OPSAWG
Internet-Draft
Updates: 5416 (if approved)
Intended status: Standards Track
Expires: January 7, 2016

Y. Chen
China Mobile
D. Liu

H. Deng
China Mobile
Lei. Zhu
Huawei

July 6, 2015

CAPWAP Extension for 802.11n and Power/channel Autoconfiguration
draft-ietf-opsawg-capwap-extension-06

Abstract

The CAPWAP binding for 802.11 is specified by RFC5416 and it was based on IEEE 802-11.2007 standard. Several new amendments of 802.11 have been published since RFC5416 was published in 2009. 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 January 7, 2016.

Copyright Notice

Table of Contents

1. Introduction

IEEE Std 802.11n[TM]-2009 [IEEE 802.11n.2009] was published in 2009 as an amendment to the IEEE 802.11-2007 standard to improve network throughput. The maximum data rate increases to 600Mbps. In the physical layer, 802.11n uses Orthogonal Frequency Division Multiplexing (OFDM) and Multiple Input/Multiple Output (MIMO) to achieve the high throughput. 802.11n uses multiple antennas to form an antenna array which can be dynamically adjusted to improve the signal strength and extend the coverage.

Capabilities of 802.11n such as radio capability, radio configuration and station information need to be supported by CAPWAP control messages. The necessary extensions for this purpose are introduced in Section 3 and specified in Section 4.

For IEEE 802.11 in general, it is desirable to be able to support power and channel auto reconfiguration. Extensions for this purpose are specified in Section 5.

2. Terminology

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].

This document uses the following abbreviations:

AC Access Controller
A-MSDU Aggregate MAC Service Data Unit
A-MPDU Aggregate MAC Protocol Data Unit
AC Access Controller
GI Guard Interval
MCS Maximum Modulation and Coding Scheme
MIMO Multiple Input/Multiple Output
MPDU MAC Protocol Data Unit
MSDU MAC Service Data Unit
OFDM Orthogonal Frequency Division Multiplexing
TSF timing synchronization function
WTP Wireless Termination Point

3. CAPWAP 802.11n Support

802.11n supports 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 the 2.4GHz band. In the large scale deployment scenario, the operator needs to use 20MHz channel configuration in the 2.4GHz band to allow more non-overlapping channels.

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

Another feature in the 802.11 MAC layer is Block ACK. 802.11n can use one ACK frame to acknowledge receipt of several MAC Protocol Data Units (MPDUs).

CAPWAP needs to be extended to support the above new 802.11n features. CAPWAP should allow the access controller to know the supported 802.11n features and the access controller should be able

to configure the different channel binding modes. This document defines extensions of the CAPWAP 802.11 binding to support 802.11n features.

3.1. CAPWAP Extension for 802.11n Support

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 the current CAPWAP 802.11 binding to support the 802.11n features.

3.1.1. 802.11n Radio Capability Information

[RFC5416] defines the IEEE 802.11 binding for the CAPWAP protocol. It defines the IEEE 802.11 Information Element, which is used to communicate any information element (IE) defined in the IEEE 802.11 protocol. This document specifies that the IEEE 802.11 Information Element defined in section 6.6 of [RFC5416] SHALL be used to transport the IEEE 802.11 HT information element defined in section 8.4.2.58 of [IEEE-802.11.2012]. The HT IE MAY in this way be included in CAPWAP Configuration Status Request/Response messages.

3.1.2. 802.11n Radio Configuration Message Element

The 802.11n Radio Configuration message element is used by the AC to provide IEEE 802.11n-specific configuration for a Radio on the WTP, and by the WTP to deliver its radio configuration to the AC. This supplements the IEEE 802.11 WTP WLAN Radio Configuration message element defined in [RFC5416]. The format of the 802.11n Radio Configuration message element is shown in Figure 1. The 802.11n Radio Configuration message element MAY be included in the CAPWAP Configuration Update Request/Response message.

