
                                 |    +-----------------+         |
                                 V    V                 |         |
     +-------------+       +-------------+       +-------------+   |
     |             |       |             |       |             |   |
     | Initial-    |-------->| Capabilities|-------->|  Connection |   |
     |    ization  |       |   Exchange  |       |             |   |
     |             |       |             |       |             |   |
     +-------------+       +-------------+       +-------------+   |
          A                     A                      |          |
          |                     |                      |          |
          |                     |                      |          |
          |                     |                      |          |
          |                     |                      V          |
          |                     |               +-------------+   |
          |                     |               |             |   |
          |                     +---------------| Configur-   |   |
          |                                     |    ation    |   |
          |                                     |             |   |
          |                                     +-------------+   |
          |                                            |          |
          |                                            |          |
          |                                            |          |
          |                                            |          |
          |                                            V          |
          |                                     +-------------+   |
          |                                     |             |   |
          +-----------------------------------------|         |-+
                                                |  Operation  |
                                                |             |
                                                +-------------+
```
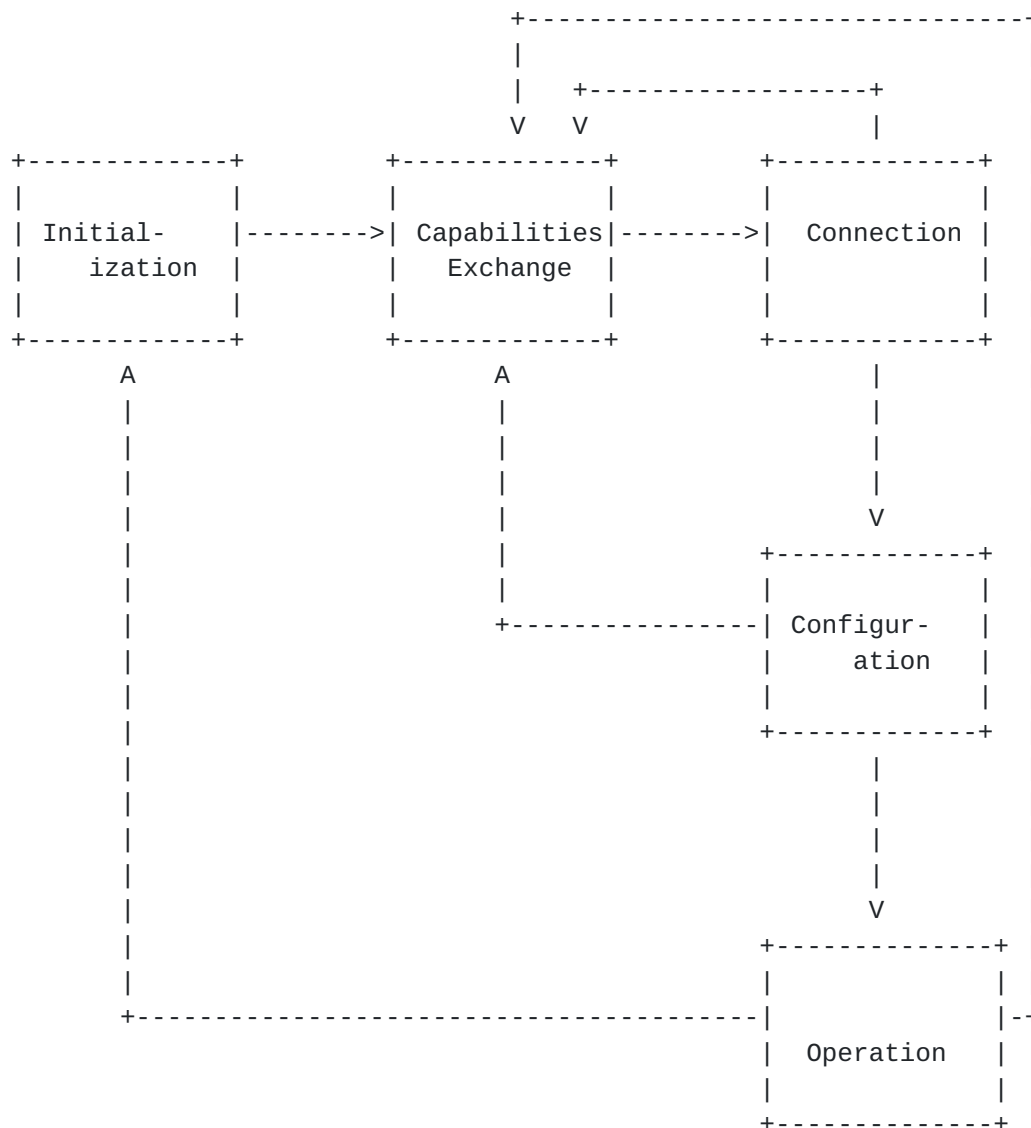
                              Figure 2

   The Initialization state represents the initial states of WTPs and
   AC. A WTP or AC in this state powers on, clears internal registers,
   runs hardware self-tests and resets network interfaces.

The Capabilities Exchange state represents initial protocol exchange
between a WTP and an AC. A WTP in this state determines possible ACs
from which it can receive management services. An AC in this state
determines the capabilities of the WTP and the WTP's compatibility
with the management services it offers.

The Connection state represents the creation of a security
infrastructure between WTP and AC. This involves mutual
authentication and the establishment of a secure connection between
the WiCoP entities.

The Configuration state represents the exchange of long-term
operational parameters and settings between a WTP and AC. A WTP in
this state receives configuration information to allow it to operate
consistently within the WLAN managed by the AC. An AC in this state
provides configuration information to the WTP based on the WTP's
capabilities and network policies.

The Operation state represents the active exchange of WiCoP
monitoring and management messages. WTPs send regular status updates
to and receive corresponding management instructions from the AC.
This state also involves firmware and configuration updates arising
from changes in network conditions and administrative policies.

5. **WiCoP Format**

   WiCoP uses separate packets for control and data message transfer
   between the AC and WTPs. A common header is used for both types of
   packets in which a single-bit flag distinguishes between them. This
   section presents the packet formats for WiCoP packets.

5.1 **WiCoP Header**

   Figure 3 illustrates the WiCoP common header for control and data
   packets.

```
0                                                               31
|                 7               15             23              |
|-------|-------|-------|-------|-------|-------|-------|-------|
|                                                               |

+---------------+-+-+-+-+-+-+-+-+-----------------------------+
|    Version    |M|D|C|R|E|F|L| |          Reserve            |
+---------------+-+-+-+-+-+-+-+-+-----------------------------+
| Fragment ID   | Fragment No.  |          Length             |
+---------------+---------------+-----------------------------+
```

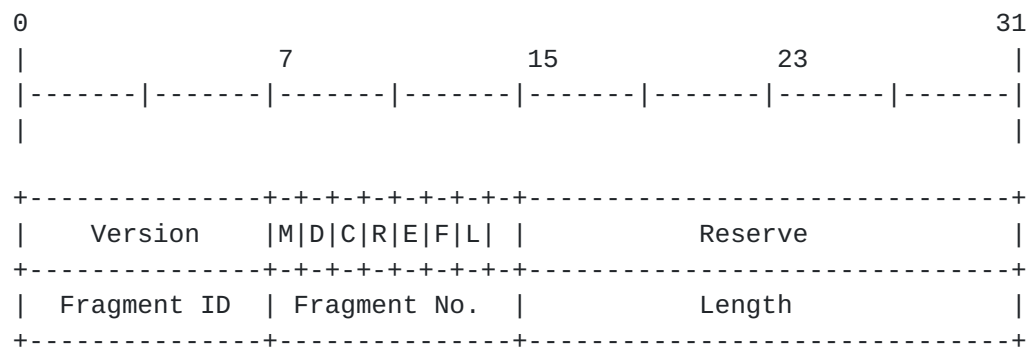   Figure 3

   Version Field

   This field indicates the protocol version.

   'M' Field

   The MAC-type field, 'M', distinguishes between local-MAC WTPs and
   split-MAC WTPs. It is used to efficiently realize interoperability
   between WTPs of the two different designs. A '0' value indicates
   WiCoP exchanges with a split-MAC WTP while a '1' value indicates
   WiCoP exchanges with a local-MAC WTP.

   The presence of this classification bit in the WiCoP common header
   serves to expedite processing of WiCoP and WLAN traffic at the AC.
   So with a single parsing of the WiCoP common header once, the AC will
   be able to determine the appropriate processing required for the
   particular WiCoP packet.

   'D' Field

The differentiator field, 'D', is used to distinguish between WTP
variants within a type of WTP design. The CAPWAP Architecture
Taxonomy [I-D.ietf-capwap-arch] illustrates that the split-MAC design
allows encryption/decryption to be performed at either the WTP or the
AC. The Architecture Taxonomy also indicates that the local-MAC
design allows authentication to take place at either the WTP or the
AC.

WiCoP acknowledges these major variants and accommodates them using
the 'D' field in conjunction with the 'M' field. So for a split-MAC
WTP, the 'D' field is used to indicate location of encryption/
decryption while for a local-MAC WTP, the 'D' field is used to
indicate location of authentication. The following table highlights
their usage.

'M'	'D'	Description
0	0	Split-MAC WTP - Encryption/decryption is performed at WTP
0	1	Split-MAC WTP - Encryption/decryption is performed at AC
1	0	Local-MAC WTP - Authentication is performed by WTP
1	1	Local-MAC WTP - Authentication is performed by AC

Similar to the 'M' field, the presence of this classification in the
WiCoP common header helps expedite processing at the AC with a single
parsing. By incorporating the classification bits in the WiCoP
common header, where it is available for all packets of a session,
the AC processing can be expedited. Alternatively, the AC would have
to check each arriving packet against an internal register and
consequently delay processing.

'C' Field

This field distinguishes between a WiCoP control and WiCoP data
packet. Each type of information is tunneled separately across the
WiCoP tunnel interfaces between WTPs and the AC. A '0' value for the
'C' field indicates a data packet while a '1' value indicates a
control packet.

The 'C' field is also used to assign WiCoP packets to distinct data
and control tunnels between AC and WTP. WiCoP also maintains logical
groups in WLANs with the 'C field.

'R' Field

The retransmission field, 'R', is used to differentiate between first
and subsequent transmission of WiCoP packets. The 'R' field is used
for critical WiCoP packets such as those relating to security key
exchanges. A '0' value for the 'R' field indicates the first
transmission of a WiCoP packet while a '1' value indicates a
retransmission.

'E' Field

The encryption field, 'E', is used to indicate if the WiCoP packet is
encrypted between the AC and WTPs. The 'E' field is used for those
WiCoP packets that are exchanged during initialization. A '0' value
indicates the WiCoP packet is unencrypted while a '1' value indicates
the packet is encrypted.

'F' Field

The fragmentation field indicates if the packet is a fragment of a
larger packet. A '0' value indicates a non-fragmented packet while a
'1' value indicates a fragmented packet. The 'F', 'L', 'Fragment ID'
and 'Fragment No.' fields are used together.

'L' Field

This field is used to indicate the last fragment of a larger packet.
It is only valid when the 'F' field has a '1' value. A '0' value for
the 'L' field indicates the last fragment of a larger packet while a
'1' value indicates an intermediate fragment of a larger packet. The
'F', 'L', 'Fragment ID' and 'Fragment No.' fields are used together.

Fragment ID Field

The Fragment ID identifies the larger packet which has been
fragmented. It is used to distinguish between fragments of different
large packets. This field is valid only when the 'F' field has a '1'
value. The 'F', 'L', 'Fragment ID' and 'Fragment No.' fields are
used together.

Fragment No. Field

The fragment number field identifies the sequence of fragments of a

larger packet. The value of the Fragment No. field is incremented
for each fragment of a larger packet so as to show the order of
fragments. This field is valid only when the 'F' field has a '1'
value. The 'F', 'L', 'Fragment ID' and 'Fragment No.' fields are
used together.

Length Field

This field specifies the length of the WiCoP payload following the
header.

5.2 WiCoP Control Packet

The WiCoP control header follows the WiCoP common header. It is
highlighted in Figure 5.


