Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 10, 2013

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

May 09, 2013

# CAPWAP Extension for 802.11n and Power/channel Reconfiguration
# draft-ietf-opsawg-capwap-extension-00

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 was several new amendent of 802.11 has been published. 802.11n is one of those amendent and it has been widely used in real deployment. This document extends the CAPWAP binding for 802.11 to support 802.11n.

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 November 10, 2013.

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 to improve network throughput. The maximum data rate increases to 600Mbit/s physical throughput rate. In the physical layer, 802.11n use OFDM and MIMO to achive the high throughput. 802.11n use multiple antennas to form antenna array which can be dynamically adjusted to imporve the signal strength and extend the coverage.

There are couple of capabilities of 802.11n need to be supported by CAPWAP control message such as radio capability, radio configuration and station information.

## 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. CAPWAP 802.11n support

IEEE 802.11n standard was published in 2009 and it is an amendment to the IEEE 802.11-2007 standard to improve network throughput. The maximum data rate increases to 600Mbit/s physical throughput rate. In the physical layer, 802.11n use OFDM and MIMO to achive the high throughput. 802.11n use multiple antennas to form antenna array which can be dynamically adjusted to imporve 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 use 800ns guard interval between the adjacent information symbols. In 802.11n, the GI can be configured to 400nm under good wireless condition.

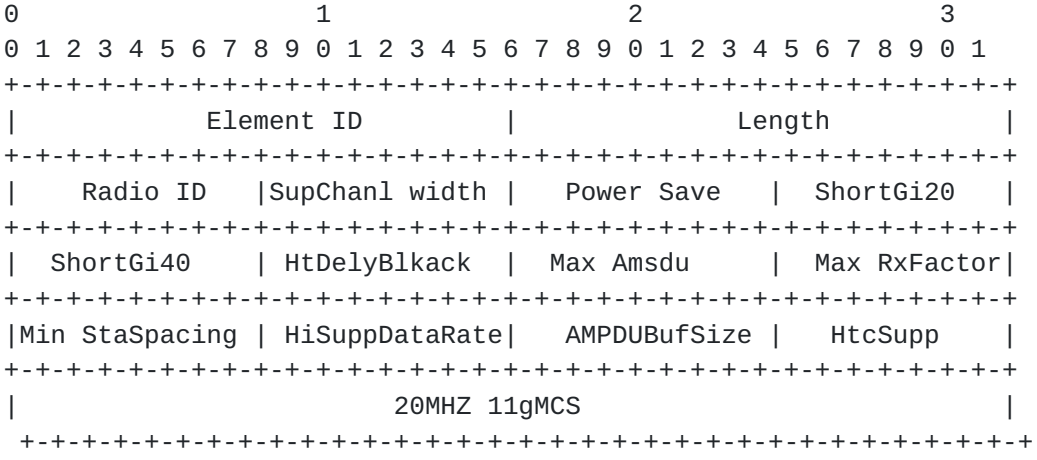
Another feature in 802.11 MAC layer is Block ACK. 802.11n can use one ACK frame to acknowledge several MPDU receiving event.

CAPWAP need 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 and the access controller should be able to configure the differe channel binding modes. One possible solution is to extend the CAPWAP information element for 802.11n.

## 4. CAPWAP extension for 802.11n support

There are couple of capabilities of 802.11n need to be supported by CAPWAP control message such as radio capability, radio configuration and station information. This section defines the extension of current CAPWAP 802.11 information element to support 802.11n.

1. 802.11n Radio Capability Information Element. Below is an example of the 802.11n radio capability information element. This 802.11n radio capability information element may also be conveyed using the IEEE 802.11 information element by carrying the IEEE 802.11 HT element information.