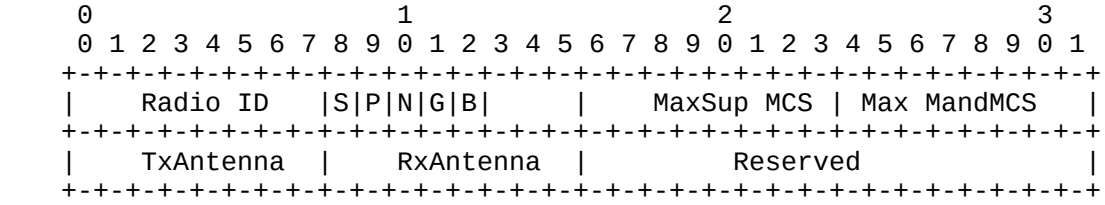

Figure 1: 802.11n Radio Configuration Message Element

Type: TBD1 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 configuration: Enable/disable Aggregate MAC Service Data Unit (A-MSDU). Set to 0 if disabled. Set to 1 if enabled.

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

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

G bit: Short GI configuration: Set to 0 if Short Guard Interval is disabled. Set to 1 if enabled.

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

Maximum supported 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 represents a certain number of antennas. Set to 1 if enabled, set to 0 if disabled.

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

The detail definition of TxAntenna/RxAntenna is as follows:

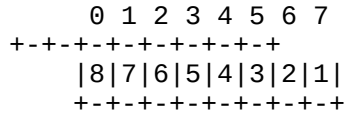

Figure 2: Definition of TxAntenna/RxAntenna

Each bit when enabled will represent the number of antennas correspondent to that bit. Only one bit is allowed to be set to 1. For example, when the first bit is enabled,it represents 8 antennas.

3.1.3. 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. The format of 802.11n Station Information MAY be included in the CAPWAP Station Configuration Request message.

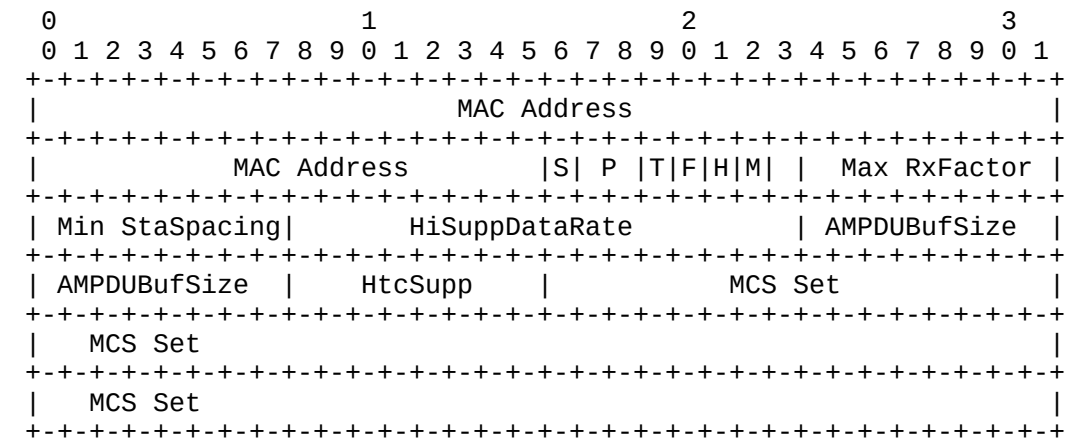

Figure 3: 802.11n Station Information

MAC Address: The station’s MAC Address.

Type: TBD2 for 802.11 Station Information.

Length: 24.

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

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

T bit: Whether to support short GI in 20MHz bandwidth mode. 0x00: Do not support short GI. 0x01: Support short GI.

F bit: ShortGi40: Whether to support short GI in 40MHz bandwidth mode. 0x00: Do not support short GI. 0x01: Support short GI.

H bit: Whether Block Ack supports delay mode. 0x00: Do not support delay mode. 0x01: Support delay mode.

M bit: The maximal A-MSDU length. 0x00: 3839 bytes. 0x01: 7935 bytes.

