OPSAWG
Internet-Draft
Updates: 5416 (if approved)
Intended status: Standards Track
Expires: August 18, 2014

Y. Chen
D. Liu
H. Deng
China Mobile
Lei. Zhu
Huawei

February 14, 2014

# CAPWAP Extension for 802.11n and Power/channel Autoconfiguration
# draft-ietf-opsawg-capwap-extension-02

## Abstract

CAPWAP binding for 802.11 is specified by RFC5416 and it was based on IEEE 802-11.2007 standard. After RFC5416 was published in 2009, there were several new amendments of 802.11 have been published. 802.11n is one of those amendments and it has been widely used in real deployment. This document extends the CAPWAP binding for 802.11 to support 802.11n and also defines a power and channel auto configuration extension.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on August 18, 2014.

## Copyright Notice

Table of Contents



## 1. Introduction

IEEE 802.11n standard was published in 2009 and it is an amendment to the IEEE 802.11-2007 standard. The maximum data rate increases to 600Mbps. In the physical layer, 802.11n use OFDM and MIMO to achieve the high throughput. 802.11n also use multiple antennas to form antenna array which can be dynamically adjusted to improve the signal strength and extend the coverage.

There are several capabilities of 802.11n need to be supported by CAPWAP control message, such as radio capability, radio configuration and station information etc. This document specifies the 802.11n and power/channel auto-configuration extensions for CAPWAP.

For the AC/WTP that does not support the extensions defined by this document, it can simply ignore the extensions and will not cause any incompatible issue.

## 2. 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 [RFC2119].

## 3. Abbreviations

AC: Access Controller
A-MSDU:Aggregate MAC Service Data Unit
A-MPDU:Aggregate MAC Protocol Data Unit
MIMO: Multi-input Multi-output
MSDU: MAC Service Data Unit
MPDU: MAC Protocol Data Unit
MCS: Maximum Modulation and Coding Scheme
OFDM: Orthogonal Frequency-Division Multiplexing
WTP: Wireless Termination Points.

## 4. CAPWAP 802.11n Support

[IEEE-802.11.2009] standard was published in 2009 and it is an amendment of the IEEE 802.11-2007 standard to improve throughput. The maximum data rate increases to 600Mbps. In the physical layer, 802.11n use OFDM and MIMO to achieve high throughput. 802.11n use multiple antennas to form antenna array which can be dynamically adjusted to improve the signal strength and extend the coverage.

802.11n support three modes of channel usage: 20MHz mode, 40MHz mode and mixed mode. 802.11n has a new feature called channel binding. It can bind two adjacent 20MHz channel to one 40MHz channel to improve the throughput.If using 40MHz channel configuration there will be only one non-overlapping channel in 2.4GHz. In the large scale deployment scenario, operator need to use 20MHz channel configuration in 2.4GHz to allow more non-overlapping channels.

In MAC layer, a new feature of 802.11n is Short Guard Interval(GI). 802.11a/g uses 800ns guard interval between the adjacent information symbols. In 802.11n, the GI can be configured to 400nm under good wireless condition.

Another feature in 802.11 MAC layer is Block ACK. 802.11n can use one ACK frame to acknowledge several MPDU receiving event.

CAPWAP needs to be extended to support the above new 802.11n features. For example, CAPWAP should allow the access controller to know the supported 802.11n features of WTP and the access controller should be able to configure the different channel binding modes for WTP.

### 4.1. CAPWAP Extension for 802.11n Support

There are three 802.11n features need to be supported by CAPWAP 802.11 binding: 802.11n radio capability, 802.11n radio configuration and station information. This section defines the extension of current CAPWAP 802.11 binding to support 802.11n features.