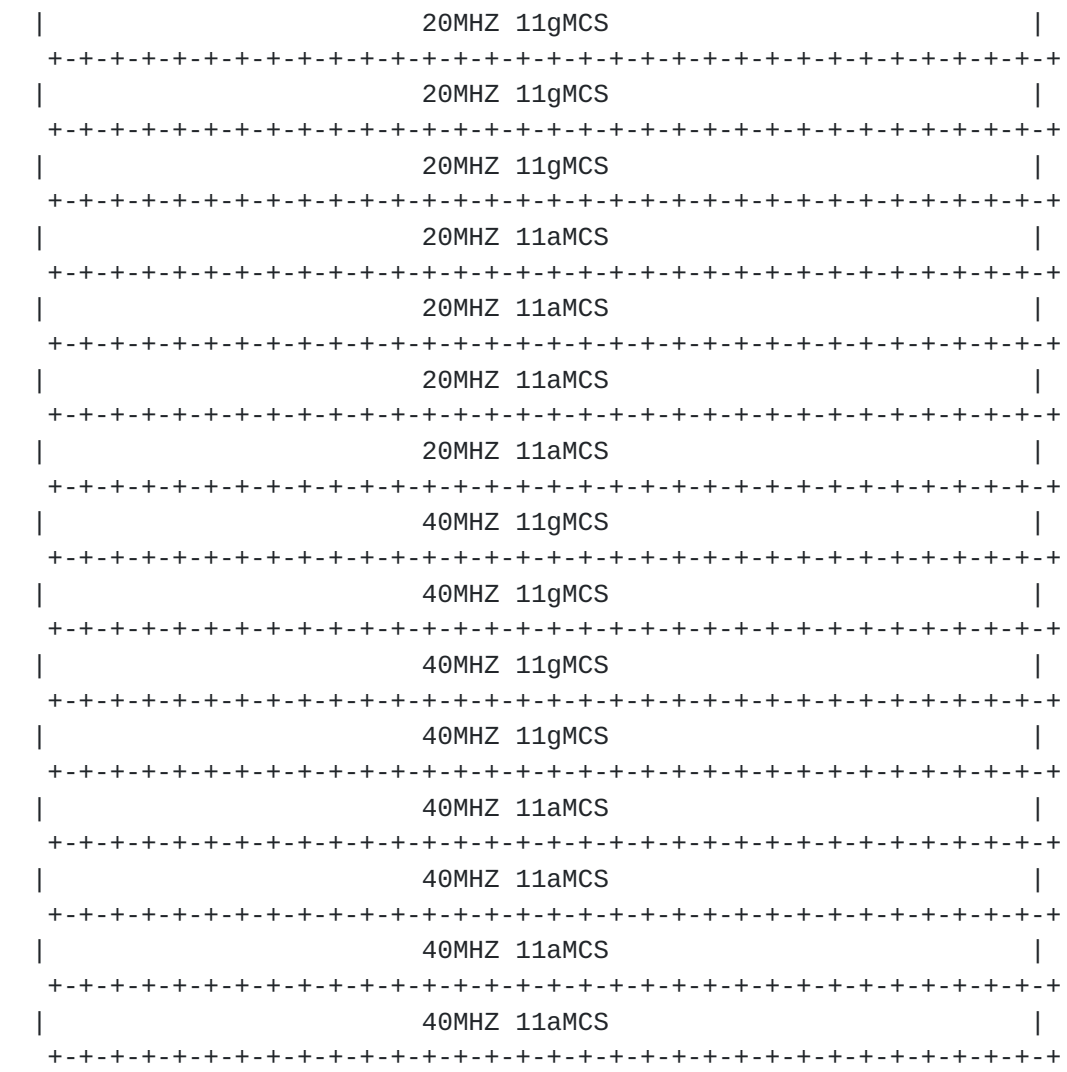



Figure 1: 802.11n Radio Capability Information Element

1. SupChanl width: The supported bandwith mode. 0x01: 20MHz bandwidth binding mode. 0x02: 40MHz bandwidth binding mode.
2. Power Save: 0x00: Static power saving mode. 0x01: Dynamic power saving mode. 0x03: Do not support power saving mode.
3. ShortGi20: Whether support short GI. 0x00: Do not support short GI. ox01: Support short GI.
4. HtDelyBlkack: Whether block Ack support delay mode. 0x00: Do not support delay mode. 0x01: Support delay mode.
5. Max Amsdu: The maximal AMSDU length. 0: 3839 bytes. 1: 7935 bytes.
6. Max RxFactor: The maximal receiving AMPDU factor. Default value: 3.
7. Min StaSpacing: Minimum MPDU Start Spacing.
8. HiSuppDataRate: Maximal transmission speed.