Max RxFactor: The maximal receiving A-MPDU factor.

Min StaSpacing: Minimum MPDU Start Spacing.

HiSuppDataRate: Maximal transmission speed (Mbps).

AMPDUBufSize: A-MPDU buffer size (Byte).

HtcSupp: Whether to place HT headers on the packets forwarded from this station.

MCS Set: The MCS bitmap that the station supports.

4. 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.

4.1. Channel Autoconfiguration When WTP Power On

Power and channel auto reconfiguration avoids potential radio interference and improves the WLAN performance. In general, the auto- configuration of radio power and channel can occur at two stages: when the WTP powers on or while the WTP is in running state. When the WTP is powered-on, it needs to configure a proper channel. 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 the channel field of those information element is set to 0, 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. As shown in Figure 3, the AC can control the scanning process by sending the IEEE 802.11 Scan Parameters message element defined in Section 5.1 to the

WTP in a Configure Status Response message or in a WTP Configure Update Request message. The WTP will send the channel quality report to the AC using the WTP Event Request message.

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

4.2. Power Configuration When WTP Power On

The IEEE 802.11 Tx Power message element defined in section 6.18 of [RFC5416] 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.

4.3. Channel/Power Auto Adjustment

The Channel Scan Procedure is illustrated by the figure 4.

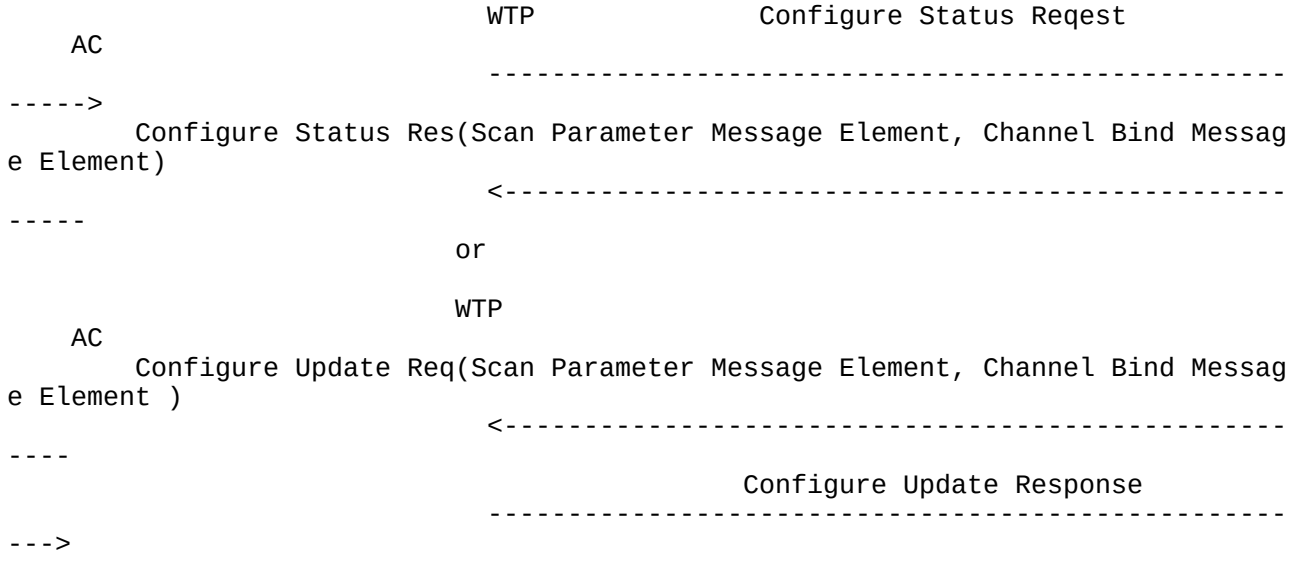

Figure 4: Channel Scan Procedure

The WTP has two work modes: normal mode and scan only mode. In normal mode, the WTP can provide service for station access and scan channels at the same time. Whether the WTP will scan a given set of channels is determined by the Max Cycles field in the IEEE 802.11 Channel Bind message element defined in Section 4.3.2. When this field is set to 0, the WTP will not scan the channel. If this field is set to 255, the WTP will scan the channel continuously. The type of the scan is determined by the Scan Type field. With the passive scan type, the WTP monitors the air interface, using the received