```
0                                                               31
|               7               15              23               |
|-------|-------|-------|-------|-------|-------|-------|-------|
|                                                               |


+---------------+---------------+-----------------------------+
|   Msg Type    |    Reserve    |            Seq Num          |
+---------------+---------------+-----------------------------+
|      Msg Element Length       |
+-------------------------------+
```
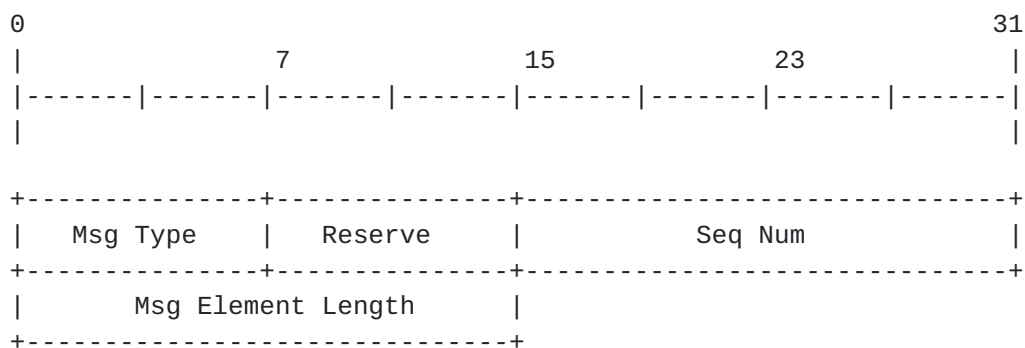
                          Figure 5

The control packet adds four additional fields to the common header.
These are described below;

Msg Type Field

The message type field specifies the type of control message
transported in the packet. The list of control messages is presented
below.

Seq Num Field

The sequence number field is used to map WiCoP request and response
sequences. The initiator of a WiCoP request message increments the
Seq Num field for each new request message. The responder then uses
these values of the Seq Num fields in its corresponding response
messages.

Msg Element Length Field

This field specifies the length in bytes of the subsequent WiCoP
control message element.

5.2.1 WiCoP Control Messages

The list of WiCoP control messages is shown below;

```
Message                           Msg Type
------------------------------------------------------------

Capabilities                          1
Capabilities Response                 2
Connection                            3
Connection Response                   4
Configuration Request                 5
Configuration Response                6
Configuration Data                    7
Configuration Data Response           8
Configuration Trigger                 9
Configuration Trigger Response       10
Feedback                             11
Feedback Response                    12
Reset                                13
Reset Response                       14
Firmware Download                    15
Firmware Download Response           16
Terminal Addition                    17
Terminal Addition Response           18
Terminal Deletion                    19
Terminal Deletion Response           20
Key Configuration                    21
Key Configuration Response           22
Notification                         23
Notification Response                24
```

5.2.2 WiCoP Control Message Elements

WiCoP control messages each include a control message header followed
by one or more message elements. The message elements are shown in
the following table.

Message Element	Type	Description
WTP-Info	1	Information regarding WTPs, such as manufacturer ID, MAC address, etc.
Cap-from-WTP	2	QoS abilities (WME) and security abilities (IEEE 802.11i) are included
Conf-If-Data	3	PHY information for each wireless interface
Conf-WTP-Data	4	Information regarding logical groups on a per-logical group basis (e.g. per-virtual AP)
Cap-to-WTP	5	Setup data sent to WTPs by AC on a per-logical group basis
QoS-Value	6	QoS setup (access categories)
Timer-Init-Value	7	Initial values of timers such as aging, echo interval etc.
Terminal-Data	8	Information relevant to wireless terminals - BSSID, association ID, etc.
BSSID	9	BSSID, and terminal MAC address
Encryption-Data	10	Details of the security framework - cipher suit, operation mode etc.
EAP-Frame	11	EAP frame
Statistics	12	Various statistics information - transmission attempts, FCS errors etc.
Interface-Error	13	Type of wireless interface failure
FROM-Error	14	Flash ROM Error information
QoS-Capability	15	Network congestion information
TFTP-Data	16	Firmware related details

```
| Result            | 17        | Result of protocol operations -   |
|                   |           | success or failure                |
|                   |           |                                   |
| OID               | 18        | SNMP OIDs                         |
|                   |           |                                   |
| GTK-Flag          | 19        | Determines type of GTK - new or   |
|                   |           | existing                          |
+-----------------+-----------+-------------------------------------+
```

Each message element comprises a number of information items that are
detailed below. The length of each information item is specified in
bytes.

WTP-Info:

Information included in the WTP-Info message element is provided on a
per-WTP basis. So each WTP exchanges one WTP-Info message element.