9. AMPDUBufSize: AMPDU buffer size.
10. HtcSupp: Whether the packet have HT header.
11. 20MHZ 11gMCS: 128 bitmap.If support should be all zero, otherwise all one.
12. 20MHZ 11aMCS: 128 bitmap.If support should be all zero, otherwise all one.
13. 40MHZ 11gMCS: 128 bitmap.If support should be all zero, otherwise all one.
14. 40MHZ 11aMCS: 128 bitmap.If support should be all zero, otherwise all one.
15. 2. 802.11n Raido Configuration TLV. Following figure is an example of 802.11n radio configuration TLV.

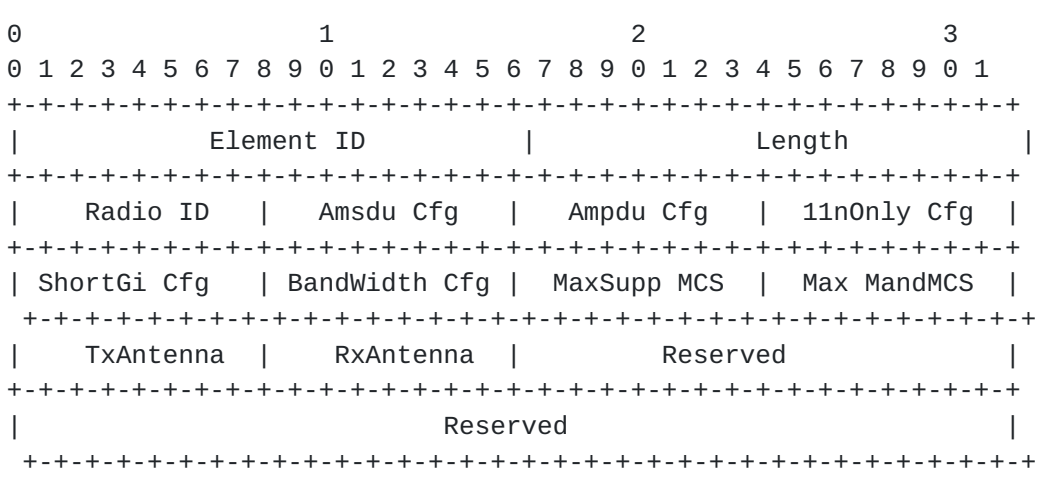



Figure 2: 802.11n radio configuration

1. A-MSDU CFG: 0x00: Disable 0x01: Enalbe
2. A-MPDU CFG: 0x00: Disable 0x01: Enalbe
3. 11N Only CFG: Whether allow only 11n user access. 0x00: Allow non-802.11n user access. 0x01: Do not allow non-802.11n user access.
4. Short GI CFG: 0x00: Disable 0x01: Enable
5. Bandwidth CFG: Bandwidth binding mode. 0x00: 40MHz 0x01: 20MHz
6. Max Support MCS: Maximal MCS.
7. Max Mandantory MCS: Maximal mandantory MCS.
8. TxAntenna: Transmitting antenna configuration.
9. RxAntenna: Receiving antenna configuration.
10. Each TxAntenna and RxAntenna bit represent one antenna, 1 means enable, 0 means disable.

3. 802.11n Station Information. Following figure is an example of 802.11n station information information element.