beacon frames to determine the nearby WTPs. With the active scan type, the WTP will send a probe message and receive probe response messages. In this case, the WTP may need to operate in station mode which means it is not a WTP function only device, it also has part of station function.

In normal mode, the WTP behaviour is controlled by three parameters: PrimeChlSrvTime, OnChannelScanTIme, and OffChannelScnTIme. These are provided by the IEEE 802.11 Scan Parameters message element defined in Section 4.3.1. The WTP will provide access service for stations for the duration given by PrimeChlSrvTime. It then scans the working channel for the duration given by OnChannelScnTime. It returns to servicing station access requests on the working channel for another period of length PrimeChlSrvTime, then moves to a different channel and scans it for duration OffChannelScnTime. It repeats this cycle, scanning a new non-working channel each time, until all the channels have been scanned. This channel scan procedure can be used to determine the interference of both the current working channel and non-working channel to avoid potential interference.

When the WTP works in scan only mode, it does not distinguish between the working channel and scan channel. Every channel’s scan duration will be OffChannelScnTime and PrimeChlSrvTime and OnChannelScanTime MUST be set to 0.

As shown in Figure 4, the AC can control the scan behaviour at the WTP by including the IEEE 802.11 Scan Parameters and IEEE 802.11 Channel Bind message elements in a Configure Status Response or WTP Configure Update Request message.

Scan Report. After completing its scan, the WTP MAY send the scan report to the AC using a WTP Event Request message. The scan report information is carried in the IEEE 802.11 Channel Scan Report message element (Section 4.3.3) and an instance of the IEEE 802.11 Information Element message element carrying a copy of theIEEE 802.11 Neighbor WTP Report information element (Section 4.3.4).

4.3.1. IEEE 802.11 Scan Parameters Message Element

The format of the IEEE 802.11 Scan Parameters Message Element is as shown in Figure 5:

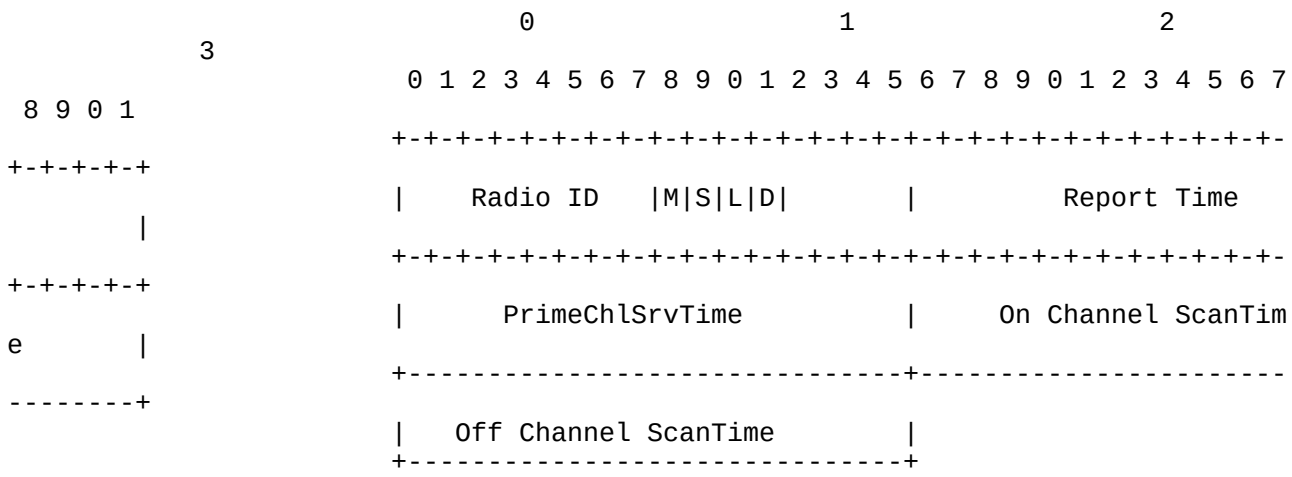

Figure 5: IEEE 802.11 Scan Parameters Message Element

Type: TBD3 for IEEE 802.11 Scan Parameters Message Element.