```
+---------------+----------+----------------+------------------------+
| Item          | Length   | Syntax         | Description            |
+---------------+----------+----------------+------------------------+
| Manufacturer  | 8        | DisplayString  | Manufacturer ID        |
| ID            |          |                |                        |
|               |          |                |                        |
| MAC Address   | 6        | PhyAddress     | WTP MAC Address        |
|               |          |                |                        |
| Firmware      | 8        | DisplayString  | Firmware version of    |
| Version       |          |                | WTP                    |
|               |          |                |                        |
| Start Time    | 4        | TimeTicks      | Starting time of WTP   |
|               |          |                | (UNIX Time)            |
+---------------+----------+----------------+------------------------+
```


Cap-from-WTP:

Information included in the Cap-from-WTP message element is provided
on a per-WTP basis. So each WTP exchanges one Cap-from-WTP message
element.

Item	Length	Syntax	Description
802.11e Cap Length	2	Integer	Length of 802.11e Capabilities
802.11e Capabilities	Variable	OCTETString	802.11e capabilities of WTP. If WTP does not have such capabilities, this field is filled with '0'
802.11i Cap Length	2	Integer	Length of 802.11i Capabilities
802.11i Capabilities	Variable	OCTETString	802.11i capabilities of WTP. If WTP does not have such capabilities,this field is filled with '0'
AuthType	2	OCTETString	Type of authentication mechanism used between WTP and AC

Conf-If-Data

The Conf-If-Data message element relates to the wireless interface.
So a WTP with many interfaces will include corresponding numbers of
Conf-If-Data message elements within its control messages to the AC.
Conf-If-Data message elements are indexed by the If ID information
item.

Item	Length	Syntax	Description
If ID	1	Integer	Denotes identification of a wireless interface
Current Power	1	Integer	Current Power Level ('1' = Max; '2' = 1/2; '3' = 1/4; '4' = 1/8

Item	Length	Syntax	Description
Radio Channel	1	Integer	Radio channel of operation
2Dot4Mode	1	Integer	Interface mode in 2.4GHz. ('1' = IEEE 802.11b; '2' = IEEE 802.11g; '3' = Both)

Conf-WTP-Data

Configuration information is provided on the basis of logical groups such as virtual APs. So there are multiple Conf-WTP-Data message elements to address the many logical groups within a WLAN managed by WiCoP. Conf-WTP-Data message elements are indexed by the BSSID information item.

Item	Length	Syntax	Description
BSSID	6	OCTETString	BSSID
ESSID	32	OCTETString	ESSID
BSSID - TunnelID	32	OCTETString	Mapping for logical groups across BSSID and WiCoP tunnels
Beacon Period	1	Integer	Time interval between Beacon transmissions
DTIM Period	1	Integer	DTIM period of Beacon transmissions
AnyRejectFlag	1	Integer	Flag indicating WTP rejection of any Probe Request within any SSID - ('1' = Rejected; '2' = Not Rejected)
SSID Stealth Flag	1	Integer	Flag indicating inclusion of ESSID within Beacon Frames ('1' = ESSID included; '2' = ESSID not included)

Operation Rate Set	2	Integer	Data rates supported by WTP for terminal being added using 12 bit format for 1.1, 2.2, 3.55, 4.6, 5.9, 6.11, 7.12, 8.18, 9.24, 10.36, 11.48 and 12.54 Mbps
Encryption Type	1	Integer	Encryption Type - （'1' = OFF; '2' = WEP40; '3' = WEP104; '4' = WEP128)
Encryption Key	16	OCTETString	Static Encryption Key

Cap-to-WTP:

Capabilities information is provided on the basis of logical groups such as virtual APs. So there are multiple Cap-to-WTP message elements to address the many logical groups within a WLAN managed by WiCoP. Conf-to-WTP message elements are indexed by the BSSID information item. If logical groups are created by other means, their corresponding identifier is used as the index.

Item	Length	Syntax	Description
BSSID	6	OCTETString	BSSID
802.11e Cap Length	2	Integer	Length of 802.11e Capabilities
802.11e Capabilities	Variable	OCTETString	802.11e capabilities of WTP. If WTP does not have such capabilities, this field is filled with '0'
802.11i Cap Length	2	Integer	Length of 802.11i Capabilities

802.11i	Variable	OCTETString	802.11i capabilities
Capabilities			of WTP. If WTP does
			not have such
			capabilities,this
			field is filled with
			'0'
+--------------+----------+----------------+-----------------------+

QoS-Value:

QoS parameters are assigned for each logical group to address their
respective individual conditions and requirements. QoS-Value message
elements are provided on a per-logical group basis. THey are indexed
by the BSSID information item. If logical groups are created by
other means, their corresponding identifier is used as the index.

Item	Length	Syntax	Description
BSSID	6	OCTETString	BSSID
WTP AC_BE	2	Integer	AC Parameters Record
			AC_BE in WTP
WTP AC_BK	2	Integer	AC Parameters Record
			AC_BK in WTP
WTP AC_VI	2	Integer	AC Parameters Record
			AC_VI in WTP
WTP AC_VO	2	Integer	AC Parameters Record
			AC_VO in WTP
TE AC_BE	2	Integer	AC Parameters Record
			AC_BE in terminals
TE AC_BK	2	Integer	AC Parameters Record
			AC_BK in terminals
TE AC_VI	2	Integer	AC Parameters Record
			AC_VI in terminals
TE AC_VO	2	Integer	AC Parameters Record
			AC_VO in terminals
+--------------+----------+----------------+-----------------------+

Timer-Init-Value:

WiCoP timers are used for the WTP as a whole. So the Timer-Init-
Value message element is provided on a per-WTP basis.

+--------------+----------+---------------+-----------------------+
| Item | Length | Syntax | Description |
+--------------+----------+---------------+-----------------------+
BSSID	6	OCTETString	BSSID
Response	4	Integer	Initial value of
Timer			Response Timer
Active	4	Integer	Initial value of
Presence			Active Presence Timer
Timer			
Feedback	4	Integer	Initial value of
Interval			Feedback Interval
Timer			Timer
+--------------+----------+---------------+-----------------------+

Terminal-Data:

The Terminal-Data message element is applicable for both local-MAC
and split-MAC WTP designs. In the case of local-MAC, Terminal-Data
is sent from WTPs to the AC. In the case of split-MAC, Terminal-Data
is sent from the AC to WTPs. So the direction of usage depends on
the type of WTP at which wireless terminal operations are performed.
Some information items may be optional for use with specific WTP
designs.

+--------------+----------+---------------+-----------------------+
| Item | Length | Syntax | Description |
+--------------+----------+---------------+-----------------------+
BSSID	6	PhyAddress	BSSID in which
			terminal is being
			added
MAC Address	6	PhyAddress	MAC address of
			terminal being added
Association	2	Integer	Association ID of
ID			terminal being added

| Operation Rate Set | 2 | Integer | Data rates supported by WTP for terminal being added using 12 bit format for 1.1, 2.2, 3.55, 4.6, 5.9, 6.11, 7.12, 8.18, 9.24, 10.36, 11.48 and 12.54 Mbps |
| Listen Period | 2 | Integer | Listen period |

BSSID:

The BSSID message element is used to identify logical groups within a WLAN. WiCoP may be extended for other types of logical groups by simply including additional message elements.

Item	Length	Syntax	Description
BSSID	6	PhyAddress	BSSID in which terminal is being added
MAC Address	6	PhyAddress	MAC address of terminal being added

Encryption-Data:

The Encryption-Data message element contains information relevant for configuring security keys at WTPs. It is used in architectures in which the authentication and encryption points are located in distinct WLAN entities.

Item	Length	Syntax	Description
MAC Address	6	PhyAddress	MAC address of terminal
Operation	1	Integer	Operational Mode ('1' = Set Key; '2' = Delete Key)
Key Index	1	Integer	Key Index - valid when Operational Mode = Set Key
Key Flag	1	Integer	Key Flag ('1' = Unicast Key or PTK; '2' = Broadcast Key or GTK) - valid only when Operational Mode = Set Key
Cipher Suit	1	Integer	Encryption Type ('1' = WEP40; '2' = WEP104; '3' = WEP128; '4' = TKIP; '5' = AES) - valid only when Operational Mode = Set Key
Key	32	OCTETString	Key body - valid only when Operational Mode = Set Key

EAP-Frame:

The EAP-Frame message element is used to carry EAP frames used in the configuration and management of the WLAN.

Item	Length	Syntax	Description
MAC Address	6	PhyAddress	MAC address of terminal
EAP	Variable	OCTETString	EAP Frames

Statistics:

Statistics information covers all aspects of WTPs. As such, this
message element is provided on a per-WTP basis. WiCoP messages
containing the Statistics message element simultaneously serve as
keep alive signals between WTPs and AC.

Item	Length	Syntax	Description
OutOctet	4	Counter 32	Octet number of frame WTP transmits
Transmit Count	4	Counter 32	Total number of frames transmitted by WTP
Successful Transmit Count	4	Counter 32	Total number of ACKs received
ACK Failure Count	4	Counter 32	Total number of failed ACKs
InOctets	4	Counter 32	Octet number of frame WTP receives
Receive Count	4	Counter 32	Total number of frames received by WTP
Receive Discard	4	Counter 32	Total number of received frames that are discarded
Retransmission Count	4	Counter 32	Number of WTP retransmission attempts"
Duplicate Receive Count	4	Counter 32	Number of duplicate frames received by WTP
FCS Error Receive Count	4	Counter32	Number to frames received with FCS errors

Unknown Frame Receive Count	4	Counter 32	Number of unknown protocol frames received
Beacon Transmit Count	4	Counter 32	Number of transmitted Beacon frames
Probe Transmit Count	4	Counter 32	Number of transmitted Probe Response frames
Probe Receive Count	4	Counter 32	Number of received Probe Response frames
Decrypt CRC Error Count	4	Counter 32	Number of received frames that cannot decrypt

Interface-Error:

This message element is used to exchange information on error
conditions related to the wireless interface.

Item	Length	Syntax	Description
Interface Index	1	Integer	Interface ID
Error Type	1	Integer	Type of error ('1' = Unrecoverable; '2' = Recoverable)

FROM-Error:

The FROM-Error message element is used to exchange information on
error conditions related to flash ROMs in WTPs or the AC.

+--------------+----------+---------------+-----------------------+
| Item | Length | Syntax | Description |
+--------------+----------+---------------+-----------------------+
FROM Index	1	Integer	FROM ID
Error Type	1	Integer	Type of error ('1' =
			Unrecoverable; '2' =
			Recoverable)
+--------------+----------+---------------+-----------------------+

QoS Capability:

The QoS-Capability message element is used to exchange information
concerning the EDCA and HCCA capabilities of WTPs.

+--------------+----------+---------------+-----------------------+
| Item | Length | Syntax | Description |
+--------------+----------+---------------+-----------------------+
EDCA	1	Integer	EDCA Capability ('1' =
			Capable; '2' = Not
			capable)
HCCA	1	Integer	HCCA Capability ('1' =
			Capable; '2' = Not
			capable)
+--------------+----------+---------------+-----------------------+

TFTP-Data:

This message element is for firmware data from AC to WTPs.

+--------------+----------+---------------+-----------------------+
| Item | Length | Syntax | Description |
+--------------+----------+---------------+-----------------------+
| TFTP Data | Variable | OCTETString | Details of TFTP |
+--------------+----------+---------------+-----------------------+

Result:

The Result message element is used in all WiCoP response messages to
indicate the status of WiCoP request messages.

```
+--------------+----------+---------------+-----------------------+
| Item         | Length   | Syntax        | Description           |
+--------------+----------+---------------+-----------------------+
| Result Code  | 1        | Integer       | '1' = OK; '2' = NG    |
+--------------+----------+---------------+-----------------------+
```

OID:

The OID message element is used for general configuration information
specified by OIDs.

```
+--------------+----------+---------------+-----------------------+
| Item         | Length   | Syntax        | Description           |
+--------------+----------+---------------+-----------------------+
| Length       | 1        | Integer       | Length of OID String  |
|              |          |               | and OID Value         |
|              |          |               |                       |
| OID String   | Variable | OCTETString   | Object Identifier that |
|              |          |               | is assigned according |
|              |          |               | to Basic Encoding     |
|              |          |               | Rules (BER)           |
|              |          |               |                       |
| Value        | Variable | OCTETString   | Value                 |
+--------------+----------+---------------+-----------------------+
```

GTK-Flag:

The GTK-Flag message element is used to inform the WTP on the type of
GTK used and correspondingly how the KeyMIC is to be computer.

```
+--------------+----------+---------------+-----------------------+
| Item         | Length   | Syntax        | Description           |
+--------------+----------+---------------+-----------------------+
| GTK Flag     | 1        | Integer       | Determines the type of |
|              |          |               | GTK ('1' = New; '2' =  |
|              |          |               | Existing)             |
+--------------+----------+---------------+-----------------------+
```

5.2.3 WiCoP Control Message Description

Message: Capabilities
Direction: WTP -> AC
Type: Request

Description: WTPs send Capabilities message upon transitioning from
the Initialization state to Capabilities Exchange state. The message
serves to discover and identify the controlling AC of the WLAN and to
provide it with identification and capabilities information. In the
IEEE 802.11 use-case, the Capabilities message also specifies the
WTP's IEEE 802.11e and IEEE 802.11i features.

TLV: The Capabilities message includes message elements of types 1
and 2.

```
                    +----------------+
                    |  Capabilities  |
                    +----------------+
                    |    WTP-Info    |
                    |                |
                    |  Cap-from-WTP  |
                    +----------------+
```

Message: Capabilities Response
Direction: AC -> WTP
Type: Response

Description: This message is sent by an AC after examining the
compatibility of the WTP and its capabilities. The compatibility is
with respect to the MAC architecture that can be supported by the AC.
If the WTP is determined to be compatible, the Capabilities Response
message also contains information on the capabilities of the AC.

TLV: The Capabilities Response message includes message elements of
types 5 and 17. The Cap-to-WTP message elements are distinguished
based on BSSIDs to represent different logical groups.