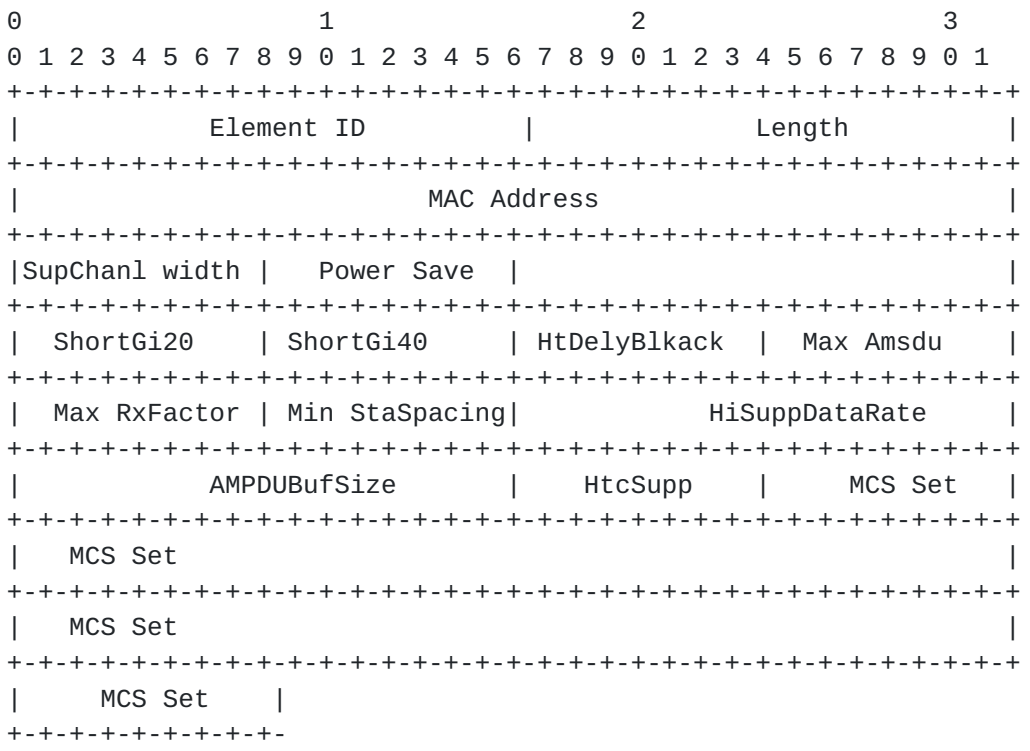



Figure 3: 802.11n Station Information

1. SupChanl width: Supporting bandwidth mode. 0x01: 20MHz bandwidth mode. 0x02: 40MHz bandwidth binding mode.
2. Power Save: 0x00: Static power saving mode. 0x01: Dynamic power saving mode. 0x03: Do not support power saving mode.
3. ShortGi20: Whether support short GI in 20MHz bandwidth mode. 0x00: Do not support short GI. ox01: Support short GI.
4. ShortGi40: Whether support short GI in 40MHz bandwidth mode. 0x00: Do not support short GI. ox01: Support short GI.
5. HtDelyBlkack: Whether block Ack support delay mode. 0x00: Do not support delay mode. 0x01: Support delay mode.
6. Max Amsdu: The maximal AMSDU length. 0x00: 3839 bytes. 0x01: 7935 bytes.
7. Max RxFactor: The maximal receiving AMPDU factor.
8. Min StaSpacing: Minimum MPDU Start Spacing.
9. HiSuppDataRate: Maximal transmission speed.
10. AMPDUBufSize: AMPDU buffer size.
11. HtcSupp: Whether the packet have HT header.
12. MCS Set: The MCS bitmap that the station supports.

## 5. Power and Channel auto reconfiguration

Power and channel auto reconfiguration could avoid potential radio interference and improve the Wi-Fi performance. In general, the

auto-configuration of radio power and channel could occurre at two stages: when the WTP power on or during the WTP running time.

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 to offer WTP a channel at this stage. Those element should be carried in the Configure Status Response message. If those information element is zero, the WTP will 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. 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.

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 during the power on phase or in the Configure Update Request message during the running phase.

Channel Scan Procedure.

The Channel Scan Procedure is illustrated by the following figure.