Length: 10.

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

M bit: Work mode of the WTP. 0:normal mode. 1: scan only mode, no service is provided in this mode.

S bit: Scan Type: 0: active scan; 1: passive scan.

L bit: L=1: Open Load Balance Scan. L=0: Disable Load Balance Scan.

D bit: D=1: Open Rogue WTP detection scan. D=0: Disable Rouge 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 1. 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 M bit is set to 1 (active scan), 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.

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

4.3.2. IEEE 802.11 Scan Channel Bind Message Element

The format of the IEEE 802.11 Scan Channel Bind Message Element is as follows:

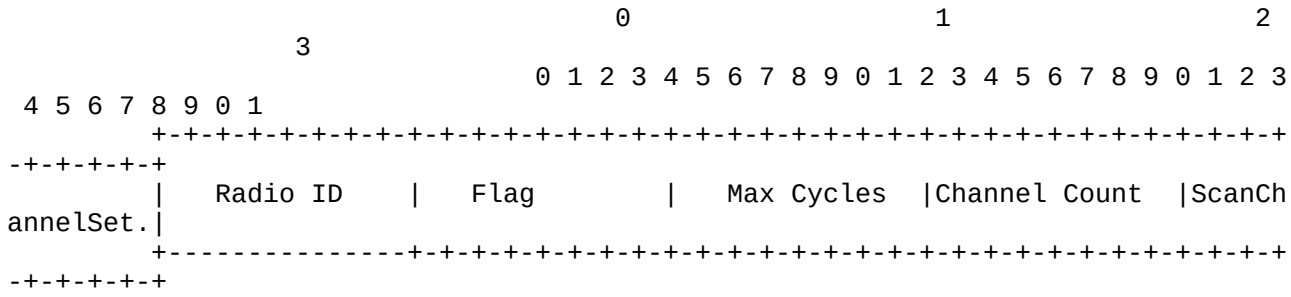

Figure 6: IEEE 802.11 Scan Channel Bind Message Element

Type: TBD4 for IEEE 802.11 Scan Channel Bind Message Element.

Length: variable.

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

Flag: reserved.

Max Cycles: Number of times the scanning cycle is repeated for the set of channels identified by this message element. 255 means continuous scan.

Channel Count: The number of channels will be scanned.

Scan Channel Set: identifies the members of the set of channels to which this message element instance applies. The format for each channel is as follows:

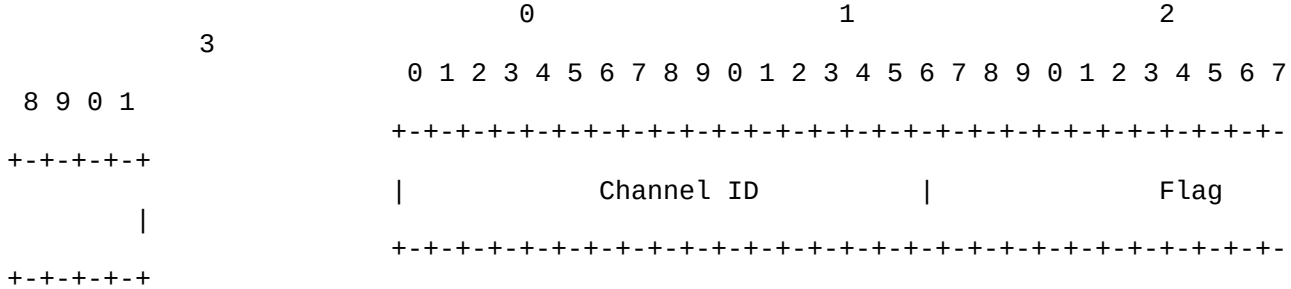

Figure 7: Channel Information Format

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

Flag: Bitmap, reserved for future use.