```
                 +-----------------------+
                 | Capabilities Response |
                 +-----------------------+
                 |     Cap-to-WTP 1      |
                 |                       |
                 |     Cap-to-WTP ...    |
                 |                       |
                 |     Cap-to-WTP n      |
                 |                       |
                 |        Result         |
                 +-----------------------+
```

Message: Connection
Direction: WTP -> AC

Type: Request

Description: The Connection message initiates the mutual security
association between AC and WTPs. This message carries the first
message of the chosen security protocol. The specific security
mechanism for the authentication is out of scope of the WiCoP
specifications.

TLV: The Connection message includes message elements of type 2.

```
                    +----------------+
                    |   Connection   |
                    +----------------+
                    | Cap-from-WTP   |
                    +---------------+
```

Message: Connection Response
Direction: AC -> WTP
Type: Response

Description: After completion of the security protocol exchange, this
message indicates the result of the WTP-AC security association. If
successful, it also represents the admission of the WTP into the
WLAN.

TLV: Type 17 message element is included.

```
                 +---------------------+
                 | Connection Response |
                 +---------------------+
                 |        Result       |
                 +---------------------+
```

Message: Configuration Request
Direction: WTP -> AC
Type: Request

Description: This message starts the Configuration state for the WTP.
It is a request for configuration information from the WTPs to the
AC.

Message: Configuration Response
Direction: AC -> WTP
Type: Response

Description: This is an acknowledgement for the Configuration Request
message.

TLV: Type 17 message element is included.

```
                 +------------------------+
                 | Configuration Response |
                 +------------------------+
                 |         Result         |
                 +------------------------+
```

Message: Configuration Data
Direction: AC -> WTP
Type: Request

Description: Configuration information including operational
parameters, QoS settings and timer values is sent using the
Configuration Data message. This message is also used for
configuration updates in the Operation state of WiCoP.

TLV: This message includes message elements of type 3, 4, 5, 6 and 7.
The Conf-WTP-Data and QoS-Value message elements are identified by
BSSIDs to denote logical groups, while the Conf-If-Data message
elements are identified by If-IDs to denote multiple wireless radios.

```
                    +---------------------+
                    |  Configuration Data |
                    +---------------------+
                    |   Conf-If-Data 1    |
                    |                     |
                    |   Conf-If-Data ...  |
                    |                     |
                    |    Conf-If-Data n   |
                    |                     |
                    |   Conf-WTP-Data 1   |
                    |                     |
                    |  Conf-WTP-Data ...  |
                    |                     |
                    |   Conf-WTP-Data n   |
                    |                     |
                    |     Cap-to-WTP 1    |
                    |                     |
                    |     Cap-to-WTP ...  |
                    |                     |
                    |     Cap-to-WTP n    |
                    |                     |
                    |     QoS-Value 1     |
                    |                     |
                    |     QoS-Value ...   |
                    |                     |
                    |     QoS-Value n     |
                    |                     |
                    |   Timer-Init-Value  |
                    +---------------------+
```

Message: Configuration Data Response
Direction: WTP -> AC
Type: Response

Description: This is an acknowledgement for the Configuration Data
message.

TLV: Type 17 message element is included.

```
              +-----------------------------+
              | Configuration Data Response |
              +-----------------------------+
              |            Result           |
              +-----------------------------+
```

Message: Configuration Trigger

Direction: AC -> WTP
Type: Request

Description: This message is used to trigger the activation of the
configuration information sent in earlier Configuration messages.

Message: Configuration Trigger Response
Direction: WTP -> AC
Type: Response

Description: This is an acknowledgement of the Configuration Trigger.
This response message is sent before activation of the configuration
information.

TLV: Message elements of type 17 are included.

```
              +--------------------------------+
              | Configuration Trigger Response |
              +--------------------------------+
              |             Result             |
              +--------------------------------+
```


Message: Reset
Direction: AC -> WTP
Type: Request

Description: This message from the AC instructs the WTP to clear
registers and revert to initial conditions.

Message: Reset Response
Direction: WTP -> AC
Type: Response

Description: This is an acknowledgement for the Reset message to the
AC.

TLV: Message elements of type 17 are included.

```
                  +----------------+
                  | Reset Response |
                  +----------------+
                  |     Result     |
                  +----------------+
```

Message: Feedback
Direction: WTP <-> AC
Type: Request

Description:
     WTP: The Feedback message is used to send regular statistics
information to the AC. It also serves as a keepalive indicator used
to update the Active Presence Timer maintained by the AC.
     AC: The Feedback message is used to determine the active state
of WTPs.

TLV: This message includes message elements of type 12.

```
                    +-------------+
                    |   Feedback  |
                    +-------------+
                    | Statistics  |
                    +-------------+
```

Message: Feedback Response
Direction: WTP <-> AC
Type: Response

Description: This is an acknowledgement for Feedback messages.

TLV: Message elements of type 17 are included.

```
                    +-------------------+
                    | Feedback Response |
                    +-------------------+
                    |      Result       |
                    +-------------------+
```

Message: Firmware Download
Direction: AC -> WTP
Type: Request

Description: This message is used to instruct WTPs to update their
firmware. The message element contains information regarding the new
firmware.

TLV: Message elements of type 16 are included.

```
              +-------------------+
              | Firmware Download |
              +-------------------+
              |     TFTP-Data     |
              +-------------------+
```

Message: Firmware Download Response
Direction: WTP -> AC
Type: Request Response

Description: This is an acknowledgement for the Firmware Download
message.

TLV: Message elements of type 17 are included.

```
          +----------------------------+
          | Firmware Download Response |
          +----------------------------+
          |           Result           |
          +----------------------------+
```

Message: Notification
Direction: WTP <-> AC
Type: Request

Description: This message is used to indicate non-periodic events.
It may be sent by either WTPs or the AC. Notification messages
indicate failures, non-periodic changes etc.

TLV: Message elements of types 13 and 14 are included.

```
              +-------------------+
              |   Notification    |
              +-------------------+
              | Interface-Error   |
              |                   |
              |    FROM-Error     |
              +-------------------+
```

Message: Notification Response
Direction: WTP <-> AC
Type: Response

Description: This is an acknowledgement for the Notification message.
It may be followed by Configuration messages to rectify errors.

TLV: Message elements of type 17 are included.

```
              +-----------------------+
              | Notification Response |
              +-----------------------+
              |        Result         |
              +-----------------------+
```

Message: Terminal Addition
Direction: WTP <-> AC
Type: Request

Description: This message may be sent from WTPs or the AC depending
on the WTP type in consideration. In both cases it is sent in
response to an IEEE 802.11 association frame.

For split-MAC WTPs, Terminal Addition is sent from the AC to the WTPs
and includes information on the wireless terminal relevant to the
WTP.

For local-MAC WTPs, Terminal Addition is sent from a WTP to the AC
and contains information on the wireless terminal relevant to the AC.

TLV: Message elements of type 8 are included.

```
              +-------------------+
              | Terminal Addition |
              +-------------------+
              |   Terminal-Data   |
              +-------------------+
```

Message: Terminal Addition Response
Direction: WTP <-> AC
Type: Response

Description: This is an acknowledgement sent from either WTPs or the
AC depending on the WTP type in consideration.

TLV: Message elements of type 17 are included.

```
              +----------------------------+
              | Terminal Addition Response |
              +----------------------------+
              |           Result           |
              +----------------------------+
```

Message: Terminal Deletion
Direction: WTP <-> AC
Type: Request

Description: This message is sent in response to a disconnection of a
wireless terminal. It can be sent from WTPs or the AC. In both
cases, Terminal Deletion instructs the recipient to remove any state
information relating to the specific wireless terminal. The message
is sent in response to an IEEE 802.11 disassociation frame, IEEE
802.11 deauthentication frame or due to the expiration of the Active
Presence Timer.

For split-MAC WTPs, Terminal Deletion is sent from the AC to the
WTPs.

For local-MAC WTPs, Terminal Deletion is sent from the WTPs to the
AC.

TLV: Message elements of type 9 are included.

```
                    +-------------------+
                    | Terminal Deletion |
                    +-------------------+
                    |       BSSID       |
                    +-------------------+
```

Message: Terminal Deletion Response
Direction: WTP <-> AC
Type: Response

Description: This is an acknowledgement sent from either WTPs or the
AC depending on the WiCoP interface.

TLV: Message elements of type 17 are included.

```
                    +---------------------------+
                    | Terminal Addition Response |
                    +---------------------------+
                    |           Result          |
                    +---------------------------+
```

Message: Key Configuration
Direction: AC -> WTP
Type: Request

Description: This message is used when authentication and encryption

points are located in distinct WLAN entities. WiCoP uses it cases
where 'M' = 0 and 'D' = 0 or where 'M' = 1 and 'D' = 1. It is used
to configure security key information from the AC to the WTPs.

TLV: The following message elements are included for Key
Configuration.

```
                    +--------------------+
                    | Key Configuration  |
                    +--------------------+
                    |      GTK-Flag      |
                    |                    |
                    |   Encryption-Data  |
                    |                    |
                    |      EAP-Frame     |
                    +--------------------+
```

Message: Key Configuration Response
Direction: WTP -> AC
Type: Response

Description: This is an acknowledgement for the Key Configuration
message.

TLV: Message elements of type 17 are included.