#### 4.1.1. 802.11n Radio Capability Information

[RFC5416] defines IEEE 802.11 binding for CAPWAP protocol. It defines IEEE 802.11 Information Element (Type 1029) which is used to communicate any IE defined in IEEE 802.11 protocol. The detail definition of IEEE 802.11 Information Element is in section 6.6 of [RFC5416]. The IEEE 802.11 HT information element is defined in section 8.4.2.58 of [IEEE-802.11.2012]. It contains the 802.11n radio capability information. This document specifies use of the IEEE 802.11 Information Element (Type 1029) transporting the IEEE 802.11 HT information element to carry the 802.11n radio capability information. 802.11n radio capability information MAY be included in the CAPWAP Configuration Status Request/Response messages.

#### 4.1.2. 802.11n Radio Configuration Message Element

The 802.11n Radio Configuration Information Element message element is used by the AC to configure a Radio on the WTP and by the WTP to deliver its radio configuration to the AC. The 802.11n Radio Configuration Information Element is defined in figure 1. 802.11n Radio Configuration Message Element MAY be included in the CAPWAP Configuration Update Request/Response message.

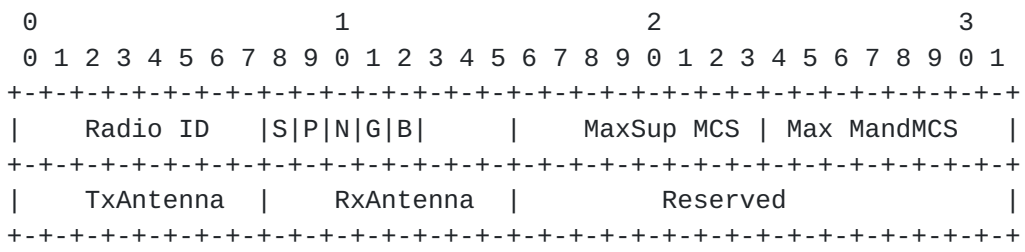


Figure 1: 802.11n Radio Configuration Message Element

Type: TBD for 802.11n Radio Configuration Message Element.

Length: 16.

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

S bit: A-MSDU Cfg: Enable/disable Aggregate MAC Service Data Unit (A-MSDU). Set to 0 if disabled. Set to 1 if enabled.

P bit: A-MPDU Cfg: Enable/disable Aggregate MAC Protocol Data Unit (A-MPDU). Set to 0 if disabled. Set to 1 if enabled.

N bit: 11n Only Cfg: Whether to allow only 11n user access. Set to 0 if allow non-802.11n user access. Set to 1 if do not allow non-802.11n user access.

G bit: Short GI Cfg: Set to 0 if disabled. Set to 1 if enabled.

B bit: Bandwidth Cfg: Bandwidth binding mode. Set to 0 if 40MHz binding mode. Set to 1 if 20MHz binding mode.

MaxSup MCS: Maximum Modulation and Coding Scheme (MCS) index. It indicates the maximum MCS index that the WTP or the STA can support.

Max Mandatory MCS: Maximum Mandatory Modulation and Coding Scheme (MCS) index. Mandatory rates must be supported by the WTP and the STA that want to associate with the WTP.

TxAntenna: Transmitting antenna configuration. Each TxAntenna bit represent a certain number of antennas. Set to 1 if enabled, set to 0 if disabled.

RxAntenna: Receiving antenna configuration. Each RxAntenna bit represent a certain number of antennas. Set to 1 if enabled, set to 0 if disabled.

The detail definition of TxAntenna/RxAntenna is as follows:

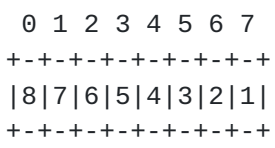


Figure 2: Definition of TxAntenna/RxAntenna

Each bit when enabled will represent the number of antennas correspondent to that bit. For example, when the first bit is enabled,it represents 8 antennas.

### 4.1.3. 802.11n Station Information

The 802.11n Station Information message element is used to deliver IEEE 802.11n station policy from the AC to the WTP. The definition of the 802.11n Station Information message element is in figure 3. 802.11n Station Information MAY be included in the CAPWAP Station Configuration Request message.