4.3.3. IEEE 802.11 Channel Scan Report

There are two types of scan report: Channel Scan Report and WTP Neighbor Report. Channel Scan Report is used to channel autoconfiguration while WTP Neighbor 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 WTP Neighbor Report Message Element.

The format of the IEEE 802.11 Channel Scan Report message element is in Figure 8.

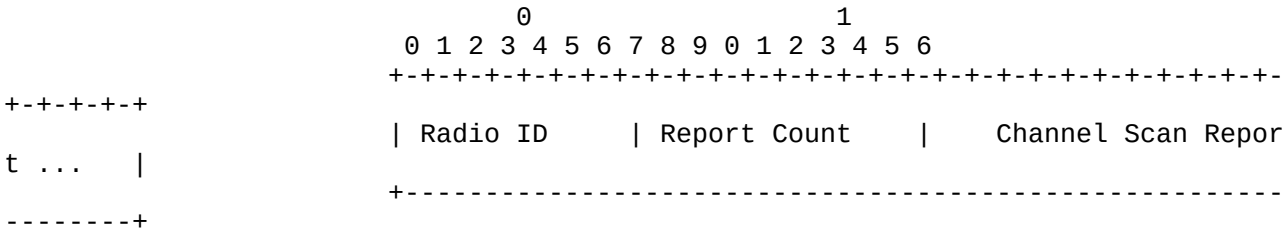

Figure 8: IEEE 802.11 Channel Scan Report Message Element

Type: TBD5 for IEEE 802.11 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 number of channels for which a report is provided.

Channel Scan Report: The format of each Channel Scan Report is shown in Figure 9.