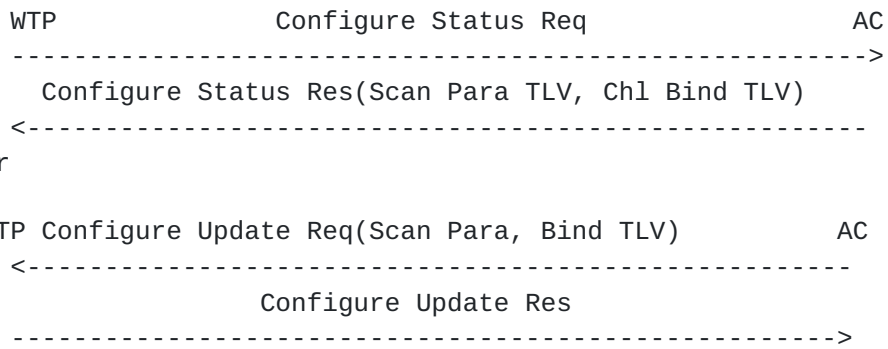



Figure 4: Channel Scan Procedure

The definition of the Scan Para TLV is as follows:

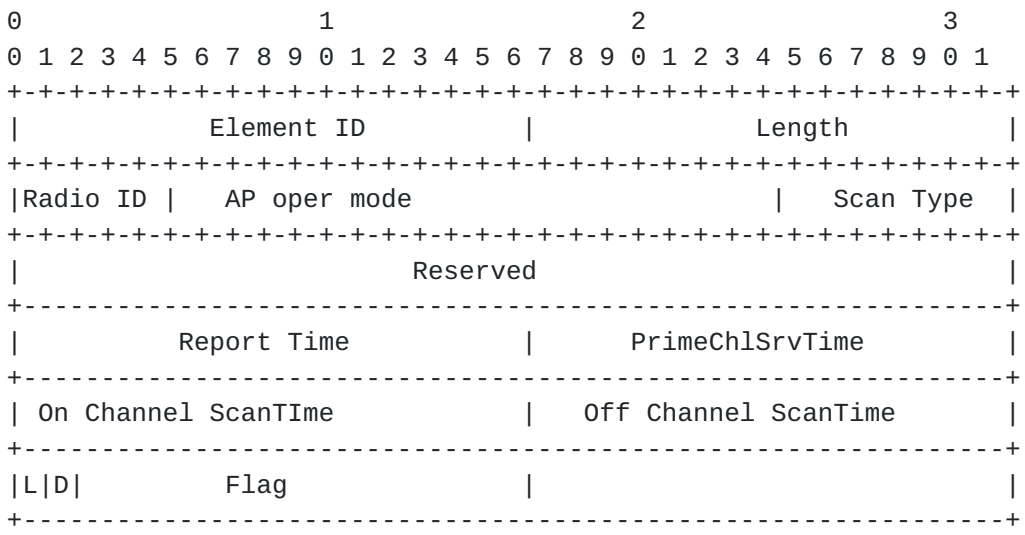



Figure 5: Scan Para TLV

Element ID: TBD; Length:18

AP oper mode: the work mode of the WTP. 0x01:normal mode. 0x02: monitor only mode.

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

Report Time: Channel quality report time.

PrimeChlSrvTime: Service time 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 Channle ScanTime: The scan time of the working channel. When the WTP oper mode is set to 2, this segment is invalid(set to 0). The maximum value of thi segment is 120, the minimum value of this segment is 60, the default value is 60.

L=1: Open Load Balance Scan. D=1: Open Rogue WTP detection scan. Flag: Bitmap, resered for furture use.

The definition of the Channel Bind TLV is as follows:

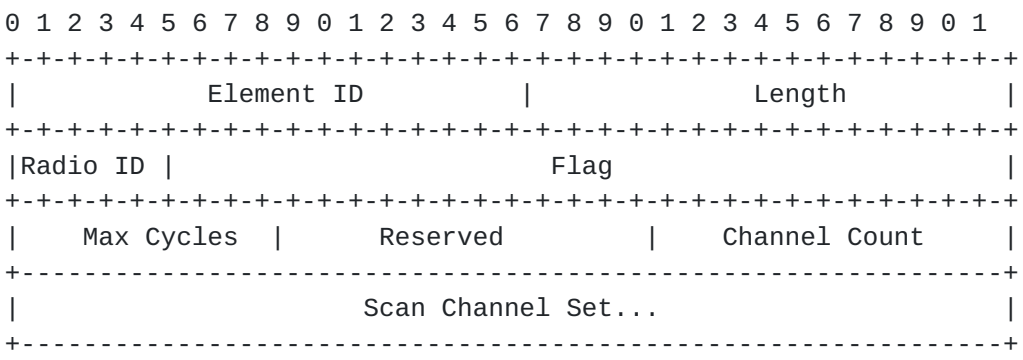



Figure 6: Channel Bind TLV

Element ID: TBD. Length>=12

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 channle information. the format is as follows:

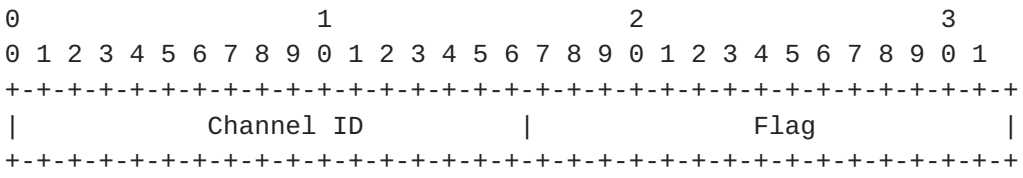



Figure 7: Channle Information Format

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

Flag: bitmap, reserved for future use.

The channle scan procedure:

The WTP has two work mode: the first one is normal mode. In this mode, the WTP can provide service for the STA access and scan the channel at the same time. Whether the WTP will scan the channel is determined by the Max Cycles segment in the Channle Bind TLV. When this segment is set to 0, the WTP will not scan the channle. If this segment is set to 255, the WTP will continuous scan the channel. The

type of the scan is determined by the Sacn Type segment. In the passive scan type, the WTP monitor the airinterface, based on the received beacon frame to determine the nearby WTPs. In the active scan type, the WTP will send probe message and receive the probe response message. In the normal scan mode, the WTP will use 3 parameters: PrimeChlSrvTime, OnChannelScanTIme, OffChannelScnTIme. The WTP will provide access service for the STAs for PrimeChlSrvTime duration and then start to scan the channel for On Channel ScnTime duration. Back to the working channel, provide STA access service for PrimeChlSrvTime, then leave the working channel, start to scan the next channel for Off Channel ScanTime duration. This process will be repeated until all the channel is scanned.

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.

Scan Report. 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 TLV and Neighbor WTP Report TLV. The example definition of the Channel Scan Report TLV is as following figure. The channel scan report may also be conveyed by IEEE 802.11 information element by carrying the IEEE 802.11 beacon report message element.

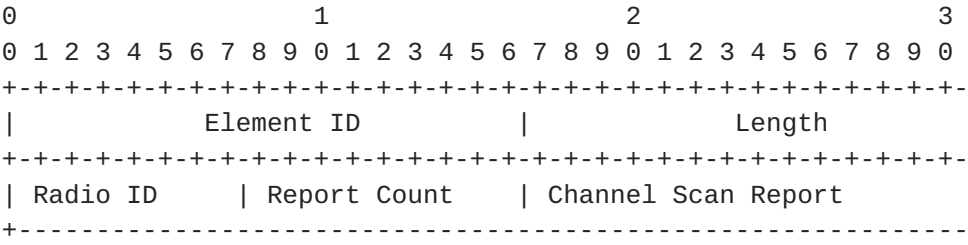
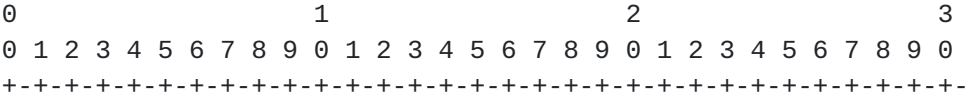



Figure 8: Channel Scan Report TLV

Element ID: 133; Length: >= 20.

Report Count: the channle number will be reported. The definition of the channel scan report is as follows:



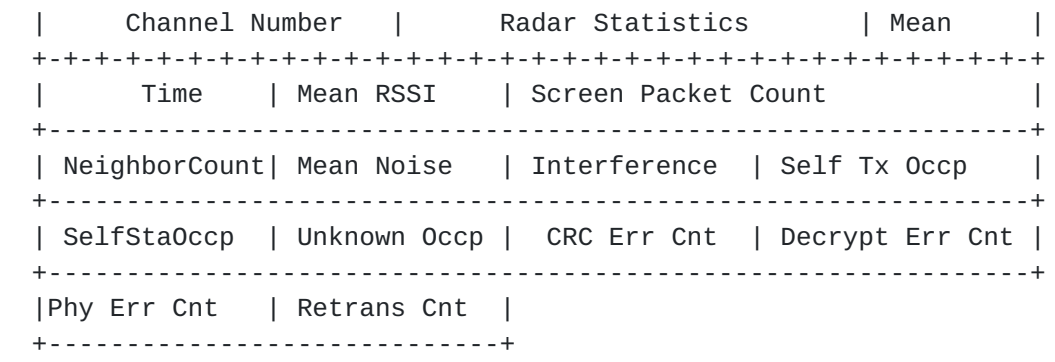



Figure 9: Channel Scan Report

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.

Mean RSSI: The signal strength of the scanned channel.

Screen Packet Count: Received packet number.

Neighbor Count: The neighbor number of this channel.

Mean Noise: the average noise on this channel.

Interference: The interference of the channel.

Self Tx Occp: The time duration for transmission.

Unknown Occp: TBD.

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.

The example definition of neighbor WTP report TLV is as follows:

The neigbor WTP report message element may also be conveyed using IEEE 802.11 information element by carrying 802.11 neighbor report information element.

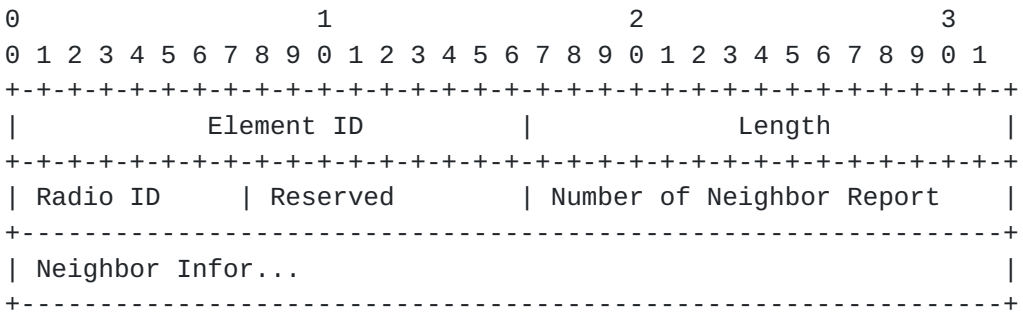



Figure 10: Neighbor WTP Report TLV

Element ID: 134; Length:>=16

The definition of Neighbor info is as follows:

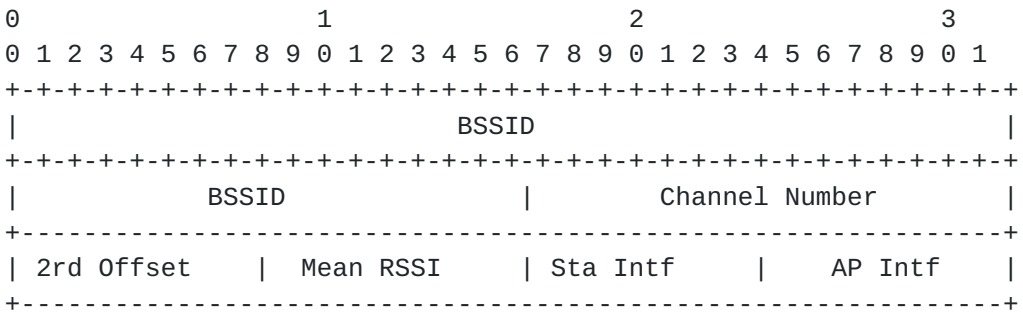



Figure 11: Neighbor info

BSSID: The BSSID of this neighbor channel.

Channel Number: The channel number of this neighbor channel.

2rd channel offset: TBD.

Mean RSSI: The average signal strength of the channel.

Sta Intf: TBD.

AP Intf: TBD.

## 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 IEEE 802.11 binding message element which is defined in RFC 5416. the corresponding type values need to be defined by IANA.

## 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 and Margaret Wasserman for their usefull suggestions. The authors also thanks Dorothy Stanley's review and useful comments.

## 10. Normative References

[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