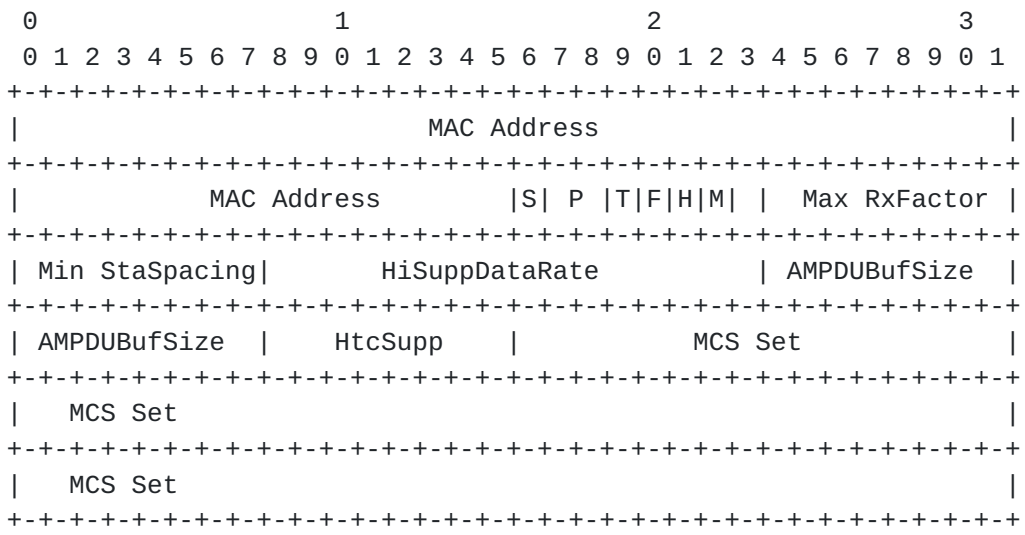


Figure 3: 802.11n Station Information

Type: TBD for 802.11 Station Information.

Length: 24.

S bit: SupChanl width: Supporting bandwidth mode. 0x00: 20MHz bandwidth mode. 0x01: 40MHz bandwidth binding mode.

P flag: Power Save: 0x00: Static power saving mode. 0x01: Dynamic power saving mode. 0x03: Do not support power saving mode.

T bit: ShortGi20: Whether support short GI in 20MHz bandwidth mode. 0x00: Do not support short GI. ox01: Support short GI.

F bit: ShortGi40: Whether support short GI in 40MHz bandwidth mode. 0x00: Do not support short GI. ox01: Support short GI.

H bit: HtDelyBlkack: Whether block Ack support delay mode. 0x00: Do not support delay mode. 0x01: Support delay mode.

M bit: Max Amsdu: The maximal AMSDU length. 0x00: 3839 bytes. 0x01: 7935 bytes.

Max RxFactor: The maximal receiving AMPDU factor.

Min StaSpacing: Minimum MPDU Start Spacing.

HiSuppDataRate: Maximal transmission speed (Mbps).

AMPDUBufSize: AMPDU buffer size.

HtcSupp: Whether the packet have HT header.

MCS Set: The MCS bitmap that the station supports.

## 5. Power and Channel Autoconfiguration

Power and channel autoconfiguration could avoid potential radio interference and improve the WLAN performance. In general, the auto-configuration of radio power and channel could occur at two stages: when the WTP power on or during the WTP running time.

### 5.1. Channel Autoconfiguration When WTP Power On

When the WTP is power-on, it is of necessity to configure a proper channel to the WTP in order to achieve best status of radio links. IEEE 802.11 Direct Sequence Control elements or IEEE 802.11 OFDM Control element defined in RFC5416 SHOULD be carried in the Configure Status Response message to offer WTP a channel at this stage. If those information element is zero, the WTP will need to determine its channel by itself, otherwise the WTP SHOULD be configured according to the provided information element.