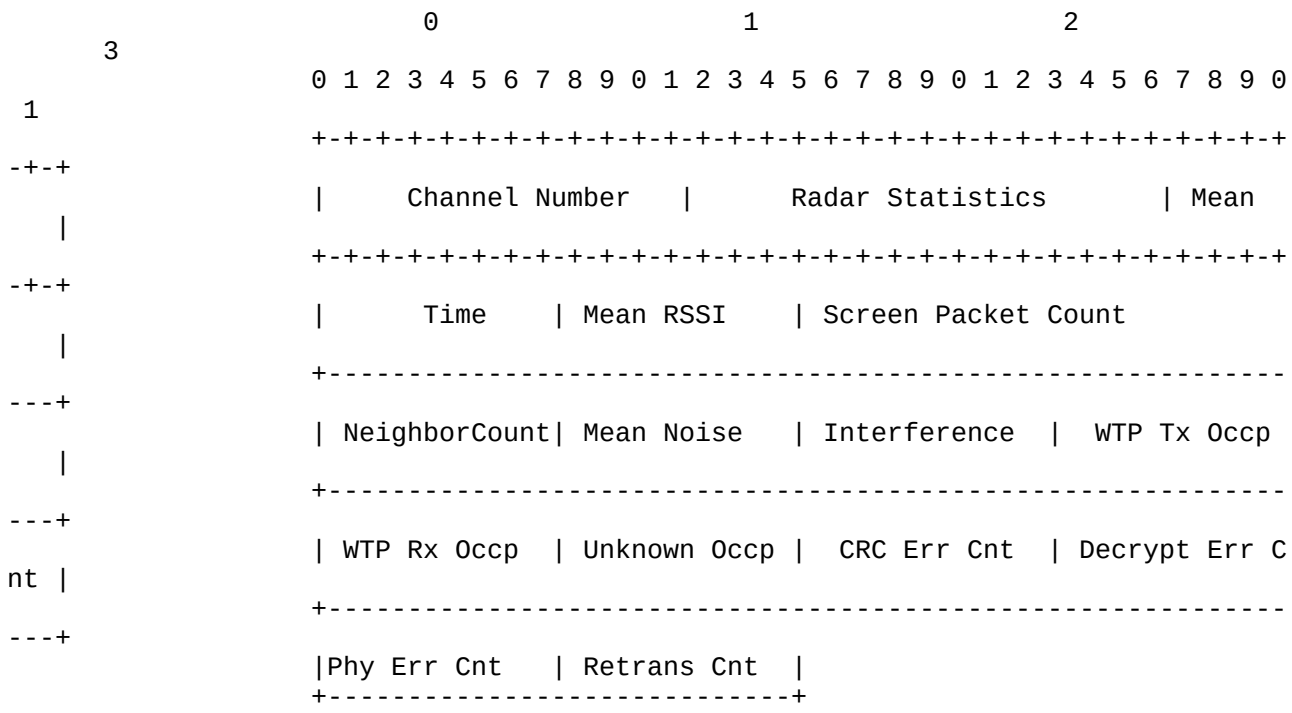

Figure 9: Channel Scan Report

Channel Number: The channel number.

Radar Statistics: Whether detect radar signal in this channel. 0x00: detect radar signal. 0x01: no radar signal is detected.

Mean Time: Channel measurement duration (ms).

Mean RSSI: The average signal strength of the scanned channel (dBm(2's complement)).

Screen Packet Count: Received packet number.

Neighbor Count: The neighbor number of this channel.

Mean Noise: the average noise on this channel (dBm(2's complement)).

Interference: The interference of the channel.

WTP Tx Occp: (The WTP transmission time/Monitor time)*255. The WTP transmission time is the total sending time of the WTP during the period of channel scan.

WTP Rx Occp: (The WTP receiving duration time/Monitor time)*255. THe WTP receiving duration time is the total receiving time of the WTP during the period of channel scan.

Unknown Occp: (All other packet transmission time duration/Monitor time)*255.

CRC Err Cnt: CRC err packet number.

Decrypt Err Cnt: Decryption err packet number.

Phy Err Cnt: Physical err packet number.

Retrans Cnt: Retransmission packet number.

Note:The values of the above four count fields for a non-operational channel can be ignored

4.3.4. IEEE 802.11 WTP Neighbor Report

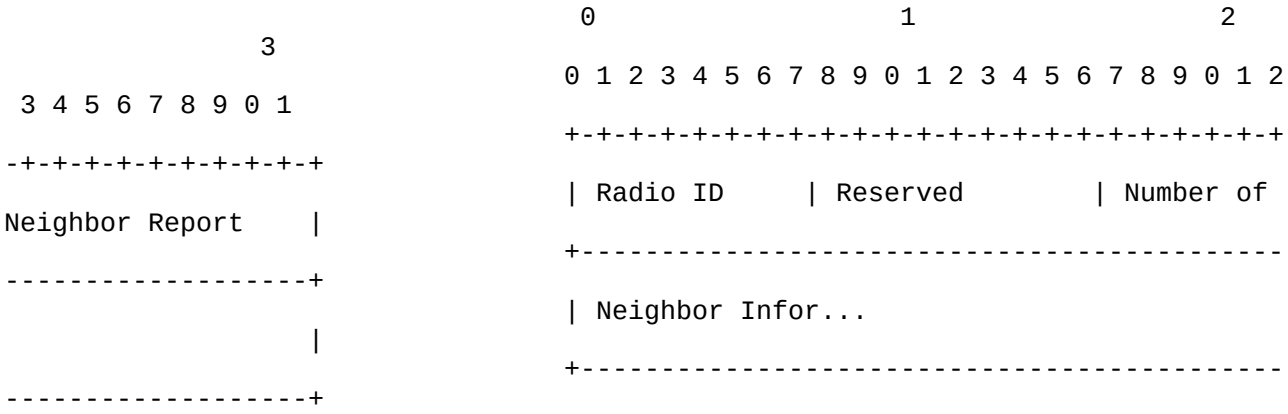

Figure 10: WTP Neighbor Report TLV

The definition of Neighbor info is as follows:

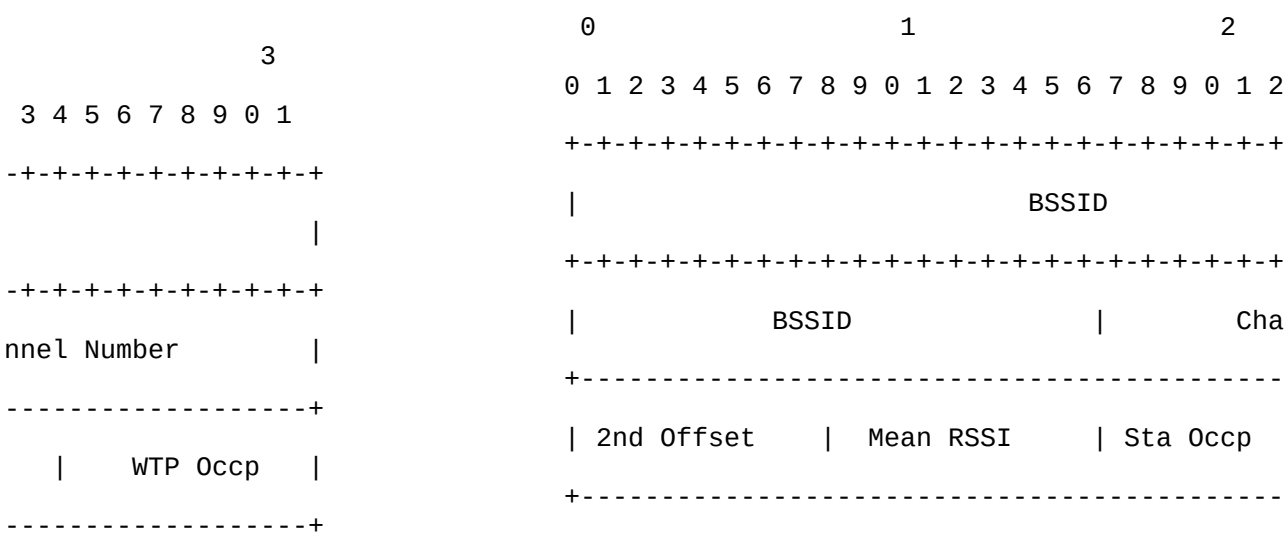

Figure 11: Neighbor info

BSSID: The BSSID of this neighbor WTP.

Channel Number: The channel number of this WTP neighbor.

2nd channel offset: The auxiliary channel offset of this WTP.

Mean RSSI: The average signal strength of this WTP (dbm).

Sta Occp: (The station air interface occupation time/Monitor time)*255.The station air interface occupation time is the air interface occupation time caused by the stations which are connected to this WTP.

WTP Occp: (The WTP air interface occupation time/Monitor time)*255. The WTP air interface occupation time is the air interface occupation time caused by the WTP.

5. Security Considerations

This document is based on RFC5415/RFC5416 and adds no new security considerations.

6. 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.

TBD1: 802.11n Radio Configuration Message Element type value described in section 4.1.2.

TBD2: 802.11n Station Message Element type value described in section 4.1.3.

TBD3: 802.11 Scan Parameter Message Element type value described in section 4.3.1.

TBD4: 802.11 Channel Bind Message Element type value described in section 4.3.2.

TBD5: Channel Scan Report Message Element type value described in section 4.3.3.

TBD6 entry for WTP Neighbor Report as descrbed in section 4.3.4 .

7. 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

Dorothy Stanley: dstanley1389@gmail.com

Tom Taylor: tom.taylor.stds@gmail.com

8. 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.

9. 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, Enhancements for Higher Throughput (Amendment 5)", 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
Beijing
China

Email: maxpassion@gmail.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