```
              +----------------------------+
              | Key Configuration Response |
              +----------------------------+
              |           Result           |
              +----------------------------+
```

5.3 WiCoP Data Packet

WiCoP data packets include the WiCoP common header followed by a
payload. Data packets are used to distinguish traffic from control
when both control and data paths are identical. Such a scenario
would involve data traffic of the WTPs traversing the AC. However,
given the diversity of large-scale WLAN deployments, there are
scenarios in which data and control paths are distinct. WiCoP can be
used in both cases.

The WiCoP data packet format is illustrated below in Figure 7
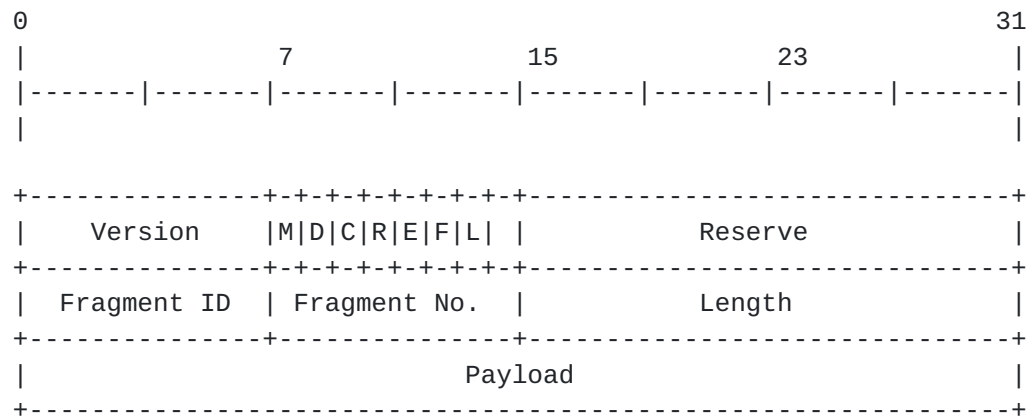together with the WiCoP common header.

```
   0                                                            31
   |                 7              15             23             |
   |-------|-------|-------|-------|-------|-------|-------|-------|
   |                                                             |


   +---------------+-+-+-+-+-+-+-+-+-----------------------------+
   |    Version    |M|D|C|R|E|F|L| |          Reserve            |
   +---------------+-+-+-+-+-+-+-+-+-----------------------------+
   | Fragment ID   | Fragment No.  |           Length            |
   +---------------+---------------+-----------------------------+
   |                          Payload                            |
   +-------------------------------------------------------------+
```


                              Figure 7

5.4 WiCoP Timers

   WiCoP uses a number of timers to determine WLAN status and maintain
   system performance.   Timers are maintained by all WiCoP entities.

5.4.1 Active Presence Timer

   The Active Presence Timer is used by each WiCoP entity - AC and WTPs
   - to verify the presence of each other. The absence of a reply to
   the Feedback message within the expiration of the Active Presence
   Timer indicates the corresponding entity is inactive. Contingency
   operations such as reset are used in this case. The value of the
   Active Presence Timer ranges from 10 to 300 seconds with a default
   value of 30 seconds.

5.4.2 Feedback Interval

   Feedback messages are periodic with the frequency defined by the
   Feedback Interval. The interval is set during WTP configuration. It
   has a value ranging from 1 to 100 seconds and a default value of 10
   seconds.

   The Feedback Interval timer sets the periodicity of WLAN system
   audits. So with this timer, the WLAN controller receives regular
   information on the state of the WLAN and all its WTPs.

5.4.3 Response Timer

   This is a general purpose timer used to limit the elapsed time
   between transmission of a request message and receipt of a
   corresponding response message. The value of this timer ranges from

1 to 3 seconds with a default value of 1 second.

5.4.4 Wireless Connectivity Timer

This timer triggers any changes in wireless connectivity. WiCoP uses
this timer to send Notification and other messages relating to
wireless conditions. It is also used to trigger the disconnection of
mobile terminals without disassociation. The value of the Wireless
Connectivity Timer ranges from 1 minute to 86,400 minutes with a
default value of 10 minutes.

6. **WiCoP Processes**

   The processes of the Wireless LAN Control Protocol are described in
   this section with respect to the operational state in which they
   occur.

6.1 **Initialization**

   The Initialization state represents the initial conditions of WiCoP
   entities. WTPs and ACs in this state are powered on, run hardware
   self-check tests and reset network interfaces.

   State transition: Initialization -> Capabilities Exchange
        WTP: Automatically upon detecting an active network interface
        AC: Upon receiving a Capabilities message from a WTP

6.2 **Capabilities Exchange**

   The Capabilities Exchange state allows WTPs to first find an AC and
   then to exchange capabilities information with it.

   WiCoP is designed to control WLANs with both local-MAC and split-MAC
   WTPs. The differences in their respective functional characteristics
   are determined in this state.

   The WTP first broadcasts a Capabilities message as soon as it
   transitions from its Initialization state. The Capabilities message
   serves to discover ACs and contains information on its identity and
   capabilities.

   The AC receiving the Capabilities message transitions from its
   Initialization state. It examines compatibility with respect to the
   WTP type, its capabilities and responds with an appropriate
   Capabilities Response message.

   The WTP continues to send Capabilities messages at an interval
   specified by the Response Timer until it receives a Capabilities
   Response message from an AC.

   The AC maintains a count of Capabilities messages received from a
   given WTP, which it uses to ignore WTPs after a limit. This is to
   ensure that rogue WTPs which are not compatible with the AC do not
   repeatedly attempt connections. The limit of connection attempts is
   3 within 60 seconds.

   State transition: Capabilities Exchange -> Connection
        WTP: Upon receiving a positive Capabilities Response message
        from an AC

          AC: Upon receiving a Connection Request message from a WTP

6.3 Connection

   The Connection state involves establishing a security infrastructure
   between WTPs and an AC.

   The WTP sends a Connection message to trigger the authentication and
   security mechanism. So this message initiates an IPSec security
   association.

   The AC sends a positive Connection Response message after
   establishment of the security association or a negative Connection
   Response message if an error occurs. The AC also monitors the
   receipt of WiCoP control messages to prevent replay attacks.

   The security association between AC and WTPs covers mutual
   authentication and also protection for integrity, confidentiality and
   modification protection for subsequent traffic exchanges.

   In order to avoid forceful disconnections of legitimate WTPs after a
   successful Connection, the AC ignores Capabilities messages received
   with a previously registered WTP identification.

   State transition: Connection -> Configuration
        WTP: Upon successful establishment of security infrastructure
        marked by sending of a Configuration Request message
        AC: Upon receiving Configuration Request message from WTP after
        successful establishment of security infrastructure

   State transition: Connection -> Capabilities Exchange
        WTP: Upon expiry of WTP Response Timer before receipt of
        positive Connection Response message from AC or upon receipt of
        negative Connection Response message
        AC: Upon expiry of AC Response Timer before receipt of
        Configuration Request message from WTP

6.4 Configuration

   The Configuration state in one in which relatively long-term
   operational parameters such as those for identification and logical
   groups, are exchanged. These parameters are based on previously
   exchanged capabilities information and network policies.

   The WTP sends a Configuration Request message to the AC.

   The AC first acknowledges the WTP's Configuration Request, after
   which it sends appropriate configuration information in subsequent

Configuration Data messages. WiCoP includes MIB objectives as
message elements in some Configuration Data messages so as to
simplify WTP configuration.

The WTP acknowledges Configuration Data messages individually or en
bloc with Configuration Data Response messages. The Response timer
is maintained at both WTP and AC to track the exchanges.

The AC also establishes relevant processing schedules according to
the WTP's architecture design. For example, for split-MAC WTPs, the
AC arranges its processing schedule to parse IEEE 802.11 control and
management messages while for local-MAC WTPs, the AC arranges
schedules processing so as to bypass parsing of IEEE 802.11
management messages.

The AC sends a Configure Trigger message after sending all relevant
configuration information to the WTP.

The WTP acknowledges a Configure Trigger message with a Configure
Trigger Response message before activating the previously exchanged
configuration parameters.

In order to avoid forceful disconnections of legitimate WTPs after
successful Configuration, the AC ignores Capabilities messages
received with a previously registered WTP identification.

State transition: Configuration -> Operation
    WTP: After receiving final Configuration Data message from AC
    marked by receipt of a Configure Trigger message from the AC
    AC: Upon receiving acknowledgement for Configure Trigger message
    marked by receipt of Configure Trigger Response message from WTP

State transition: Configuration -> Capabilities Exchange
    WTP: Upon expiry of WTP Response Timer before receipt of
    Configure Trigger message from AC
    AC: Upon expiry of AC Response Timer before receipt of Configure
    Data Response message or Configure Trigger Response message

The following describe major configuration aspects of WiCoP.

6.4.1 Logical Groups

Configuration Data messages are used to establish logical groups in
the WLAN and also to separate traffic among them. The logical groups
are established based on network administrative policies and other
external considerations. In the IEEE 802.11 use-case, logical groups
are established with BSSID-based virtual APs and are separated over
the WiCoP interface using tunnels.

The AC assigns particular BSSIDs of the WTP to specific VLAN tunnels.
This assignment is specified to the WTP using the BSSID-TunnelID
parameter in the Configuration Data message. The logical group
mapping therefore works across the wireless and WiCoP interfaces.

The WTP then identifies the specified BSSID and VLAN tunnel as
corresponding to one logical group. It creates internal state such
that traffic belonging to the logical group is kept distinct from
that of other logical groups.

The AC and WTP also use distinct VLAN tunnels for data and control
traffic. The 'C' field in the WiCoP header is used to distinguish
and assign WiCoP packets to particular data and control VLAN tunnels.

6.4.2 Resource Control

The AC sends QoS information using QoS-Value message elements in
Configuration Data messages. The QoS-Value message element contains
values for EDCA and HCCA parameters. This information is specified
for each of the logical groups. In the IEEE 802.11 use-case, QoS-
Value message elements are specified for each BSSID.

The WTP configures QoS parameters locally and also forwards relevant
settings to wireless terminals in appropriate encapsulations. In the
IEEE 802.11 use-case, QoS parameters are sent to wireless terminals
in corresponding Beacon or Probe Response frames.

6.5 Operation

This is the active operation state of the WLAN in which short-term
dynamics are examined.

The WTP begins operations according to the operational parameters
exchanged in the previous Configuration state.

The AC monitors WTPs according to network administrative policies and
configurations.

In order to avoid forceful disconnections of legitimate WTPs after
successful Operation setup, the AC ignores Capabilities messages
received with a previously registered WTP identification.

State transition: Operation -> Capabilities Exchange
     WTP: Upon expiry of WTP Active Presence Timer before receipt of
     Feedback Response message from AC
     AC: Upon expiry of AC Active Presence Timer before receipt of
     Feedback message from WTP

State transition: Operation -> Initialization
     WTP: Upon receipt of Reset message from AC
     AC: Upon receipt of Reset Response message from WTP

The following describe major operation aspects of WiCoP.

6.5.1 Updates

The dynamic nature of WLAN systems requires regular updates to
network operations.

The AC sends additional configuration information in the
Configuration Data messages. This is applicable to establishment of
new logical groups, changes to existing logical groups, changes in
QoS settings etc. Configuration information is followed by a
Configure Trigger message.

The WTP sends a Configure Trigger Response before activating the
additional configuration information.

Configuration updates can be used to clear statistics information by
reflecting initial values.

An extreme case of configuration update involves use of the Reset
message from the AC, which instructs the WTP to revert to initial
conditions. The WTP replies with a Reset Response message before
reverting to its initial state.

6.5.2 Feedback and Statistics

The Operation state also sees regular feedback being sent by WTPs to
the AC.

The WTP sends Feedback messages to indicate various statistics and
congestion condition information. Feedback also includes information
on the state of the WTP and wireless medium such as queue levels and
channel interference. Feedback messages are sent with a frequency
defined by the Feedback Interval. In addition to statistics, the
Feedback message also serves as a WTP keepalive indicator to the AC.
So Feedback messages combine statistics information together with WTP
status information.

The AC monitors Feedback messages for their statistics value and
implicit indication of WTP activity. The AC also tracks the state of
congestion at wireless terminals and WTPs. This information enables
the AC to adapt its downstream transmissions, such as scheduling
transmission away from congested WTPs, so as to relieve congestion.

The AC additionally uses the Feedback message to randomly determine
the active state of WTPs. An active WTP replies with a corresponding
Feedback Response message.

6.5.3 Non-periodic Events

The WTP and AC use the Notification message for non-periodic events.
They send Notification messages to indicate error conditions or
drastic changes in congestion state.

The recipient of the Notification message acknowledges with a
Notification Response message. The response may contain information
on rectifying the error or may simply be an acknowledgement of the
Notification.

6.5.4 Firmware Trigger

The AC sends a Firmware Download message to update firmware at WTPs.
The Firmware Download message contains TFTP information, which the
WTP uses to refresh its firmware. This is used when a new version of
firmware is available for the WTPs.

The WTP acknowledges new firmware with a Firmware Download Response
message after which it is activated.

6.5.5 Wireless Terminal Management

The Operation state of WiCoP also involves configuration of WTPs and
the AC with wireless terminal specific information.

Here the Terminal Addition message is used in response to a new
wireless terminal entering the WLAN. This message may be sent by
either the WTPs or the AC depending on the WiCoP interface being
used. The recipient of this message replies with the Terminal
Addition Response message.

The Terminal Deletion message is used when a wireless terminal leaves
the WLAN. This is used to delete state information that was
maintained by either the WTPs or the AC. It is acknowledged with the
Terminal Deletion Response message.

Figure 8 below illustrates the exchange of Terminal Addition and
Terminal Deletion messages for both local-MAC and split-MAC based
WiCoP interfaces.

Here the WiCoP Terminal Addition message is triggered as a response
to IEEE 802.11 Association message. In the case of local-MAC
architecture, the WTP sends the message to the AC. However, in the

split-MAC architecture, Terminal Addition is sent from AC to the WTP.