When the WTP determines its own channel configuration, it should first scan the channel information, then determine which channel it will work on and form a channel quality scan report. The channel quality report will be sent to the AC using WTP Event Request message by the WTP.

AC will determine whether to change the channel configuration based on the received channel quality report. The AC can use IEEE 802.11 Direct Sequence Control or IEEE 802.11 OFDM Control information element carried by the configure Update Request message to configure a new channel for the WTP.

## 5.2. Power Configuration When WTP Power On

IEEE 802.11 Tx Power information element is used by the AC to control the transmission power of the WTP. The 802.11 Tx Power information element is carried in the Configure Status Response message or in the Configure Update Request message.

## 5.3. Channel/Power Auto Adjusment

The Channel Scan Procedure is illustrated by the figure 4.

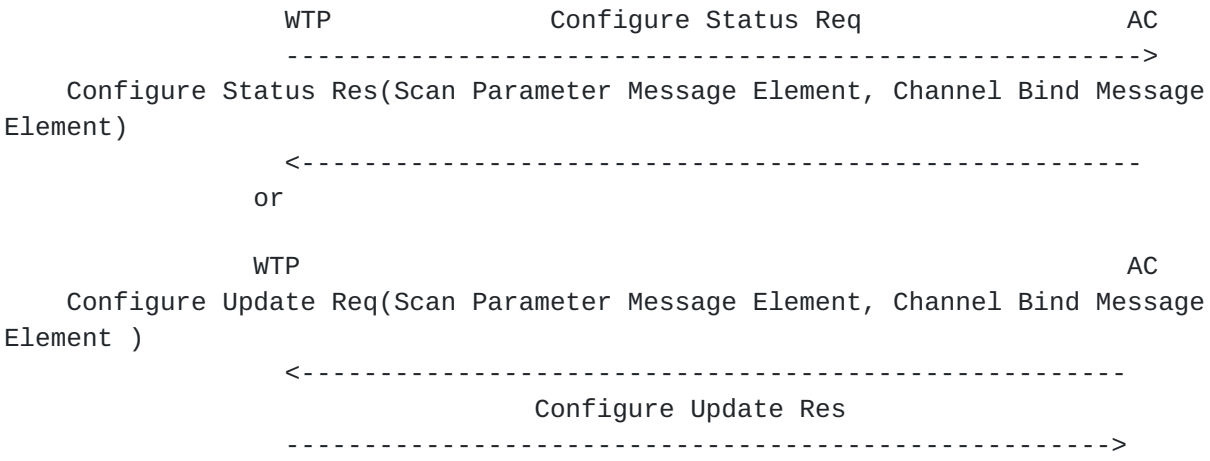


Figure 4: Channel Scan Procedure

WTP has two working modes, the first one is normal working mode. In this mode, the WTP can scan the channel while providing the service to STA. Whether WTP will provide scanning service is determined by the Max Cycles value of Channel Bind Message Element. If this value equls to zero, the WTP will not perform scanning. If this value equls to 255, the WTP will scan the channel continuously until getting notification from AC. Otherwise, the WTP will perform scanning with the number that specified the value of Max Cycles. The second working mode is scan only mode. The WTP will not provide service to STA in this case. In this mode, WTP will scan the channel continuously.

When the WTP work in the scan only mode, there is no difference between the working channel and scan channel. Every channel's scan duration will be OffChannelScnTime and the PrimeChlSrvTime and OnChannelScanTime is set to 0.

There are two scan types which is determined by the Scan Type value. The first type is passive scan. The WTP will listen the channel

passively in this case. The other type is active scan. The WTP will

send probe for the scan. There are three parameters that will determine the working mode of scan: PrimeChlSrvTime, On Channel ScanTime, Off Channel ScanTime. The WTP will provide service for the period of "PrimeChlSrvTime" time then start channel scan for the period of "On Channel ScanTime" time; then continue to provide service for the period of "PrimeChlSrvTime" time; then leave the current working channel and scan next channel for the period of "Off Channel ScanTime" time; then provide service on the next channel for the period of "PrimeChlSrvTime"..until finishing the scan procedure.