```
   +----------+            +--------------+            +------+
   | Terminal |            | Local-MAC WTP |            |  AC  |
   +----------+            +--------------+            +------+
        |                         |                         |
        |                         |                         |
        | IEEE 802.11 Association |         WiCoP           |
        |------------------------>|     Terminal Addition   |
        |                         |=========================>|
        |                         |                         |
        |                         |      WiCoP Terminal     |
        |                         |<========================|
        | IEEE 802.11 Association |   Addition Response     |
        |<------------------------|                         |
        |        Response         |                         |
        |                         |                         |
        |                         |                         |
        |                                                   |
        |                                                   |
        |                                                   |
        |            +---------------+                      |
        |            | Split-MAC WTP |                      |
        |            +---------------+                      |
        |                    |                              |
        |                    |                              |
        | IEEE 802.11 Association |                         |
        |------------------------>|                         |
        |                    |  IEEE 802.11 Association     |
        |                    |=========================>|
        |                    |       (Over WiCoP)          |
        |                    |                              |
        |                    |                              |
        |                    |          WiCoP              |
        |                    |     Terminal Addition       |
        |                    |<========================|
        |                    |                              |
        |                    |                              |
        |                    |       WiCoP Terminal        |
        |                    |=========================>|
        |                    |     Addition Response       |
        |                    |                              |
        |                    |                              |
        |                    |  IEEE 802.11 Association     |
        |                    |<========================|
        |                    |    Response (Over WiCoP)    |
        | IEEE 802.11 Association |                         |
        |<------------------------|                         |
        |         Response        |                         |
        |                    |                              |
```
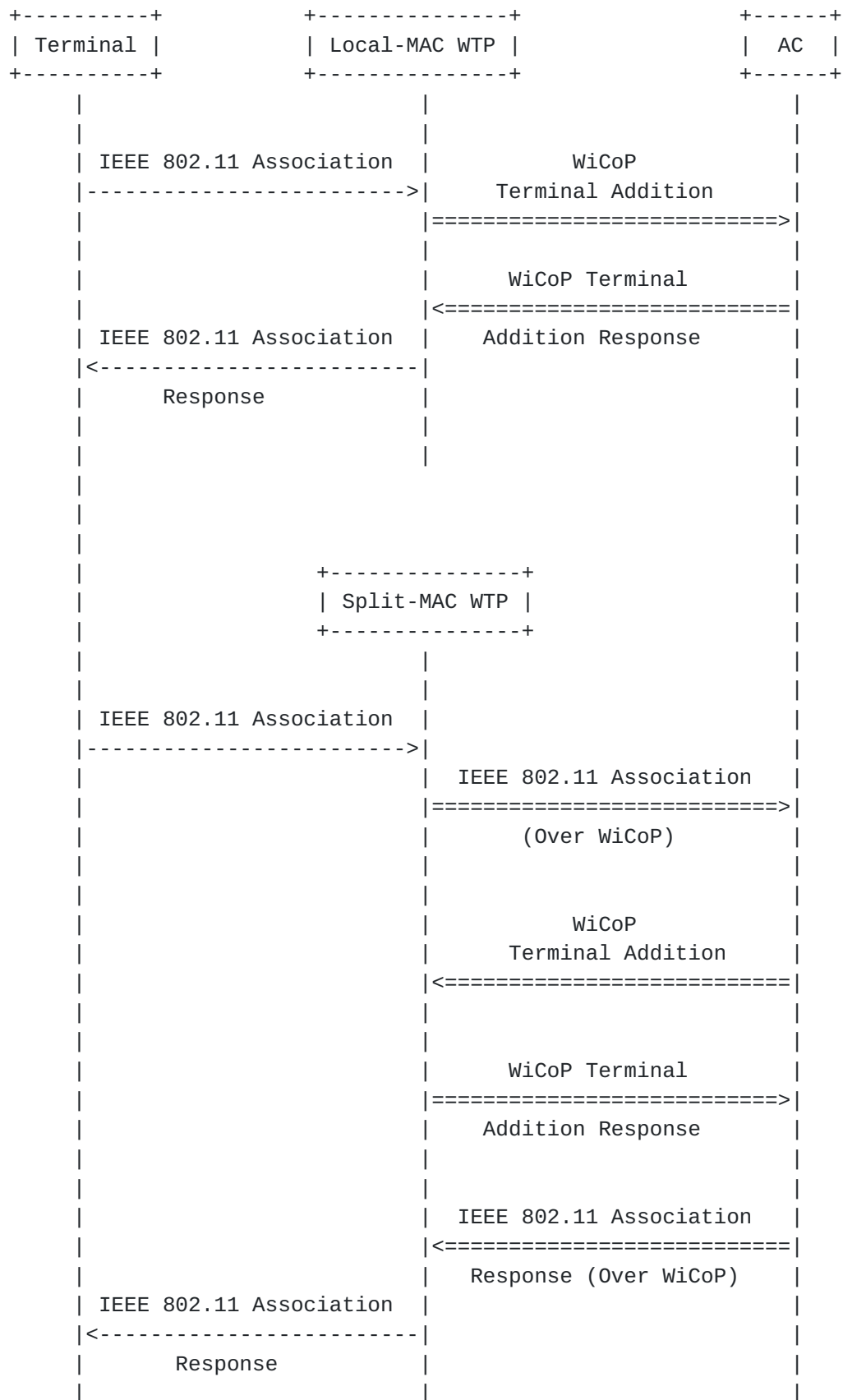
Figure 8

6.5.6 **Key Configuration**

   One of the differences between split-MAC and local-MAC WTPs is the
   location of the over-the-air encryption. Some split-MAC and local-
   MAC WTPs perform encryption locally while others leave it to the AC.
   WiCoP accommodates these differences by enabling security key
   configuration in those cases where encryption is performed at the
   WTP. The encryption setup process is therefore contingent on the
   WiCoP protocol interface.

   When dynamic WEP is used, the WiCoP Key Configuration message is used
   to notify WTPs of encryption keys for each associated wireless
   terminal. Here, the EAPoL Key frame is encapsulated in the Key
   Configuration message and sent to a WTP. Upon receiving the Key
   Configuration message, the WTP sets the encryption key in its local
   security table, decapsulates the EAPOL Key frame and forwards it to
   the wireless terminal. This is illustrated in Figure 9.