### 5.3.1. Scan Parameter Message Element

The definition of the Scan Para Message Element is as follows:

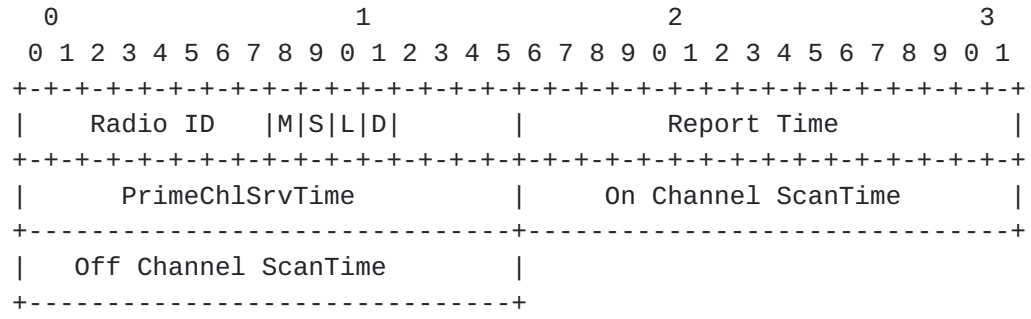


Figure 5: Scan Parameter Message Element

Type: TBD for Scan Parameter Message Element.

Length: 10.

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

M bit: AP oper mode: the work mode of the WTP. 0x01:normal mode. 0x02: monitor only mode, no service is provided in this mode.ss

S bit: Scan Type: 0x01: active scan; 0x02: passive scan.

L bit: L=1: Open Load Balance Scan. D bit: D=1: Open Rogue WTP detection scan.

Report Time: Channel quality report time (unit: second).

PrimeChlSrvTime: Service time (unit: millisecond) on the working scan channel. This segment is invalid(set to 0) when WTP oper mode is set to 2. The maximum value of this segment is 10000, the minimum value of this segment is 5000, the default value is 5000.

On Channel ScanTime: The scan time (unit: millisecond) of the working channel. When the WTP oper mode is set to 2, this segment is invalid(set to 0). The maximum value of this segment is 120, the minimum value of this segment is 60, the default value is 60.

### 5.3.2. Channel Bind Message Element

The definition of the Channel Bind Message ELement is as follows:

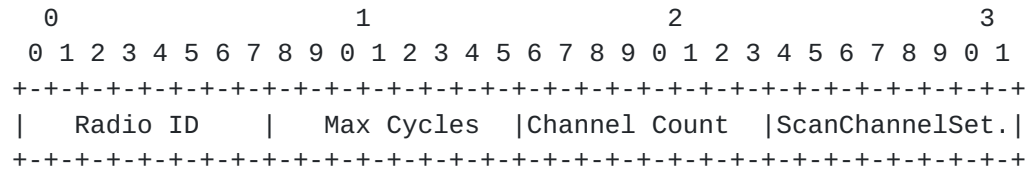


Figure 6: Channel Bind Message Element

Type: TBD for Channel Bind Message Element.

Length: 4.

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

Flag: bitmap, reserved.

Max Cycles: Scan repeat times. 255 means continuous scan.

Channel Count: The number of channel will be scanned.

Scan Channel Set: The channel information. The format is as follows:

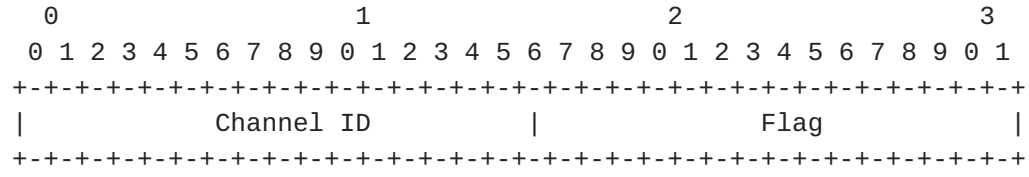


Figure 7: Channel Information Format

Channel ID: the channel ID of the channel which will be scanned.

Flag: Bitmap, reserved for future use.

### 5.3.3. Channel Scan Report

There are two types of scan report: Channel Scan Reprot and Neighbor STA Reprot. Channel Scan Report is used to channel autoconfiguration while Neighbor WTP Report is used to power autoconfiguration. The WTP send the scan report to the AC through WTP Event Request message. The information element that used to carry the scan report is Channel Scan Report Message Element and Neighbor WTP Report Message Element.

The definition of the Channel Scan Report Message Element is in figure 8.

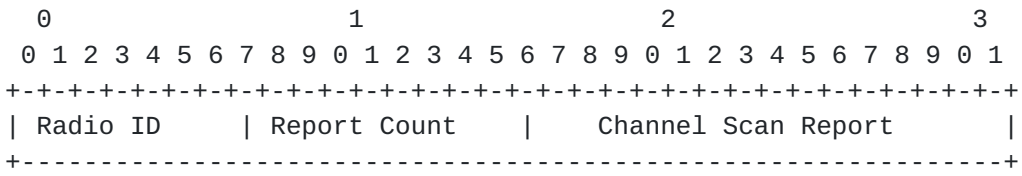


Figure 8: Channel Scan Report Message Element

Type: TBD for Channel Scan Report Message Element.

Length: >=29.

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

Report Count: The channel number will be reported.

Channel Scan Report: The definition of the Channel Scan Report is in figure 9. It complies with the IEEE 802.11 Beacon report that defined in section 8.4.2.24.7 of [IEEE-802.11.2012].

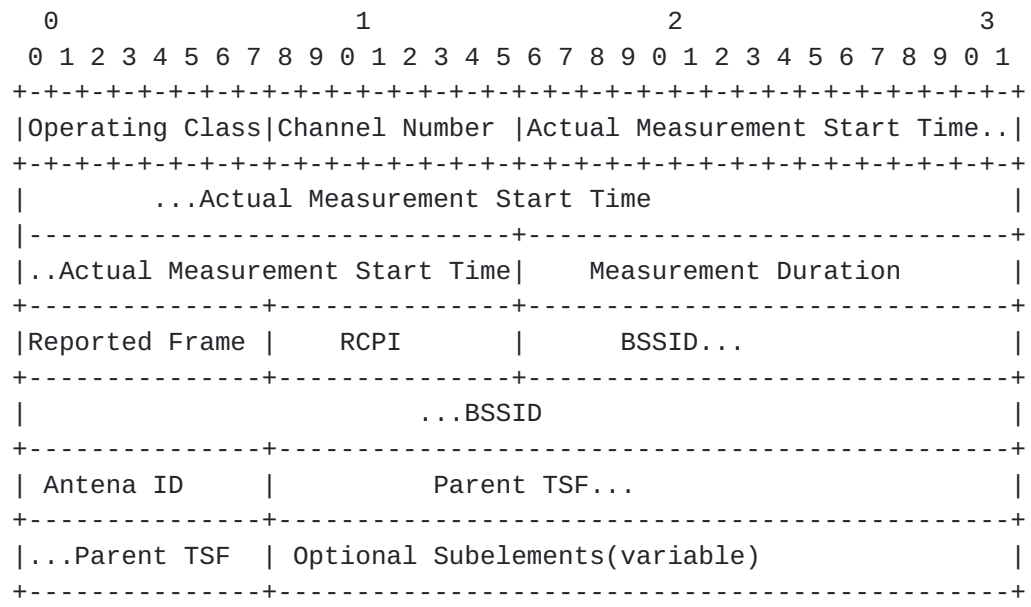


Figure 9: Channel Scan Report

Operating Class: Indicates the channel set for which the measurement request applies. The definition of this field complies with the definition in section 8.4.2.24.7 of [IEEE-802.11.2012].

Channel Number: Indicates the channel number for which the measurement report applies. The definition of this field complies with the definition in section 8.4.2.24.7 of [IEEE-802.11.2012].

Actual Measurement Start Time: Is set to the value of the measuring STA's TSF timer at the time the measurement started.

Measurement Duration: Is set to the duration over which the Beacon Report was measured. The definition of this field complies with the definition in section 8.4.2.24.7 of [IEEE-802.11.2012].

Reported Frame Information: This field contains two subfields as defined in [IEEE-802.11.2012].

RCPI: Indicates the received channel power of the Beacon, Measurement Pilot, or Probe Response frame.

RSNI:Indicates the received signal to noise indication for the Beacon, Measurement Pilot, or Probe Response frame.

BSSID: This field contains the BSSID from the Beacon,Measurement Pilot, or Probe Response frame being reported.

Antenna ID: This field contains the identifying number for the antennas used for this measurement.

Parent TSF: This field contains the lower 4 octets of the measuring STA's TSF timer value at the start of reception of the first octet of the timestamp field of the reported Beacon, Measurement Pilot, or Probe Response frame at the time the Beacon frame being reported was received.

Optional Subelements: This field contains zero or more subelements.

### 5.3.4. Neighbor WTP Report

The neighbor WTP report message element is composed of the IEEE 802.11 Information Element that defined in section 6.6 of [RFC5416] and IEEE 802.11 Neighbor Report Element that defined in section 8.4.2.39 of [IEEE-802.11.2012]. The Neighbor Report Element is carried by the IEEE 802.11 Information Element to form the neighbor WTP report message element.

## 6. Security Considerations

This document is based on RFC5415/RFC5416 and it doesn't increase any security risk. The security considerations of this document aligns with RFC5415/5416.

## 7. IANA Considerations

The extension defined in this document need to extend CAPWAP IEEE 802.11 binding message element which is defined in section 6 of [RFC5416]. The following IEEE 802.11 specific message element type need to be defined by IANA.

802.11n Radio Configuration Message Element type value described in section 4.1.2.

802.11n Station Message Element type value described in section 4.1.3.

Scan Parameter Message Element type value described in section 5.3.1.

Channel Bind Message Element type value described in section 5.3.2.

Channel Scan Report Message Element type value described in section 5.3.3.

## 8. Contributors

This draft is a joint effort from the following contributors:

Gang Chen: China Mobile chengang@chinamobile.com

Naibao Zhou: China Mobile zhounaibao@chinamobile.com

Chunju Shao: China Mobile shaochunju@chinamobile.com

Hao Wang: Huawei3Come hwang@h3c.com

Yakun Liu: AUTELAN liuyk@autelan.com

Xiaobo Zhang: GBCOM

Xiaolong Yu: Ruijie Networks

Song zhao: ZhiDaKang Communications

Yiwen Mo: ZhongTai Networks

## 9. Acknowledgements

The authors would like to thanks Ronald Bonica,Romascanu Dan, Benoit Claise, Melinda Shore and Margaret Wasserman for their useful suggestions. The authors also thanks Dorothy Stanley and Tom Taylor for their review and useful comments.

## 10. Normative References

[IEEE-802.11.2009]
"IEEE Standard for Information technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2009.

[IEEE-802.11.2012]
"IEEE Standard for Information technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", March 2012.

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

[RFC4564] Govindan, S., Cheng, H., Yao, ZH., Zhou, WH., and L. Yang, "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 4564, July 2006.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

[RFC5416] Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", RFC 5416, March 2009.

## Authors' Addresses

Yifan Chen
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: chenyifan@chinamobile.com

Dapeng Liu
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: liudapeng@chinamobile.com

Hui Deng
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: denghui@chinamobile.com

Lei Zhu
Huawei
No. 156, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan Beiqing Road, Haidian District
Beijing 100095
China

Email: lei.zhu@huawei.com