```
 +----------+              +-----+               +------+
 | Terminal |              | WTP |               |  AC  |
 +----------+              +-----+               +------+
      |                       |                     |
      |              802.1x Authentication         |
      |<=========================================>|
      |                       |                     |
      |                       |                     |
    PMK                       |                    PMK
      |                       |                     |
      |                       |                     |
      |<----------------------|<========================|
      |      EAPoL Packet     |      WiCoP Control Packet   |
      |                       |        (Key Configuration)  |
      |                       |      | +----------------------+
      |                       |      \|- Encryption-Data      |
      |                       |      |     Unicast-Key        |
    Set                    Receive   |- EAP-Frame             |
  Unicast-Key            Unicast-Key |    Key Signature       |
      |                       |      +----------------------+
      |                       |                     |
      |                       |=========================>|
      |                       |      WiCoP Control Packet   |
      |                       |        (Key Configuration   |
      |                       |         Response )          |
      |                       |                     |
      |                       |                     |
      |                       |                     |
      |                       |                     |
      |<----------------------|<========================|
      |      EAPoL Packet     |      WiCoP Control Packet   |
      |                       |        (Key Configuration)  |
      |                       |      | +----------------------+
      |                       |      \|- Encryption-Data      |
      |                       |      |     Broadcast-Key      |
    Set                    Receive   |- EAP-Frame             |
  Broadcast-Key        Broadcast-Key |    Key Signature       |
      |                       |      |    Broadcast Key       |
      |                       |      +----------------------+
      |                       |                     |
      |                       |=========================>|
      |                       |      WiCoP Control Packet   |
      |                       |        (Key Configuration   |
      |                       |         Response )          |
```
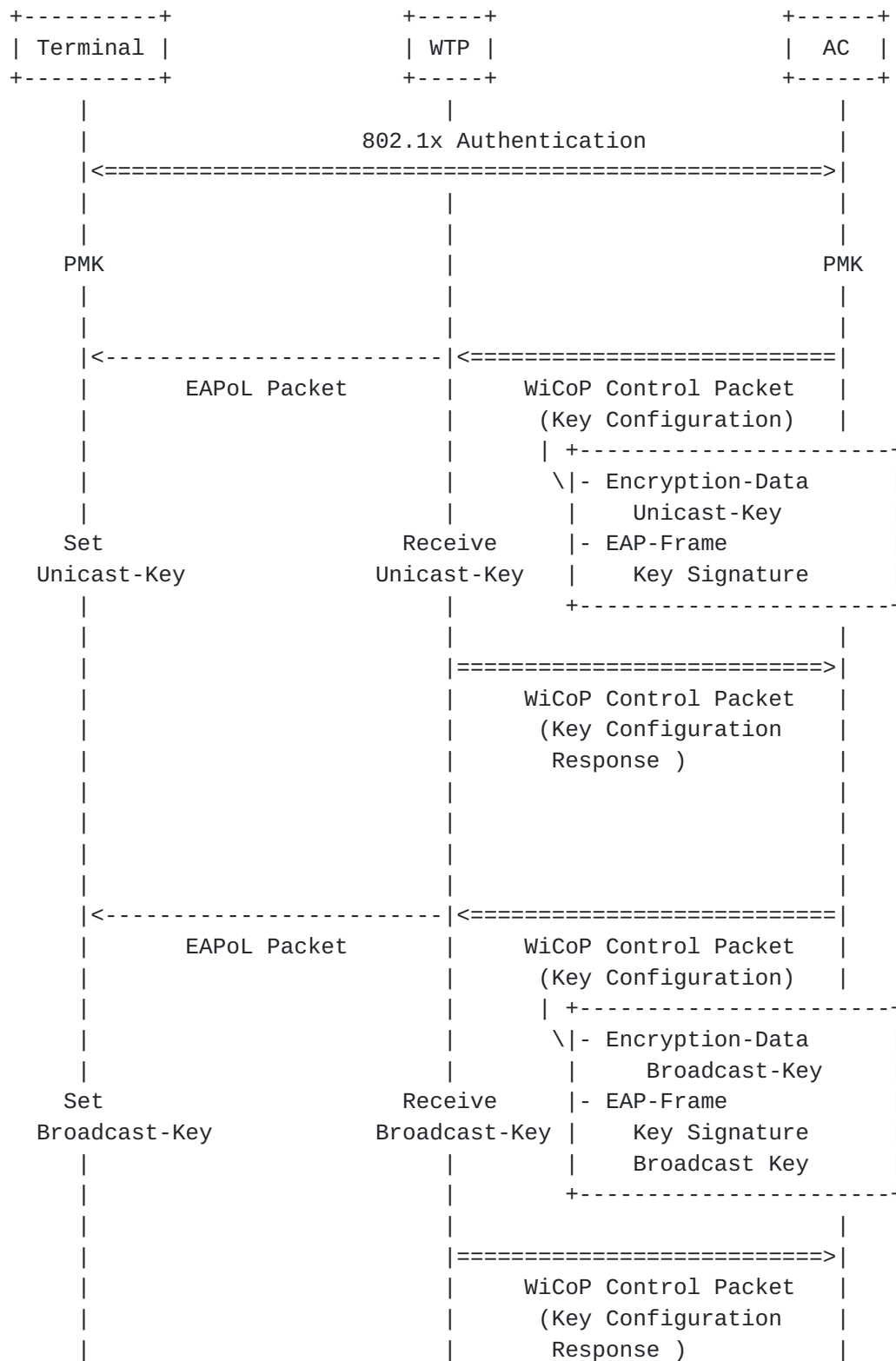
                              Figure 9

   When WPA or IEEE 802.11i is used in WLAN architectures in which the

authenticator is located at the AC and encryption points at WTPs, the
exchanges of the 4-way handshake are managed distinctly. This is
because the AC is no longer in a position to calculate the KeyMIC as
it is not aware of the KeyRSC sequence counter. So here, WiCoP Key
Configuration message is used to transport the 3rd message of the
4-way handshake - containing the EAPoL-Key - with unassigned KeyRSC
and KeyMIC fields. When the WTP receives the WiCoP Key Configuration
message, it first assigns the sequence number value to the KeyRSC
field. Then, the WTP calculates the KeyMIC value using the PTK and
KeyRSC. So the WiCoP Key Configuration message allows the KeyMIC to
be calculated at the WTPs instead of the AC. The GTK-Flag message
element is used to deterermine how the KeyMIC is calculated - in case
of new GTK, KeyMIC is computed with a KeyRSC value of 0 and in case
of an existing GTK, KeyMIC is computed with a KeyRSC value
corresponding to the actual counter.

Figure 10 illustrates this case where the WiCoP common header is
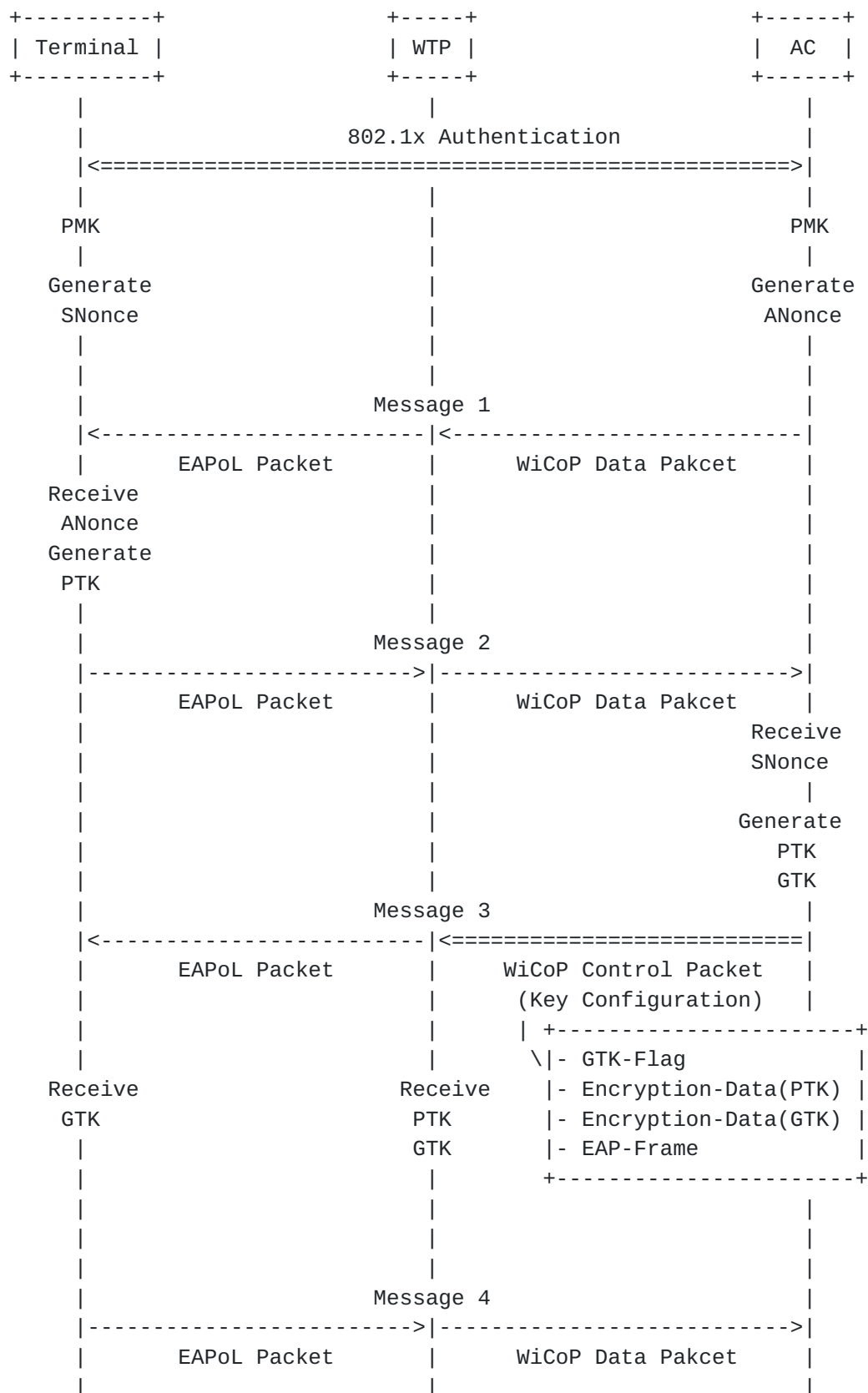either 'M' = 0 and 'D' = 0 or 'M' = 1 and 'D' = 1.

```
  +----------+              +-----+                +------+
  | Terminal |              | WTP |                | AC   |
  +----------+              +-----+                +------+
       |                       |                      |
       |              802.1x Authentication           |
       |<===========================================>|
       |                       |                      |
     PMK                       |                     PMK
       |                       |                      |
     Generate                  |                    Generate
      SNonce                   |                     ANonce
       |                       |                      |
       |                       |                      |
       |                Message 1                     |
       |<----------------------|<---------------------|
       |       EAPoL Packet    |    WiCoP Data Pakcet |
     Receive                   |                      |
      ANonce                   |                      |
     Generate                  |                      |
      PTK                      |                      |
       |                       |                      |
       |                Message 2                     |
       |---------------------->|--------------------->|
       |       EAPoL Packet    |    WiCoP Data Pakcet |
       |                       |                    Receive
       |                       |                     SNonce
       |                       |                      |
       |                       |                    Generate
       |                       |                      PTK
       |                       |                      GTK
       |                Message 3                     |
       |<----------------------|<=====================|
       |       EAPoL Packet    |    WiCoP Control Packet
       |                       |    (Key Configuration)  |
       |                       |      | +----------------------+
       |                       |      \|- GTK-Flag            |
     Receive              Receive     |- Encryption-Data(PTK) |
      GTK                   PTK       |- Encryption-Data(GTK) |
       |                    GTK       |- EAP-Frame            |
       |                       |      +----------------------+
       |                       |                      |
       |                       |                      |
       |                       |                      |
       |                Message 4                     |
       |---------------------->|--------------------->|
       |       EAPoL Packet    |    WiCoP Data Pakcet |
       |                       |                      |
```

Figure 10

The 1st, 2nd and 4th messages of the 4-way handshake are transported
in WiCoP data packets that are assigned priorities similar to that of
WiCoP control packets.

Similarly, for the group key handshake in WPA and IEEE 802.11i, the
1st message of the handshake is transported using the WiCoP Key
Configuration message with unassigned KeyRSC. The WTP again assigns
the sequence number value to the KeyRSC and then calculates the
KeyMIC. The 2nd message of the handshake however is transported in
WiCoP data packets with priorities similar to that of WiCoP control
packets. This is illustrated in Figure 11.

```
+----------+                 +-----+                 +------+
| Terminal |                 | WTP |                 |  AC  |
+----------+                 +-----+                 +------+
     |                          |                       |
     |                      Message 1                   |
     |<------------------------|<======================|
     |        EAPoL Packet      |    WiCoP Control Packet   |
     |                          |      (Key Configuration)   |
     |                          |    | +----------------------+
     |                          |    \|- GTK-Flag            |
   Receive                    Receive |- Encryption-Data(GTK) |
    GTK                         GTK    |- EAP-Frame            |
     |                          |    +----------------------+
     |                          |                       |
     |                          |                       |
     |                          |                       |
     |                          |                       |
     |                      Message 2                   |
     |------------------------>|---------------------------->|
     |        EAPoL Packet      |    WiCoP Data Pakcet       |
     |                          |                       |
```
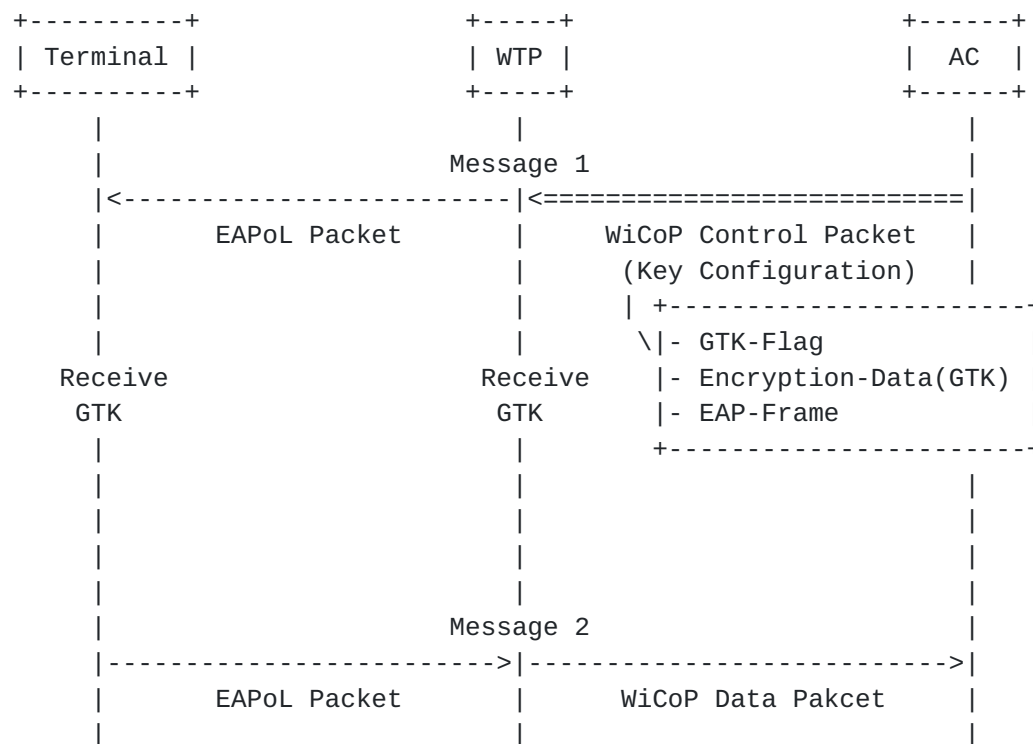
Figure 11

The Key Configuration Response message is used by the WTP to notify
the AC of the encryption setup process.

7. WiCoP Performance

   WiCoP is an efficient protocol. This section illustrates various
   examples of its efficiency.

7.1 Operational Efficiency

   The fact that WiCoP requires a single operation to distinguish and
   manage WTPs of different designs makes it operationally efficient.
   Because WiCoP assigns dedicated classification bits in the common
   header, an AC needs to parse incoming packets only once to determine
   the particular manner in which it is to be processed. Without the
   dedicated classifications in the common header, an AC would have to
   perform a lookup after parsing every incoming packet, which would
   result in delaying processing. The scale and sensitivity of large-
   scale deployments require that WLAN control protocols be efficient in
   operation.

7.2 Semantic Efficiency

   In certain cases, WiCoP combines utilities in a single operation.
   One particular case is that of statistics and activity feedback.
   Here, WTPs send regularly send a single Feedback message containing
   statistics and other state information, which also acts as an
   implicit keepalive mechanism. This helps to reduce the number of
   message exchanges and also simplifies protocol implementation.
   Similarly, the Capabilities messages serves the purpose of finding
   ACs and also informing them of WTP capabilities and design.

8. **Summary and Conclusion**

   The Wireless LAN Control Protocol presents a solution for managing
   large-scale WLANs with diverse elements. It addresses the challenges
   presented in the CAPWAP Problem Statement [I-D.ietf-capwap-problem-
   statement] and realizes the requirements of the CAPWAP Objectives
   [I-D.ietf-capwap-objectives].

   WiCoP enables integral control of split-MAC and local-MAC WTPs by
   defining appropriate differentiators within the protocol message
   exchanges and processes. It addresses architecture designs in which
   the authenticator and encryption points are located on distinct
   entities. And in doing so, WiCoP realizes the interoperability
   objective and its benefits.

   WiCoP also addresses shared WLAN deployments by configuring and
   managing WTPs on a logical group basis. It is further provisioned to
   separate control and data traffic within WLANs. So the protocol
   addresses the objectives of logical groups and traffic separation.

   Overall, the specifications presented in this document allows for an
   effective WLAN control and provisioning protocol.

9. **Security Considerations**

   Illegitimate WTPs and ACs pose a significant threat to WLAN security.
   This can be mitigated by requiring all WiCoP entities to be mutually
   authenticated before initiating critical protocol exchanges. WiCoP
   includes a trigger for a suitable authentication mechanism. This is
   to accommodate different security mechanism that may be used between
   WTPs and AC depending on the nature of the deployment.

   In extension to mutual authentication, the subsequent exchange of
   protocol information between WTPs and AC need to be protected. The
   exchanges have to be protected against alterations of any sort and
   DoS attacks. Also, the information should not be accessible to any
   third party. Encryption of protocol exchanges is therefore
   necessary. WiCoP includes appropriate procedures to select and
   establish a security association between WTPs and AC in the Connection
   state.

   Architecture designs in which authentication is performed at the AC
   and encryption at the WTPs can be exposed to the threat of replay
   attacks. Since the AC will not be aware of the exact value of the
   sequence counter, it will not make the corresponding assignment
   within the 4-way handshake. This leaves the wireless terminal to
   accept all incoming frames including illegitimate frames as it cannot
   verify the sequence counter value. Such a threat needs to protected
   against by allowing the WTP to assign the correct value of the
   sequence counter. WiCoP accomplishes this by sending the 3rd message
   of the 4-way handshake within a control message to the WTP, which
   then updates the sequence counter field before forwarding to the
   wireless terminals.

   Another issue to consider is that of rogue WTPs using identifiers
   similar to that of legitimate WTPs. In such instances, a rogue WTP
   can send a Capabilities message to the AC thereby causing
   disconnection of the existing legitimate WTP of the same identifier.
   It is important for the AC to ignore Capabilities messages received
   with existing identifiers.

10. **References**

   [I-D.ietf-capwap-arch]
              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.

   [I-D.ietf-capwap-objectives]
              Govindan, S., "Objectives for Control and Provisioning of

                    Wireless Access Points (CAPWAP)",
                    draft-ietf-capwap-objectives-03 (work in progress),
                    June 2005.

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

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
                    Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

   Satoshi Iino
   Panasonic Mobile Communications
   600, Saedo-cho
   Tsuzuki-ku
   Yokohama 224 8539
   Japan

   Phone: +81 45 938 3789
   Email: iino.satoshi@jp.panasonic.com

   Saravanan Govindan
   Panasonic Singapore Laboratories
   Block 1022, Tai Seng Industrial Estate
   #06-3530, Tai Seng Avenue
   Singapore 534 415
   Singapore

   Phone: +65 6550 5441
   Email: saravanan.govindan@sg.panasonic.com

   Mikihito Sugiura
   Panasonic Mobile Communications
   600, Saedo-cho
   Tsuzuki-ku
   Yokohama 224 8539
   Japan

   Phone: +81 45 938 3789
   Email: sugiura.mikihito@jp.panasonic.com

   Hong Cheng
   Panasonic Singapore Laboratories
   Block 1022, Tai Seng Industrial Estate
   #06-3530, Tai Seng Avenue
   Singapore 534 415
   Singapore

   Phone: +65 6550 5447
   Email: hong.cheng@sg.panasonic.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment