

# WLAN Tests with Signaling and Packet Data Application Note

## Products:

- R&S®CMW500
- R&S®CMW290
- R&S®CMW270

This document describes WLAN tests which rely on communication (signaling) between R&S®CMW and device under test (DUT) and on transmission of packet data over WLAN. On the R&S®CMW side the WLAN Signaling application is required, for some tests also the Data Application Unit (DAU) and the LTE Signaling application.

The test principles and the necessary settings are explained and background information is given. Step-by-step procedures are provided for the main configuration tasks.

## Note:

Please find the most up-to-date document on our homepage  
<https://www.rohde-schwarz.com/appnote/1C107>.

This document is complemented by software. The software may be updated even if the version of the document remains unchanged.

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>2</b>	<b>Background Information</b>	<b>5</b>
<b>2.1</b>	<b>WLAN Standards and Signal Properties</b>	<b>5</b>
2.1.1	Coding and Data Rates	6
2.1.2	Frame Structures	7
2.1.3	Net Data Rates	9
2.1.4	Transmission Scheme	11
<b>2.2</b>	<b>Internet Protocol and Routing</b>	<b>12</b>
<b>3</b>	<b>Test Setups</b>	<b>14</b>
<b>4</b>	<b>TX (DUT) Tests with Packet Data</b>	<b>17</b>
<b>4.1</b>	<b>Tests with IP packets</b>	<b>17</b>
4.1.1	Test Principle	17
4.1.2	Configuring Packet Data transfer	18
4.1.3	TX (DUT) Measurement	20
<b>4.2</b>	<b>PER Measurements with MAC packets</b>	<b>23</b>
4.2.1	Test Principle	23
4.2.2	PER Measurement	23
<b>5</b>	<b>Throughput Test</b>	<b>25</b>
<b>5.1</b>	<b>Test Principle</b>	<b>25</b>
<b>5.2</b>	<b>Configuring Throughput Measurements</b>	<b>25</b>
<b>6</b>	<b>WLAN Offloading</b>	<b>27</b>
<b>6.1</b>	<b>Test Principle</b>	<b>27</b>
<b>6.2</b>	<b>Configuring WLAN Offloading</b>	<b>28</b>
<b>7</b>	<b>End-to-End Tests for Access Point DUTs</b>	<b>33</b>
<b>7.1</b>	<b>Starting Situation</b>	<b>33</b>
<b>7.2</b>	<b>One Subnet: CMW - DUT (- PC over LAN)</b>	<b>34</b>
7.2.1	Test Principle Path A	34
7.2.2	Configuring Path A	35
<b>7.3</b>	<b>Two Subnets: PC - CMW - DUT - PC over LAN</b>	<b>37</b>
7.3.1	Test Principle Path B	37
7.3.2	Configuring Path B	37

<b>7.4</b>	<b>Three Subnets: PC - CMW - DUT - PC over WAN .....</b>	<b>42</b>
7.4.1	Test Principle Path C .....	42
7.4.2	Configuring Path C.....	42
<b>7.5</b>	<b>Routing Configuration Summary .....</b>	<b>46</b>
<b>7.6</b>	<b>Final Steps.....</b>	<b>47</b>
<b>8</b>	<b>Message Log Analysis with CMWmars.....</b>	<b>48</b>
8.1	Getting Started .....	48
8.2	Recording Message Logs .....	50
8.3	Analyzing Message Logs .....	52
8.4	Advanced Analysis .....	56
<b>9</b>	<b>Literature .....</b>	<b>57</b>
<b>10</b>	<b>Ordering Information.....</b>	<b>58</b>
<b>A</b>	<b>Installing CMWmars.....</b>	<b>60</b>

# 1 Introduction

The R&S®CMW<sup>1</sup> supports extensive testing of WLAN devices for WLAN implementations as specified in the IEEE 802.11 standards and amendments [1].

Background information and configurations for the following tests and measurements are considered in this document:

- DUT TX measurements of WLAN data frames, testing the transmitter properties of the DUT
- PER measurement, Packet Error Ratio measurement, a kind of DUT RX test since the DUT's receiver properties are analyzed
- Throughput measurements, analyzing the performance of data transmission on the IP layer
- WLAN offloading where IP traffic over LTE is switched to WLAN and back
- End-to-end tests for a DUT acting as access point; one or both ends of the IP data path can be realized with PCs connected to the CMW or the DUT
- WLAN message log analysis with the CMWmars software tool, where IP traffic between the CMW and the DUT is recorded and displayed in log files.

**All tests are based on an established WLAN connection between the CMW and the Device under Test (DUT). For detailed information about connection establishment, see the 1C106 application note [9].**

On the CMW side, the required communication between CMW and DUT is controlled by the WLAN Signaling application which is also responsible for the PER measurements. The DUT TX measurements are performed by the WLAN Measurement application. The throughput measurements, WLAN offloading and the end-to-end tests extend the test area to the IP layer and require that the CMW is equipped with the Data Application Unit (DAU).

The descriptions are confined to SISO tests – one spatial stream – and the WLAN standards 802.11a,b,g,n,ac. Only WLAN channels with 20 MHz bandwidth and SISO configurations are considered.

For information about operation with other WLAN standards, MIMO testing, WLAN channels with 40 MHz bandwidth, WLAN non-signaling measurements and more, see the WLAN user manual [7]. For detailed information about the 802.11ac and 802.11ax standard with bandwidths up to 160 MHz, see the 1CM101 application note [2] and the 1MA222 white paper [4].

Detailed descriptions of DAU applications, used for some measurements (for example IPerf for throughput measurements), and of the LTE Signaling application, required for WLAN offloading, are beyond the scope of this document. Only a basic guideline can be provided for the related tests. For details regarding the DAU and LTE Signaling, see the specific user manuals [5], [6].

---

<sup>1</sup> The R&S®CMW500, R&S®CMW290 or R&S®CMW270 is referred to as CMW in this document.

## 2 Background Information

### 2.1 WLAN Standards and Signal Properties

The figure below shows the WLAN standards for 20 MHz channels which are relevant for this document and the mapping onto CMW parameters. Note that the WLAN Signaling application allows some selections which cover more than one standard.



Fig. 2-1: WLAN standards, data rates (20 MHz channels) and mapping on the CMW “Standard”

Additionally, the 802.11n standard allows 40 MHz channels, the 802.11ac standard allows 40 MHz, 80 MHz, 80+80 MHz and 160 MHz channels which are not considered here.

- OFDM: Orthogonal Frequency Division Multiplex
- DSSS: Direct Sequence Spread Spectrum
- CCK: Complementary Code Keying

## 2.1.1 Coding and Data Rates

The data rates listed in the standards refer to the data part of the WLAN data frames comprising the protocol overhead of the MAC layer and higher layers and the actual payload. The tables show how the data rates are connected with modulations and coding rates and they relate these parameters to bits and symbols.

802.11b				
Data Rate	Modulation	Coding Rate	Mapping	Using
1 Mbit/s	DBPSK	1/11	1 bit	Barker Sequences
2 Mbit/s	DQPSK	2/11	2 bit on 11 IQ values	Barker Sequences
5.5 Mbit/s	DQPSK	1/2	4 bit on 8 IQ values	CCK
11 Mbit/s	DQPSK	1	8 bit on 8 IQ values	CCK

Table 2-1: Data rates and encoding details for 802.11b

802.11a, 802.11g (OFDM)				
Data Rate	Modulation	Coding Rate	Coded Bits per Subcarrier	Data Bits per Symbol
6 Mbit/s	BPSK	1/2	1	24
9 Mbit/s	BPSK	3/4	1	36
12 Mbit/s	QPSK	1/2	2	48
18 Mbit/s	QPSK	3/4	2	72
24 Mbit/s	16-QAM	1/2	4	96
36 Mbit/s	16-QAM	3/4	4	144
48 Mbit/s	64-QAM	2/3	6	192
54 Mbit/s	64-QAM	3/4	6	216

Table 2-2: Data rates and encoding details for 802.11a/g

The relations between the Table 2-2 columns for the standard 802.11a,g (using OFDM) can be reproduced taking into account that a 20 MHz WLAN OFDM channel comprises 48 subcarriers for data (plus 4 subcarriers for pilot signals) and that the transmission time for one symbol is 4  $\mu$ s. The calculation shall be described for the 802.11a standard and the 54 Mbit/s data rate by example:

- Using 64-QAM, one subchannel carries the information of 6 bits ( $2^6 = 64$ ).
- So, the 48 data subcarriers carry  $48 \cdot 6$  bits = 288 bits all together.
- The coding rate of  $\frac{3}{4}$  indicates that only  $\frac{3}{4}$  of the bits represent data after encoding (the additional bits are introduced for error correction). Thus we have  $\frac{3}{4} \cdot 288$  bits = 216 data bits.

One symbol carries 216 data bits in 4  $\mu$ s. This is equivalent to a data rate of  $216 \text{ bits} / 4 \mu\text{s} = 54 \text{ Mbit/s}$ .

802.11n				
MCS	Modulation	Coding Rate	Coded Bits per Subcarrier	Data Bits per Symbol
0	BPSK	1/2	1	26
1	QPSK	1/2	2	52
2	QPSK	3/4	2	78
3	16-QAM	1/2	4	104
4	16-QAM	3/4	4	156
5	64-QAM	2/3	6	208
6	64-QAM	3/4	6	234
7	64-QAM	5/6	6	260

Table 2-3: MCS and encoding details for 802.11n (SISO, 20 MHz)

802.11ac				
MCS	Modulation	Coding Rate	Coded Bits per Subcarrier	Data Bits per Symbol
0	BPSK	1/2	1	26
1	QPSK	1/2	2	52
2	QPSK	3/4	2	78
3	16-QAM	1/2	4	104
4	16-QAM	3/4	4	156
5	64-QAM	2/3	6	208
6	64-QAM	3/4	6	234
7	64-QAM	5/6	6	260
8	256-QAM	3/4	8	312
9 <sup>1)</sup>	256-QAM	5/6	8	346

<sup>1)</sup> Not supported for 20 MHz channels

Table 2-4: MCS and encoding details for 802.11ac (SISO, 20 MHz)

## 2.1.2 Frame Structures

### Data Frames

Data to be transmitted – the payload – is embedded in a MAC frame and the MAC frame is packed in a WLAN physical layer frame. Higher protocol layers (IP, UDP) may also be involved depending on the kind of payload. All layers add additional information, particularly headers, to the payload.

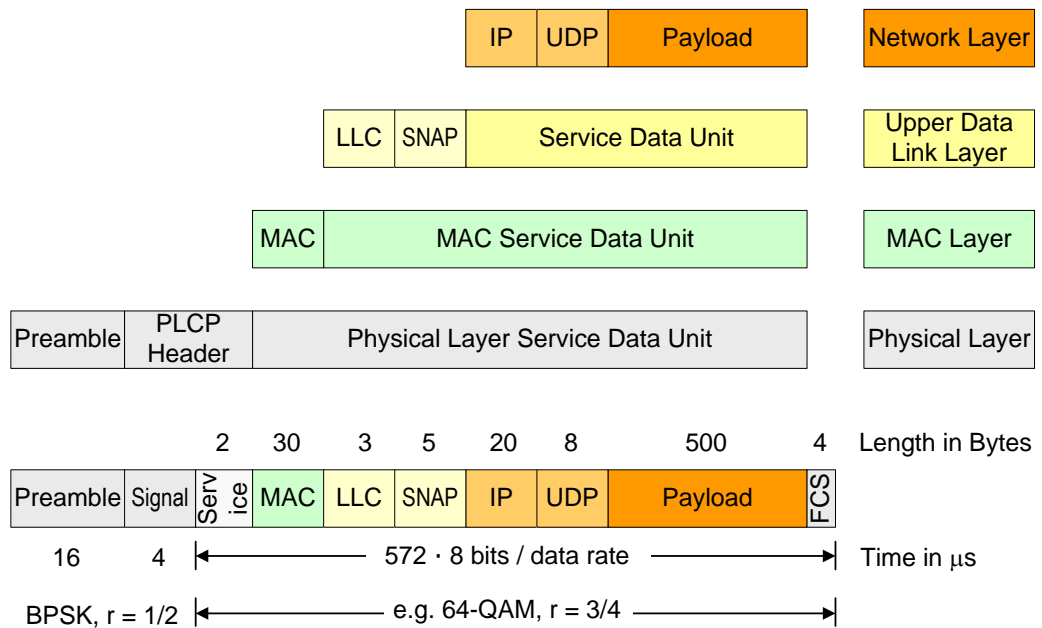


Fig. 2-2: Payload and overhead in data frames

### WLAN Data Frame Lengths

The CMW can filter out WLAN frames whose number of symbols in the data section (after the preamble and the signal part) of a WLAN data frame is too small. The data section includes the payload, the MAC and higher layer headers and – for OFDM bursts – some service and tail bits, all of them encoded according to the selected data rate (while the WLAN header part is always encoded according to the most robust data rate). For OFDM bursts the CMW calculates the number of data symbols with the following formula:

$$\text{Number of Data Symbols} = (\text{MAC \& Higher Layers Overhead} + \text{Payload Length} + \text{Service \& Tail Bits}) / \text{Data Bits per Symbol}$$

The MAC and Higher Layers Overhead is 66 bytes, the Service & Tail Bits add up to 22 bits.

For example, a Payload Length of 500 bytes, in 802.11n with MCS-7 leads to 18 data symbols:

$$\text{Number of Data Symbols} = (66 \cdot 8 + 500 \cdot 8 + 22) / 260 = 18$$

### Acknowledgement (Ack) Frames

Each successful reception of a data frame (and several other frame types) is acknowledged by the receiving device with an Ack frame sent back. Ack frames are short. They do not carry any payload and the MAC header only contains the address of the receiving device. Acknowledgements for DSSS/CCK data frames use the same modulations as the data frames. For acknowledgements of OFDM data frames the small data section of the Ack frames is sometimes modulated with a lower data rate than the data frames, see the following table.



Bit rates for OFDM frames			
Frame type	Data		Ack
IEEE 802.11	a, g	n, ac	a, g, n, ac
Bit Rates in Mbit/s	6, 9 12, 18 24, 36, 48, 54	6.5 (MCS-0) 13, 19.5 (MCS-1, MCS-2) 26 to 65 (MCS-3 to MCS-7) 78, 86.6 (MCS-8, MCS-9) <sup>1)</sup>	6 12 24 48
<sup>1)</sup> 802.11ac only			

Table 2-5: Bit rates for OFDM data frames and corresponding Ack frames

Regarding testing with the CMW, the characteristic property of Ack frames is their short length (24  $\mu$ s). The CMW automatically filters them out if required.

### Beacon Frames

WLAN access points broadcast information required for association via beacon frames. The beacons are usually sent at the lowest mandatory data rate and in intervals of 102.4 ms. On the CMW (acting in access point mode), the beacon interval can be changed in multiples of 1.024 ms. The period of 1.024 ms is called Time Unit (TU).

The beacon frames include the SSID (Service Set Identifier, the name of the WLAN access point used by the WLAN station for access) and BSSID (Basic SSID) information. They also contain information about the supported rates, channel numbers, security requirements, time synchronization and more.

If the CMW acts in Station mode, the beacons from the DUT (acting as access point) might be seen in the measurements. Note that the DUT might use different data rates / modulations for transmitting data frames and beacons.

### 2.1.3 Net Data Rates

This section is not required for DUT TX and PER measurements.

The net data rate specifies the number of payload bits transmitted per second over many frames. Two sources reduce the net data rate compared to the overall WLAN data rate:

- The headers and other overhead information from the different protocol layers.
- The periods with no data transmission. The sender has to pause between two data frame transmissions to get the Ack frame from the receiver. Additionally, all frames are separated by short time intervals. The time interval before the Ack frame is called SIFS (Short Interframe Spacing) lasting 24  $\mu$ s, the time interval before sending a new data frame is called DIFS (Distributed Coordination Function Interframe Spacing) lasting 34  $\mu$ s for 802.11a and 56  $\mu$ s for 802.11g.

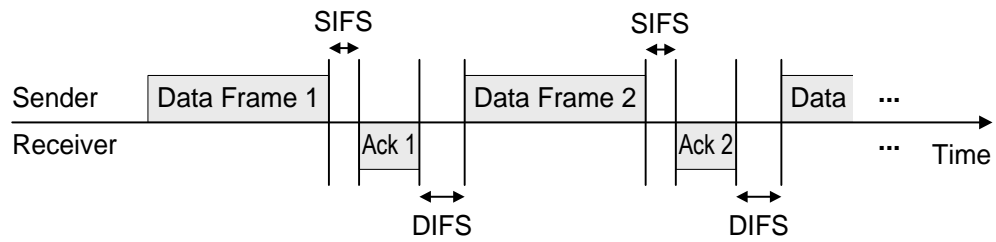


Fig. 2-3: Sequence of data frames with interframe spacing

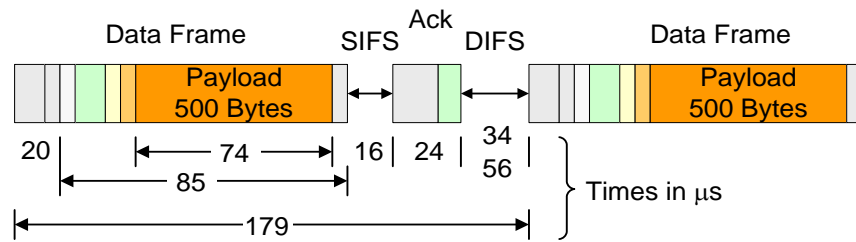


Fig. 2-4: Overhead times (example for 802.11a and 54 Mbit/s data rate)

Referring to the figure above (which itself refers to the figure in the chapter “Frame Structures”), the time spent for the payload transmission is calculated by

Number of bits / data rate.

For  $500 \cdot 8$  bits and 54 Mbit/s we get 74 μs. The overall time from the beginning of one WLAN data frame to the beginning of the next one is 179 μs, so only  $74/179 = 41\%$  of this time is spent on the payload transmission. This means a net data rate of  $54 \text{ Mbit/s} \cdot 41\% = 22.3 \text{ Mbit/s}$ .

## 2.1.4 Transmission Scheme

The following figure complements the previous considerations and shall help to get a full picture. The white spaces after 8, 16, 20, ...  $\mu\text{s}$  represent guard intervals.

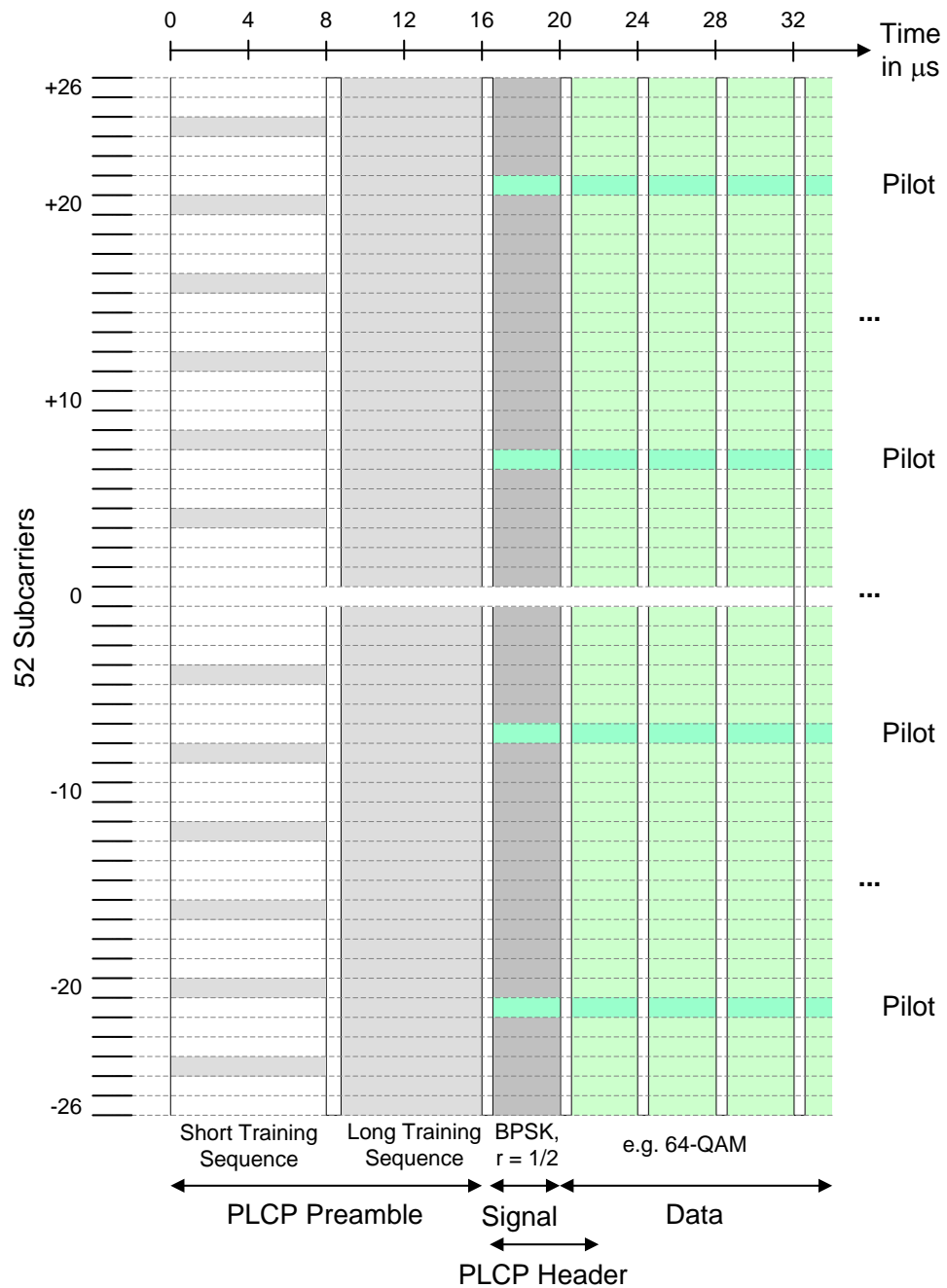


Fig. 2-5: OFDM transmission scheme for 802.11a

48 of the 52 subcarriers of a 20 MHz WLAN channel are used for data transmission, 4 subcarriers carry the pilot signals. The transmission time for one symbol is 4  $\mu\text{s}$ . The pilot signals are always modulated with BPSK.

For more details, see the WLAN 802.11 specifications [1].

## 2.2 Internet Protocol and Routing

IP data exchange and routing in a network is performed using protocols of the Internet protocol suite. The IP connection between the CMW and the DUT is established with the Data Application Unit (DAU). The DAU supports Internet Protocol Version 4 and 6 (IPv4 and IPv6) for this purpose.

### IPv4 Address Format

An IPv4 address is unique within a subnet. The subnet is identified by a subnet mask. Both parameters consist of 32 bits, typically written in dot-decimal notation.

Example: IPv4 address = 192.168.168.170, subnet mask 255.255.255.0, all addresses from 192.168.168.0 to 192.168.168.255 belong to the same subnet.

### IPv6 Address Format

An IPv6 address consists of 128 bits, typically written in blocks of 4-digit hexadecimal numbers, separated by a colon. Addresses can be abbreviated by omitting leading zeros within a block and by replacing consecutive blocks of zeros by a double colon (only once per address).

Example with equivalent addresses:

- fcb1:cafe:0001:86c1:0000:0000:0000:0001
- fcb1:cafe:1:86c1:0000:0000:0000:1
- fcb1:cafe:1:86c1::1

### IPv6 Prefix:

The initial bits of an address are called prefix and identify the subnet. The maximum length of the prefix is 64 bits. The remaining bits are called interface identifier and uniquely identify a link within a subnet.

The DAU must know both its own address and the prefix identifying its subnet. This information can be combined into a single string by appending the prefix length to the address. Example: The address fcb1:cafe:1:86c1::1 with the initial 64 bits identifying the subnet can be written as fcb1:cafe:1:86c1::1/64.

IPv6 prefixes are written in the same notation (address + length). Prefixes with less than 64 bits indicate a whole group of 64-bit prefixes with the same initial digits.

Examples for IPv6 prefixes:

- 64-bit prefix: fcb1:cafe:0001:86c1:0000:0000:0000:0001
- Abbreviations: ac42:45d2:0001:0000::/64  
= ac42:45d2:1:0::/64  
= ac42:45d2:1::/64
- Prefix groups: fcb1:cafe:0001::/48 comprises the 64-bit prefixes fcb1:cafe:0001:0000::/64 to fcb1:cafe:0001:ffff::/64

*IPv6 Interface Identifier:*

The last 64 bits of an IPv6 address are called interface identifier (IID) and define the unique network interface based on the MAC address. The MAC address, which consists of 48 bits, is therefore enlarged to 64 bits using the Modified Extended Unique Identifier (EUI-64).

Modified EUI-64 conversion of a MAC address to an IID, exemplary on the CMW:

1. CMW's MAC address: 00-90-B8-01-FF-F1
2. Splitting of the CMW's MAC address into 24-bit blocks  
 Organisationally Unique Identifier (OUI): 00-90-B8  
 Network Interface Control (NIC): 01-FF-F1
3. Addition of the 16-bit pattern "FF-FE" to the middle of the split MAC address
4. Replacing the seventh bit by "1" in the OUI block
5. Modified EUI-64 IPv6 Interface Identifier: 02-90-B8-FF-FE-01-FF-F1

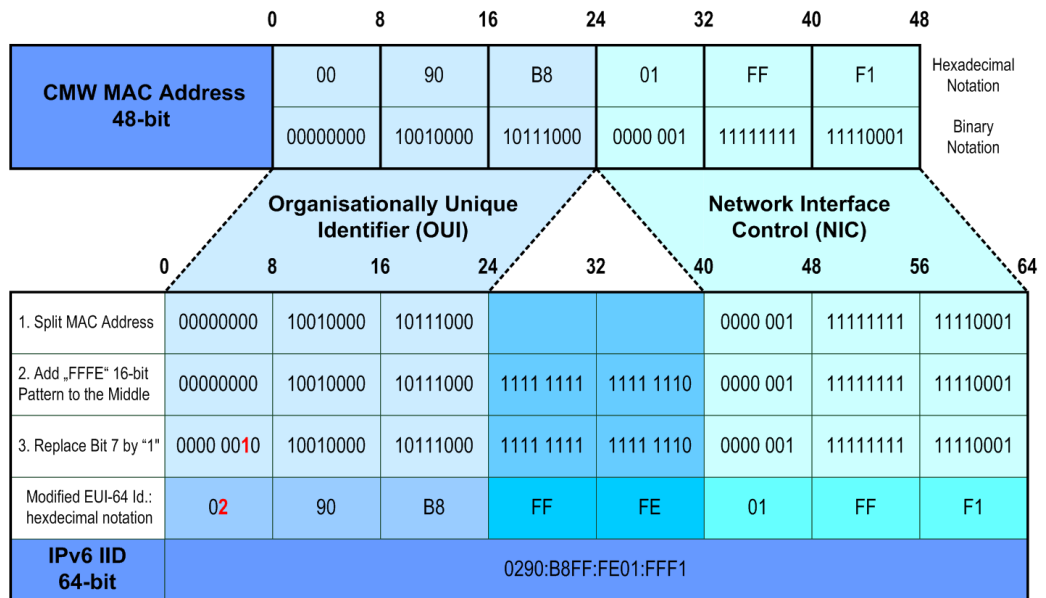


Fig. 2-6: IPv6 Interface Identifier conversion of the MAC address via Modified EUI-64

*IPv6 address:*

The total IPv6 address consists of the 64-bit prefix and the 64-bit interface identifier. With the examples given above a total IPv6 address for the CMW is given in the figure below.

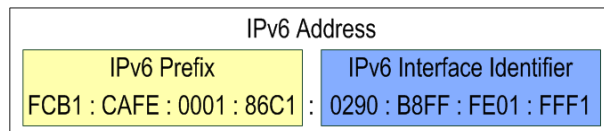
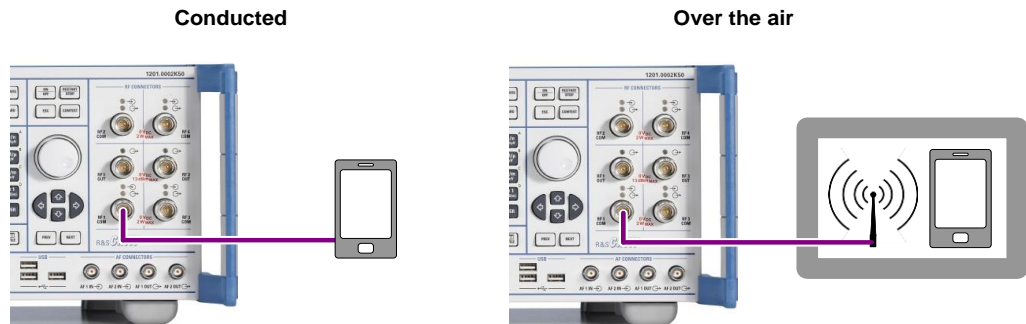


Fig. 2-7: Example for an IPv6 address of the CMW

### 3 Test Setups

The device under test (DUT) is connected to one of the bidirectional RF COM connectors at the front panel of the CMW. No additional cabling and no external trigger is needed. The input level ranges of all RF COM connectors are identical.



**Fig. 3-1: Test setups, WLAN only**

The “Conducted” test setup is the easiest and preferred solution since it avoids power loss by over-the-air radio transmission.

In case of testing over-the-air via antennas, it is recommended to encapsulate the DUT and the RF antenna for the CMW in an RF shielding box. Thereby interference from any WLAN access point and other devices using WLAN or Bluetooth is avoided. The over-the-air RF connection causes a power loss of 15 dB or more compared to the conducted RF connection. The path loss without RF shielding box would be much higher (typically about 30 to 39 dB compared to the conducted RF connection).



**Fig. 3-2: R&S®CMW-Z10 RF shielding box**

Notes on using the R&S®CMW-Z10 RF shielding box:

- Position the DUT at the center of the box.
- A small displacement of the DUT in the RF shielding box can result in an additional external attenuation of about 10 dB.
- The optimum position of the DUT depends on its antenna arrangement. So try out several DUT positions around the center of the box.
- Close the RF shielding box cover in order to ensure that no interference by other WLAN devices operating in the same channel can occur.

See the 1C106 application note [9] for appropriate configuration of the RF power related parameters.

The test setups shown above are valid for all operating modes described in the table.

Mode of the CMW	Mode of the DUT
<b>Access Point (AP) mode</b> The CMW operates as WLAN access point that allows to perform tests on an associated WLAN station.	<b>Station (STA) mode</b>
<b>Station (STA) mode</b> The CMW operates as WLAN station that allows to associate with and to perform tests on a WLAN access point.	<b>Access Point (AP) mode</b>
<b>IBSS mode (= STA in IBSS mode)</b> Allows WLAN stations to communicate directly with each other without the need of a dedicated wireless access point. This type of operation is often referred to as ad hoc network.	<b>Station (STA) in IBSS mode</b>
<b>Hotspot 2.0 / Wi-Fi Direct mode</b> The CMW simulates a Wi-Fi Hotspot 2.0 access point or Wi-Fi direct group owner. Requires R&S®CMW-KS660 "WLAN advanced signaling" option.	<b>Station (STA) as Hotspot 2.0 or Wi-Fi Direct client</b>

Table 3-1: Operating modes

### WLAN Offloading

For WLAN offloading the WLAN and the LTE Signaling applications must use different TRX modules.



Fig. 3-3: Test setup, WLAN offloading

### End-to-end Test with LAN-connected PC

Use the "LAN DAU" connector on the rear panel of the CMW.



Fig. 3-4: End-to-end test setup with LAN-connected PC

### Message log analysis with CMWmars

CMWmars is running on a LAN-connected PC.  
Use the "LAN SWITCH" connector on the rear panel of the CMW.



Fig. 3-5: CMWmars PC LAN-connected with the CMW



## 4 TX (DUT) Tests with Packet Data

### Combined Signal Path

TX tests are executed in combined signal path mode, i.e. the WLAN Signaling and WLAN Measurement applications work together with the WLAN Measurement application using some parameters of the WLAN Signaling application.

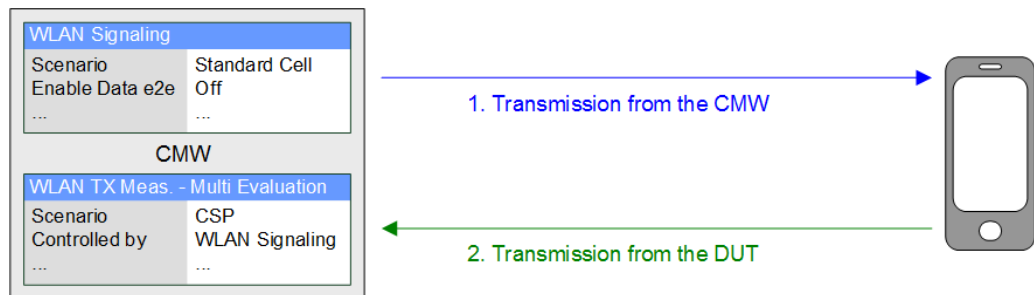


Fig. 4-1: Combined Signal Path (CSP)

### Packet generators

The packet generator used by the main WLAN signaling configuration and the packet generator for PER measurements are different applications and can be operated independently.

## 4.1 Tests with IP packets

### 4.1.1 Test Principle

IP packet exchange between the CMW and the DUT is based on the Internet Control Message Protocol (ICMP) Echo implementation:

- The WLAN Signaling application packs Echo Request ("Ping") packets into WLAN data frames and transmits them to the DUT.
- The DUT acknowledges the received WLAN data frames and responds with Echo Reply packets, which ideally contain the same WLAN data frames.
- The WLAN Measurement application receives the WLAN acknowledgement and data frames. It skips the Ack frames and analyzes the Echo Reply data frames.

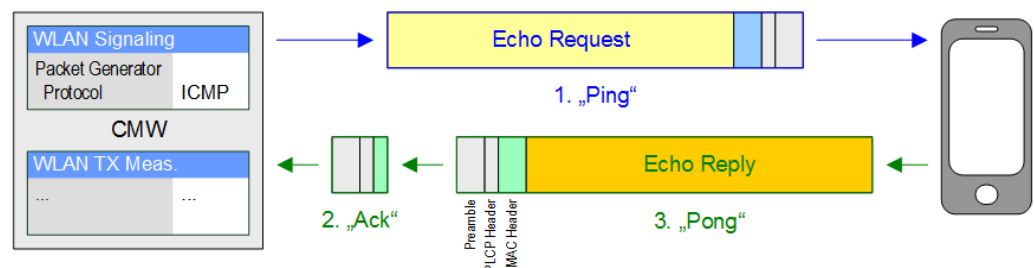


Fig. 4-2: ICMP Echo principle: Request/Reply packets for TX tests

The content of an ICMP Echo Reply packet is identical with that of the corresponding ICMP Echo Request packet. This allows the WLAN Signaling application on the CMW to define the payload of the WLAN frames to be received from the DUT and analyzed. The WLAN Signaling application provides an ICMP packet generator where the payload length of the Echo Request packet and other details can be configured.

For identifying the desired received WLAN frames and synchronizing the reception of the frames with the measurement start, the CMW uses a MAC Frame RX Trigger (located in the WLAN Signaling application but also used by the WLAN Measurement application). This trigger detects the preamble and the PLCP header of WLAN frames and the starting point of the MAC header. It allows to filter for OFDM bursts or DSSS/CCK bursts and to define a minimum data length of MAC header plus payload. The very short Ack frames are automatically skipped.

#### 4.1.2 Configuring Packet Data transfer

For transmitting data of a defined type and length you have to configure the packet generator in the main WLAN signaling configuration. For receiving WLAN frames of a selectable transmission mode and data length the Frame RX Trigger is provided.

*Packet Generator:*

1. In the "Packet Generator Configuration" panel on the GUI, select the "Protocol" "ICMP" which realizes "Ping" data frames for TX Tests.
2. Set the "Payload Size" to 600 Byte(s). For the 802.11b standard (with its low data rates) it is sufficient to have a payload size of 300 bytes.
3. Switch on the packet generator with the "On" radio box.

Packet Generator	Data Frame Control	
State	<input type="radio"/> Off	<input checked="" type="radio"/> On
Protocol	ICMP	
Interval (TU)		100
Payload Size (Byte)		600
Payload Type	Default	

Fig. 4-3: Packet generator configuration

Note: A "Payload Size" of 600 bytes ensures that the data frames contain at least 18 OFDM symbols up to the highest modulation rate. 16 OFDM symbols at minimum are required according to IEEE specifications and for a reliable frame analysis.

*Trigger:*

WLAN frame triggers are permanently enabled without user action. The "MAC Frame RX Trigger" is the critical one for WLAN measurements.

4. Open the configuration dialog of the WLAN Signaling application via the "Config..." key and expand the "Trigger" node.
5. Under "MAC Frame RX Trigger", select the "Trigger Mode":
  - "OFDM Bursts" in case of OFDM data frames (e.g. for standard 802.11a)
  - "DSSS/CCK Bursts" in case of DSSS data frames (e.g. for standard 802.11b)

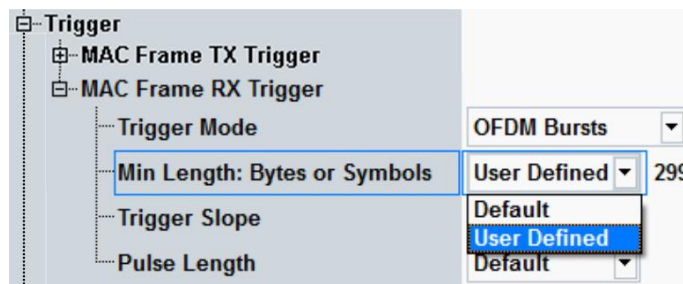


Fig. 4-4: MAC Frame RX Trigger

Note: You can further refine the Trigger setting by selecting a "Modulation Filter" appropriate for the expected input signal at the WLAN measurement application.

6. Select "User Defined" for the "Min Length: Bytes or Symbols" and enter the payload size:
  - "18" in case of OFDM data frames (e.g. for standard 802.11a)
  - "299" in case of DSSS data frames (e.g. for standard 802.11b)
7. Close the configuration dialog.
8. For DSSS/CCK data frames (e.g. for standard 802.11b), set the "RX filter" to "Auto" (recommended).



Fig. 4-5: RX filter

The "RX Filter" provides predefined or adaptive inter-symbol interference filters for CCK signals, i.e. for the data rates 5.5 and 11 Mbit/s. This filter allows to adapt the receiver to CCK input signals. The "Default" and "Alternative" values provide two alternative predefined, static filters. "Auto" provides an adaptive filter. For the 2.4 GHz band, it is recommended to set the "RX Filter" to "Auto". If the association fails, the selected RX Filter might be unsuitable, so change your selection.

#### Rate:

"Rate" in the "Management Frame Rate Control" and "Data Frame Rate Control" sections define transmission rates from the CMW to the DUT. Generally, you can keep the default setting.

Note: Even frame rates can be selected that are incompatible with the configured supported rates.

Note: Disconnecting and turning off the signaling application sets the packet generator to Off. So, take care that the packet generator is On during the measurement.

### 4.1.3 TX (DUT) Measurement

The TX measurements are executed by the WLAN Measurement application which operates in combined signal path mode. Hence, the measurement application takes several settings (like connectors, frequency) from the WLAN Signaling application.

*Starting situation:*

The WLAN Signaling application has been configured and the connection between CMW and DUT has been established. See the 1C106 application note for details [9].

Generation of packet data at the CMW has been configured within the WLAN Signaling application as described in the previous chapter.

Proceed as follows:

1. In the WLAN Measurement application, open the configuration dialog via the "Config ..." key.
2. Make sure that the "Scenario" is set to "Combined Signal Path (Signaling)" and that it is "Controlled by" the active "WLAN Sig" application.



Fig. 4-6: Combined signal path scenario

3. In the WLAN "Input Signal" section:
  - a) Set the "Standard" according to the settings in the WLAN signaling application.
  - b) Select the "Modulation Filter" according to the expected modulation of the data frames to be measured.

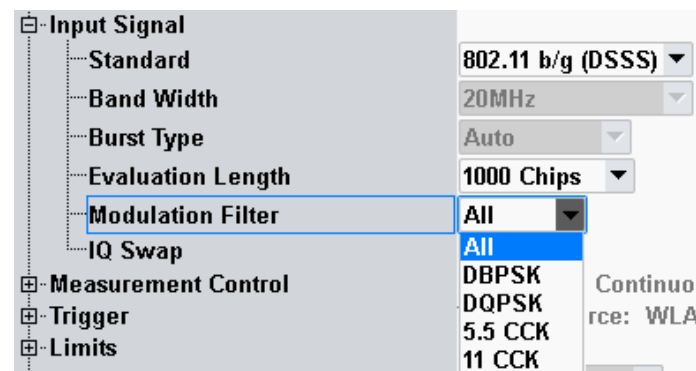


Fig. 4-7: WLAN standard and Modulation Filter (for Combined Signal Path only)

Note: The "Modulation Filter" is only available in the "Combined Signal Path" scenario and refines the "MAC Frame RX Trigger" setting of the WLAN Signaling application. It allows to limit the evaluation to bursts of a particular modulation type. This helps to filter out the beacons from the DUT (acting as WLAN access point) since the beacons are usually sent at the lowest mandatory data rate with the most robust modulation.

4. Set/check the trigger parameters:
  - "Trigger Source": "WLAN Sig1: RXFrameTrigger"  
(this is the default value in case of combined signal path)
  - "Trigger Slope": "RisingEdge"  
The default values of the other trigger parameters can be kept. The trigger threshold is related to the Expected Peak Envelope Power.



Fig. 4-8: WLAN frame trigger

5. Close the configuration window.
6. Press ON | OFF to start the measurement.

Check if the measurements produce reasonable results by monitoring the properties of the received signals in the "TX Measurement (Scalar)" view.

Notes:

- "Sync Errors" will occasionally be displayed in case of a WLAN standard applying DSSS. This does not affect the measurement results.
- Occasionally, "Underdriven" input and "Trigger Timeout" is indicated. This does not affect the measurement results.

## Check of Successful Operation with Measurement Results

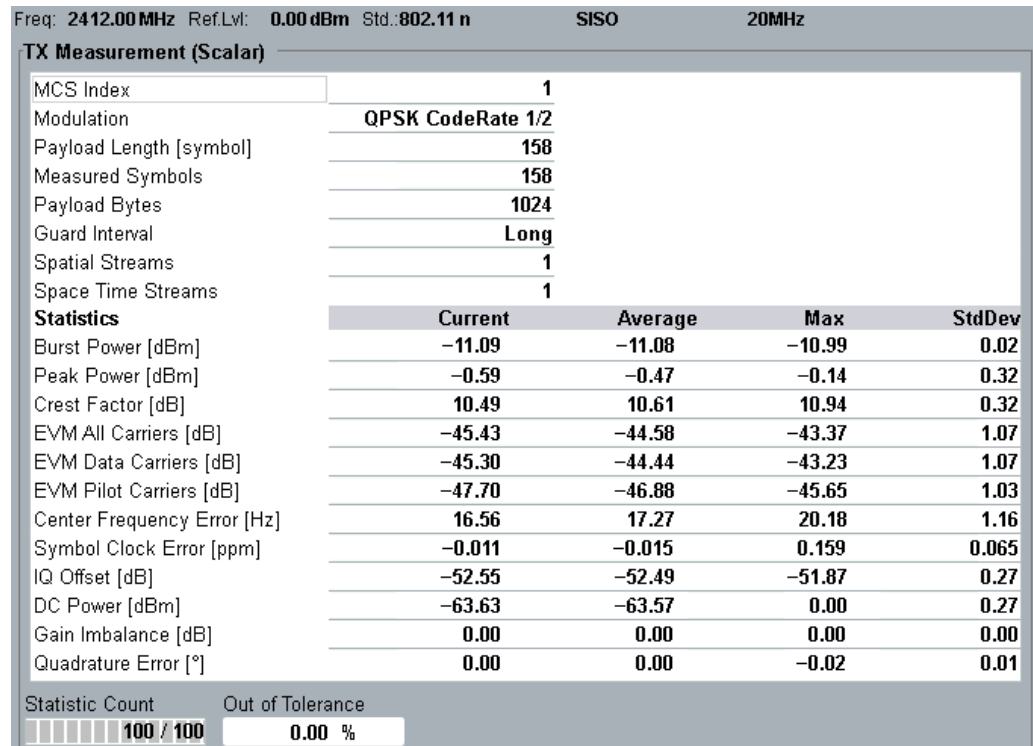


Fig. 4-9: TX measurement (scalar)

At the WLAN Measurement application, the views "TX Measurement (Scalar)" and "Power vs. Time" can be used to check if the test configuration is appropriate. E.g. check the "Payload Length [symbol]" value in "TX Measurement (Scalar)" to verify that data frames are measured and not Ack frames.

## 4.2 PER Measurements with MAC packets

### 4.2.1 Test Principle

Packet Error Ratio (PER) measurements are carried out by the WLAN Signaling application. The generator from the WLAN PER window does not use IP frames. Instead a MAC Data request containing just a text string as payload is sent to the DUT:

- The WLAN Signaling application packs MAC data packets into WLAN data frames and transmits a certain number of them – all with identical payload – to the DUT.
- On successful reception, the MAC layer of the DUT acknowledges the received WLAN data frames with WLAN Ack frames.
- The WLAN PER Measurement application receives the WLAN Ack frames and counts their number.
- PER is calculated as the ratio of unacknowledged packets to transmitted packets.

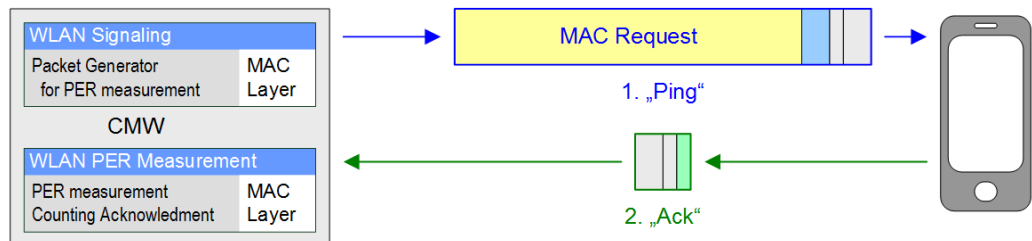


Fig. 4-10: PER measurement principle

Notes:

- The CMW does not retransmit unacknowledged packets.
- The DUT will pass the MAC frame data to its next layer, but this layer will recognize that it is no IP frame inside and discard the data.

### 4.2.2 PER Measurement

To access the measurement, press the softkey "WLAN PER" in the WLAN signaling main view. The following procedures are valid, when this softkey is active.


1. Press the "Config" hotkey to open the PER configuration dialog. You can keep the default settings.



Fig. 4-11: PER configuration dialog

*Modulation Coding Rate in the PER view*

- Select the "Modulation Coding Rate" expected for the transmitted MAC data frames (Fig. 4-12:).

Results		Cell Settings	
PER	0.20 %	TX Burst Power	-16.00 dBm
Packets	 1 000 / 1000	<b>Traffic Burst</b>	
Packets Lost	2 Frame	Frame Format	Non HT
RX Burst Power	-28.56 dBm	Channel Bandwidth	20MHz
Last Ack Rate	QPSK 1/2 12Mbps	Modulation Coding Rate	QPSK 3/4 18Mbps
		Guard Interval	Long

**Fig. 4-12: PER view results and settings**

Note that in case of an OFDM transmission mode, a more robust modulation and coding rate/scheme may be used for the ACK frames than for the acknowledged data frames, so the value of "Last Ack Rate" and "Modulation Coding Rate" may differ in these cases.

- Press ON | OFF to start the measurement.

Note: Disconnecting and turning off the signaling application sets the packet generator to Off. So, take care that the packet generator is On when measuring.



## 5 Throughput Test

### 5.1 Test Principle

- The Data Application Unit (DAU) extends the connection to the IP layer.
- The throughput measurement is executed on the DAU using the IPerf module. IPerf must also run on the DUT.

The CMW acts as access point (for testing with the CMW in “Station” mode, see chapter 7 “End-to-End Tests for Access Point DUTs”).

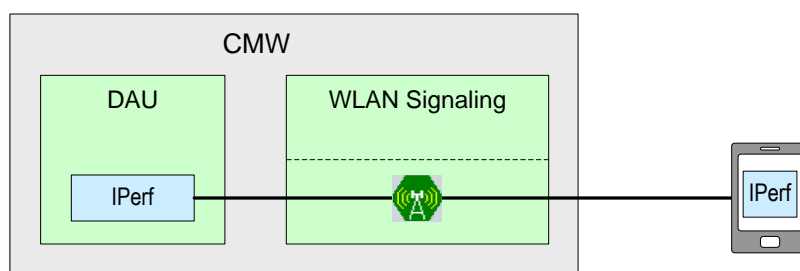


Fig. 5-1: IPerf throughput test

### 5.2 Configuring Throughput Measurements

The throughput measurement is done with IPerf on the Data Application Unit (DAU). The IPerf tool must also run on the DUT. The measurement shows the properties of the IP data reception.

Detailed descriptions of DAU and IPerf configurations are beyond the scope of this document. For details regarding the DAU, see the DAU user manual [5].

The DAU network configuration must be complete before switching on WLAN Signaling and establishing the connection to the DUT. The WLAN Signaling application relays incoming DHCP requests to the DAU.

#### Starting Situation

- The DUT is connected with the CMW.
- WLAN Signaling is in OFF state.
- The WLAN Signaling application is configured for WLAN association and with operation mode AP, Hotspot 2.0 or Wi-Fi Direct.
- IPerf is available on the DUT and configured (the settings are equal to the settings on the DAU, for details see the DAU user manual [5]).

**Procedure**

*At the DAU application:*

1. To open the "Data Application Control" dialog, press "Setup", and in the "Setup" dialog in the "System" section press the "Go to config" button.
2. Setup the "IP Configuration", particularly the IP address used at the DAU end of the data path.
3. To open the "Data Application Measurements" dialog, press the MEASURE key. Then enable "Data Appl. > Measurements" and press "Data Meas" on the task bar at the bottom.
4. At the top of the "Data Application Measurements" dialog select the WLAN Signaling application at "Select RAN".

*At WLAN Signaling:*

5. Make sure that the "IP Version" setting is consistent with the DAU's IP configuration.
6. Switch on the WLAN Signaling application.  
The WLAN connection between CMW and DUT is established. The DUT receives its IP configuration from the DAU's DHCP server.
7. Find out which IP address has been assigned to the DUT.

*At the DAU application:*

8. If you want to verify that the IP connection is all right:
  - a) Activate the Ping measurement (via the "Measurement Controller" dialog, entry "Data Appl. > Measurements") and access the "Ping" measurement tab via Task bar.
  - b) For "Destination IP" enter the IP address of the DUT.
  - c) Start pinging the DUT.
  - d) Verify that the DUT replies the Ping requests. Then stop pinging.
9. Select the "IPerf" tab.
10. Open the "IPerf Config" dialog via the "Config" hotkey and adjust the settings according to your needs ("Test Duration", "Packet Size", "UE IP Address", ...).

Start the IPerf measurement and monitor the IP performance.

## 6 WLAN Offloading

Offloading is commonly used to shift IP data traffic from cellular networks (e.g. LTE) to non-cellular broadband networks (e.g. WLAN). This chapter describes how IP data traffic originating from a voice or video call over LTE is shifted in the presence of a stronger WLAN signal.

The CMW simultaneously emulates an LTE base station and WLAN access point. This is provided by a CMW with two SUAs, since the LTE and WLAN Signaling applications must be active in parallel and use different TRX modules. Additionally, the Data Application Unit (DAU) controls the IP traffic at the CMW to induce the offloading process. A comprehensive overview about required components at the CMW and DUT is given in Table 6-1:

Prerequisites for WLAN Offloading		
Instrument	Required components	R&S option
CMW500	Signaling Unit Advanced (SUA) WLAN Signaling application LTE Signaling application DAU application IPv4 or IPv6 enabler IMS basic software WLAN Offloading test software	CMW-B500I CMW-KS650, -KS651 and -KS660 CMW-KS500 (FDD) or -KS550 (TDD) CMW-B450A, -B450B, -450D and -450H CMW-KA100 or -KA150 CMW-KAA20 CMW-KA065
DUT	Voice/Video over LTE support "Wi-Fi Preferred" operation mode	-

Table 6-1: Soft-, hardware and feature requirements at the CMW and DUT for WLAN offloading

### 6.1 Test Principle

- A voice or video call over LTE is established using the LTE Signaling application and the IMS service of the DAU application.
- The ePDG service on the DAU allows to connect WLAN with the IP network used for LTE Signaling.
- When the DUT detects strong signals from the WLAN access point provided by WLAN Signaling, it automatically switches from LTE to WLAN.
- An IPsec tunnel for the IP traffic between ePDG and DUT is established.
- The characteristics of the IP traffic are analyzed with DAU measurements.

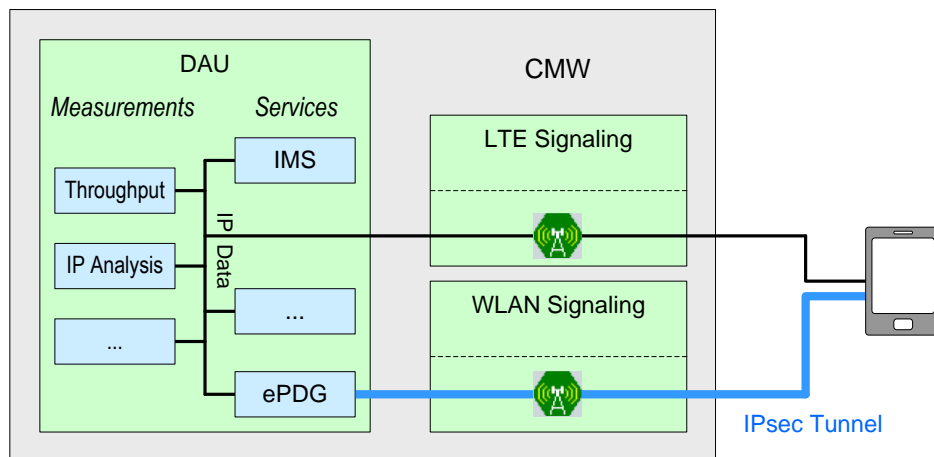


Fig. 6-1: IP data routing at the CMW for WLAN offloading

## 6.2 Configuring WLAN Offloading

Detailed descriptions of LTE Signaling and DAU configurations are beyond the scope of this document. For a comprehensive description, see the LTE and DAU user manual [6], [5].

### Starting Situation

- The DUT is connected with the CMW as described in chapter 3 (Fig. 3-3).
- The WLAN Signaling application is configured for WLAN association and in OFF state or at low "TX Burst Power", e.g. -100.00 dBm. See the 1C106 application note for details [9]. WLAN Signaling operates in AP, Hotspot 2.0 or Wi-Fi Direct mode.
- An LTE end-to-end connection is configured, a voice or video call is ready to be activated (see the LTE and the DAU user manual for details).

### Procedures

*At the LTE Signaling application:*

1. In section "RF Settings", set "External Attenuation" values:
  - E.g. 15.00 dB when using an RF shield box for a wireless DUT-CMW connection.
  - E.g. 2.00 dB for a wired DUT-CMW connection.

Note: The values for the external attenuation result from testing procedures. The optimal setting depends on the manufacturer of the DUT.

2. Configure the section "Network" settings compatible to your DUT:
  - a) Check sections "Identity", "Security Settings" and NAS Signaling
  - b) In section "NAS Signaling" particularly:
    - Enable "EPS Network Feature Support".
    - Set "IMS Voice Over PS Session Indicator" to "Supported".

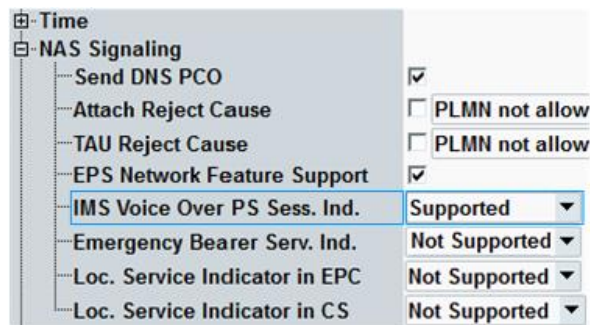


Fig. 6-2: LTE Signaling network settings

3. In section "Connection", set "Connection Type" to "Data Application".
4. Disable "Use 'Activate Testmode' Message"



Fig. 6-3: LTE Signaling connection settings

At the DAU application:

5. Press "Setup" to open the "Setup" dialog.
6. In the "System" section press the "Go to config" button.  
The "Data Application Control" dialog opens.
7. Switch on the DAU, unless it is already switched on (default setting).
8. In the "ePDG" tab, configure the ePDG settings compatible to your DUT.
  - a) The "ePDG IP address" within "ePDG IP Configuration".
  - b) The "ID Type" and ID value within "ePDG ID Configuration".
  - c) The "P-CSCF IKEv2 Attribute" and "Authentication Data" settings.

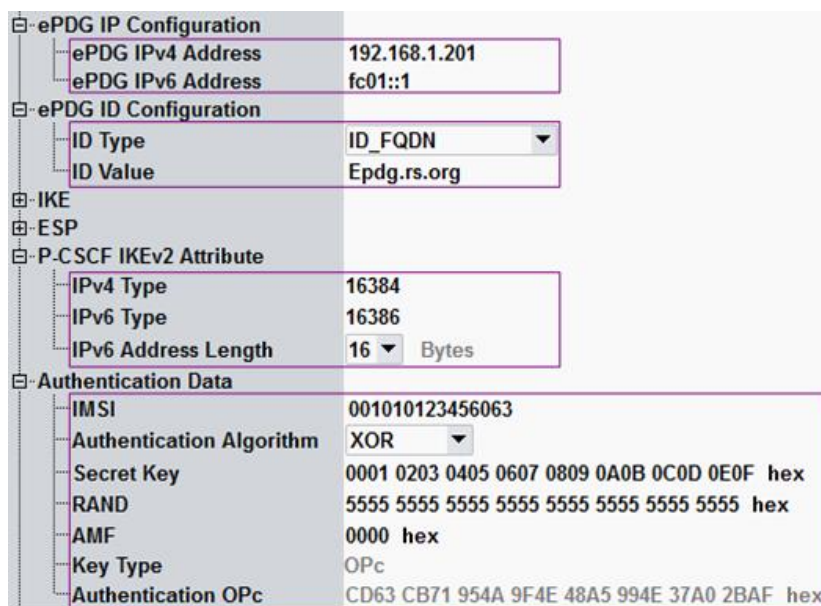


Fig. 6-4: DAU ePDG configuration

The ePDG identifies itself according to these settings in messages to the DUT.

9. Switch on the IMS service.
10. Switch on the DNS service.
11. Switch on the ePDG service.

Notes:

The ePDG domain depends on the manufacturer of the DUT. If the domain is unknown there is no entry "epdg.xxx" in the DNS tab, section "Local DNS entries" -> column "Domain". You can find out the ePDG domain by sending a DNS request and manually add the two domain entries. The procedures a)-d) are only required once per DUT.

- a) Repeat the previous procedures 1.-9. .
- b) In the "DNS req." tab of the Data Application Measurement dialog:
  - Switch on the "DNS Requests" measurement.
  - Search the "Requested Domain/Application" area in the event log for "epdg.xxx" related domain entries.
- c) In the "DNS" tab of the Data Application Control dialog:
  - Add the two "epdg.xxx" related domain entries as requested by the DUT into the "Local DNS Entries" -> "Domain" column.
  - Check the IP address in the "IP" column. The address must be identical with the address configured in the ePDG IP configuration dialog (see point 8.a)).
- d) Proceed with step 10. above.

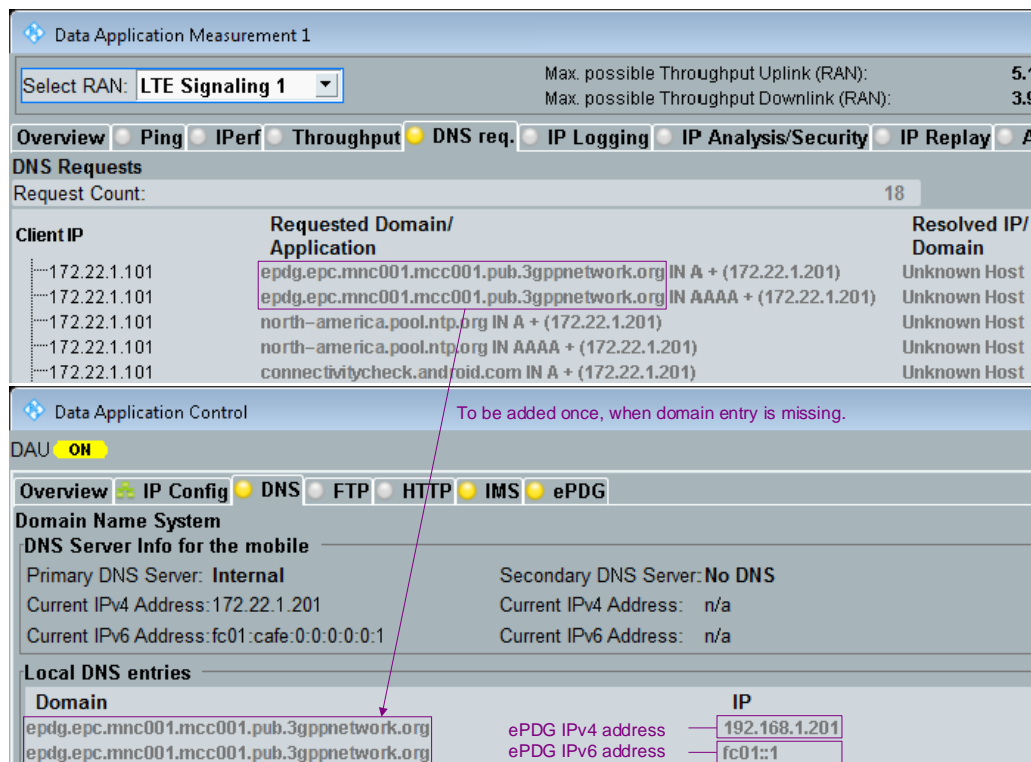


Fig. 6-5: DNS request and DNS tabs

You may have to repeat the procedures a)-e) above, when using another DUT.

At the LTE Signaling and DAU application:

12. Switch on the LTE Signaling application in order to attach the DUT to the LTE cell.
13. Monitor the IMS registration in the "IMS" tab -> "General IMS Info" section. The IMS client at the DUT will register to the IMS server of the CMW.
14. Start the voice or video call by dialing a random number on the DUT. The IMS server will pick up this call as displayed in the IMS server log.

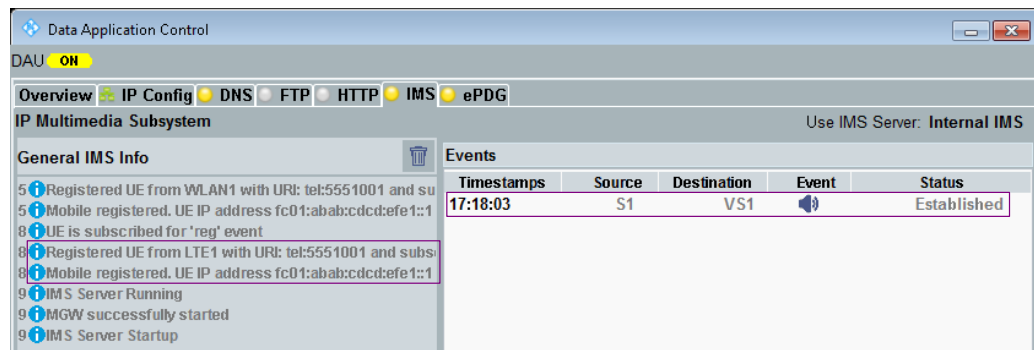


Fig. 6-6: IMS registration and established VoLTE call info

Note: Dedicated bearers are not supported for WLAN Offloading over the audio board (R&S®CMW-B400B).

At the WLAN Signaling application:

15. Make sure that the "IP Version" conforms with the DAU's IP configuration.
16. Switch on the WLAN Signaling application.
17. Make sure that the "TX Burst Power" of the WLAN signaling application is set high enough, e.g. -16.00 dBm, so that the DUT prefers it to the LTE network. The WLAN connection between CMW and DUT is automatically established and the data transfer is switched from LTE to WLAN. When connecting for the first time it is normally necessary to connect manually at the DUT side.

At the DAU application:

18. Monitor the offloading. You can use the following sources:
  - The DUT lists the access point within its list of available WLAN access points.
  - In the WLAN Signaling application main view, the connection state changes to "Associated".
  - In the LTE Signaling application main view, the list of established bearers is reduced by one entry.
  - In the ePDG service main view, a new connection is listed.
19. To hand over the connection back to LTE, reduce the "TX Burst Power" at the WLAN Signaling application, e.g. to -100.00 dBm.

20. Monitor the process. You can use the following sources:
  - The DUT lists the access point with very low power or not at all.
  - In the LTE Signaling application main view, a bearer is added to the list of established bearers.
  - In the ePDG service main view, the IMS connection is released.
  
21. Start the throughput measurement and monitor the throughput to verify that IP data is transmitted.
 

Fig. 6-7 shows a throughput measurement of LTE and WLAN IP traffic. The stronger signal determines which RAN throughput dominates.

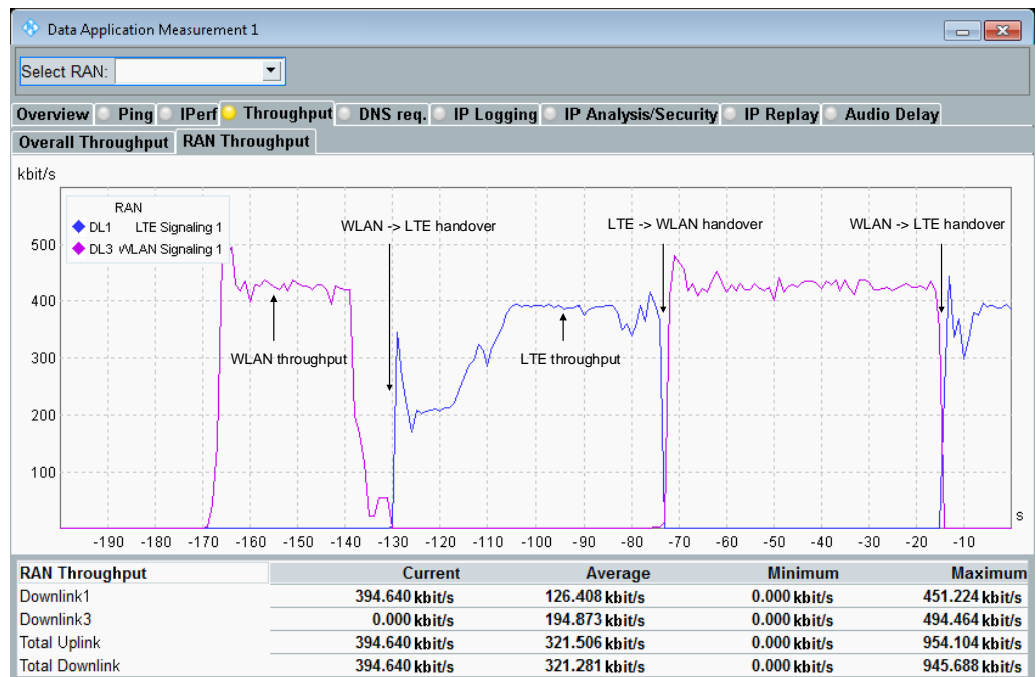


Fig. 6-7: WLAN offloading in data throughput measurement



## 7 End-to-End Tests for Access Point DUTs

“End-to-end” indicates that the test scenarios are not confined to WLAN conditions but are extended to IP data exchange over WLAN. The data source and destination can reside inside the CMW and the DUT or in connected network devices.

The following subchapters introduce three test scenarios / IP data paths with increasing complexity:

- Path A (one subnet test scenario): CMW - DUT (- PC over LAN)
- Path B (two subnets test scenario): PC - CMW - DUT - PC over LAN
- Path C (three subnets test scenario): PC - CMW - DUT - PC over WAN

A summary of starting instructions as well as final steps, which are the same for all test scenarios, provide the framework. Among the test principle, detailed configuration steps and relevant parameters are described for each test.

The configuration effort becomes quite large for the more complex test scenarios. The test scenario chapters are therefore followed by an overview of the IP settings for all paths.

### 7.1 Starting Situation

- The DUT, CMW and PC(s) are connected according to the test setup.
- The WLAN Signaling application is configured for WLAN association with the CMW in Station Mode (see the application note 1C106 for details [9]).
- WLAN Signaling is in OFF state.

## 7.2 One Subnet: CMW - DUT (- PC over LAN)

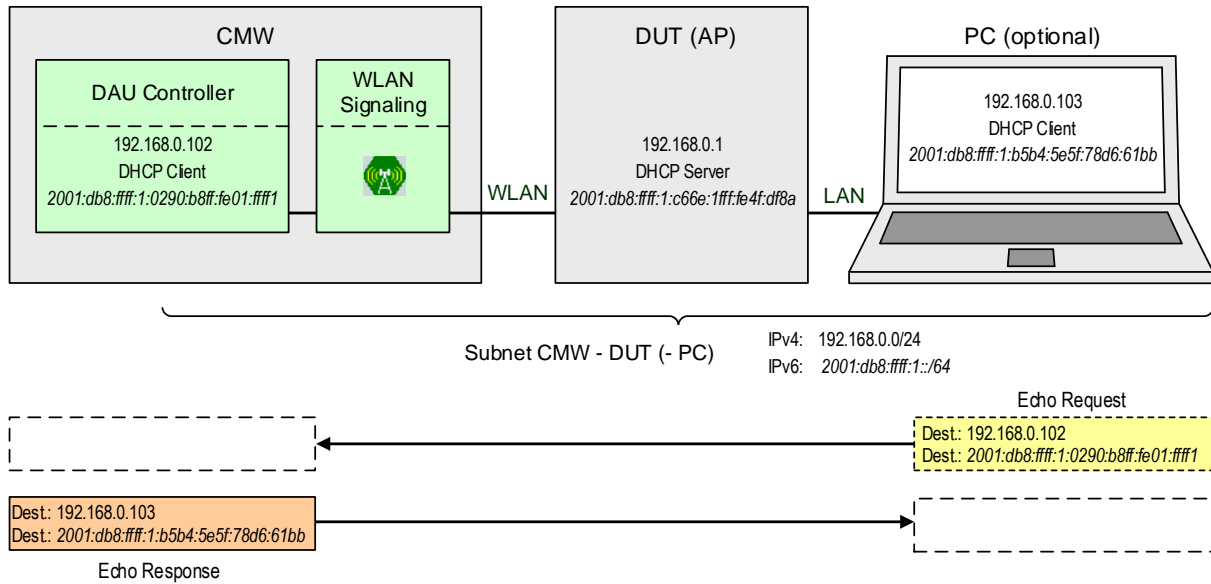


Fig. 7-1: End-to-end test with one subnet, Path A

### 7.2.1 Test Principle Path A

- The DUT acts as access point.
- The DAU Controller provides the IP interface on the CMW for data transmission.
- The access point may route data between the CMW and an external network device, here a LAN-connected PC.
- DHCPv4 mechanism: For IP connection establishment between the DAU on the CMW and DUT, the DHCPv4 server of the DUT is used. The CMW provides the DAU's MAC address to the DUT and the DUT assigns an IP address to the DAU.



Fig. 7-2: DHCPv4 message sequence

- NDP mechanism: The IP connection between the DAU on the CMW and the DUT is established using the Neighbour Discovery Protocol (NDP). A Router Solicitation message from the CMW's DAU is sent to the DUT via NDP. In response, a Router Advertisement message from the DUT containing the IPv6 Prefix is sent.

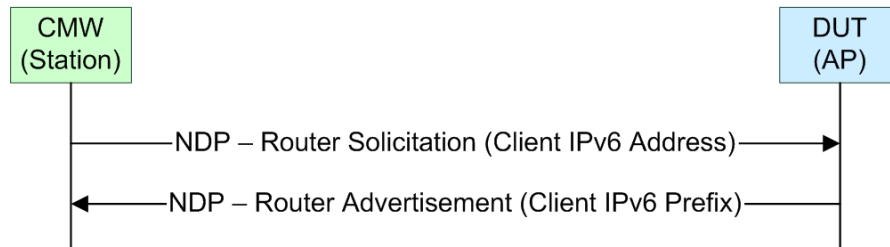


Fig. 7-3: NDP message sequence

Note: DHCPv6, which, similarly to NDP, is used to establish an IP connection based on IPv6, is currently not supported.

### 7.2.2 Configuring Path A

The IP version, which is supported by the DUT and PC, is the only relevant parameter on the CMW. The DHCP and NDP mechanism is used for establishing the IP connection respectively. The PC, which is LAN-connected to the DUT, causes no additional configurations since all devices belong to the same subnet.

#### Configurations at WLAN Signaling on the CMW

For checking the MAC address and setting the IP version:

- Open the configuration dialog via the "Config ..." key.
- Expand the "Connection" node.
- The default "MAC Address (BSSID)" is displayed and suspended.
- Verify that "IP Version Support" is set to the IP version, which is supported by the DUT and the PC of the same subnet.

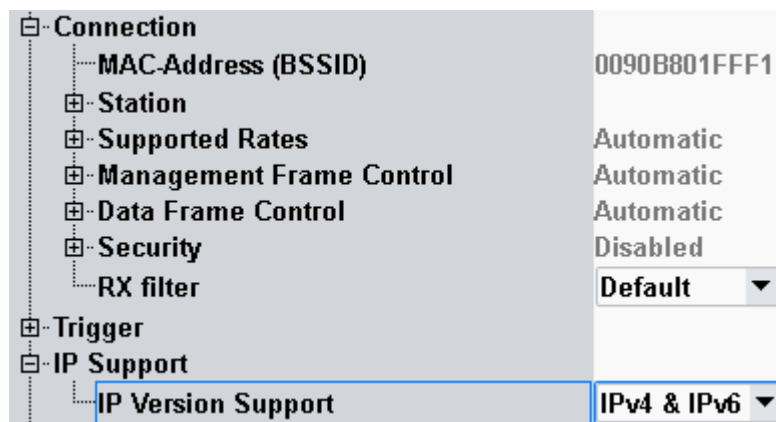


Fig. 7-4: IP version verification at WLAN Signaling for Path A

**Notes:**

- The MAC address is currently fixed to 00-90-B8-01-FF-F1.  
This holds also for the Interface Identifier 02-90-B8-FF-FE-01-FF-F1  
of the IPv6 address after conversion of the MAC address via “Modified EUI-64”.  
The conversion mechanism is described in chapter 2.2.
- When selecting "IP V4 & V6" in "IP Version Support", the channel bandwidth of  
the IP data channel is shared by both IP versions. This has no effect on the net  
data rate of the channel.

**Configurations at the DAU Controller on the CMW**

No IP configuration is required at the DAU Controller on the CMW. IP configuration is relevant for the static IP connections used in Path B and Path C.

**Configurations at the PC at the DUT side**

Check the IP version, which is supported by the PC at the DUT side. No IP configuration is required here, since there is one subnet only: CMW - DUT - PC.

**Configurations at the DUT**

Check the IP version, which is supported by the DUT. No IP configuration is required here, since there is one subnet only: CMW - DUT - PC.

### 7.3 Two Subnets: PC - CMW - DUT - PC over LAN

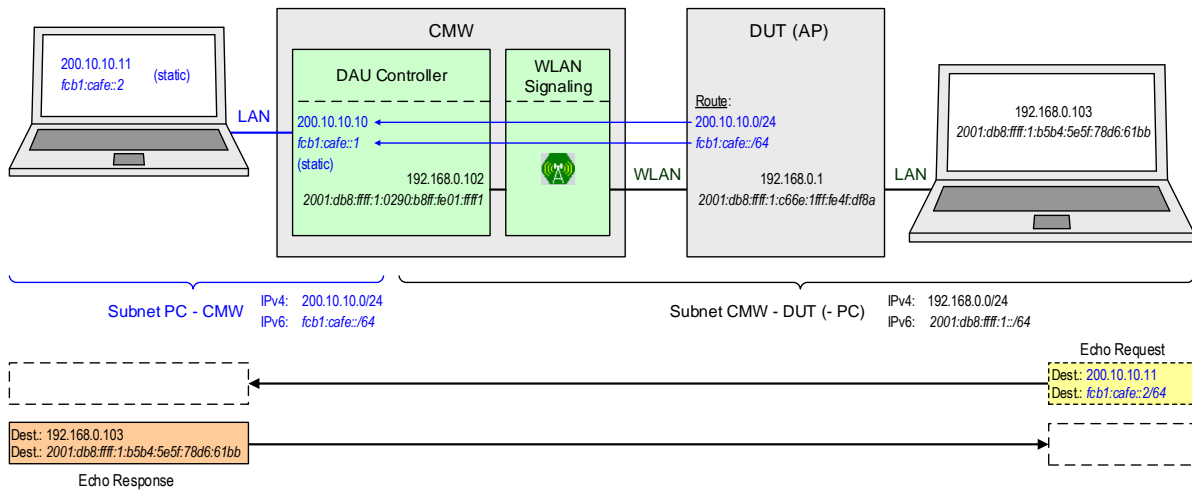


Fig. 7-5: End-to-end test with two subnets, Path B

#### 7.3.1 Test Principle Path B

The characteristics of Path A apply to the CMW - DUT - PC subnet, additional properties:

- A PC is the end of the IP data path at the CMW side. The PC represents an external network. So, the end-to-end path comprises two subnets: Subnet PC - CMW and Subnet CMW - DUT (- PC).
- The DAU of the CMW routes IP data between this PC and the DUT side. It acts as IP gateway separating the CMW-internal IP network from the external IP network. The gateway address at the PC is the DAU's IP address.
- The IP connection between this PC and the DAU relies on a static IP configuration (no use of DHCP and NDP).
- For routing IP data packets from the PC at the DUT side to the PC at the CMW side, the DUT needs routing information (the destination is in an external network). The IP address of Subnet PC - CMW has to be set on the DUT.

#### 7.3.2 Configuring Path B

The IP version, which is supported by the devices of the two subnets, is relevant on the CMW. Static IP configuration (LAN) is required for the PC - CMW subnet.

## Configurations for Subnet CMW - DUT - PC

### At WLAN Signaling on the CMW

For checking the MAC address and setting the IP version, which is supported by the devices of the two subnets, proceed in the same way as described for Path A. No additional configuration is required here.

### On the PC at the DUT side

Check the IP version, which is supported by the PC at the DUT side. No IP configuration is required for the CMW - DUT - PC subnet, since the DHCPv4 and NDP mechanism is used for this purpose respectively.

### At the DUT

Check the IP version, which is supported by the DUT. No IP configuration is required for the CMW - DUT - PC subnet, since the DHCPv4 and NDP mechanism is used for this purpose respectively.

## Configurations for Subnet PC - CMW

### At the DAU Controller on the CMW

For establishing the static IP connection (LAN) of the PC - CMW subnet:

- To open the "Data Application Control" dialog, press "Setup", and in the "Setup" dialog in the "System" section press the "Go to config" button.  
The "Data Application Control" dialog opens.

IPv4 settings at the DAU for the PC - CMW subnet (for IPv6 settings go to 4.):

- Press the "Config" hotkey and select the "IPv4 Address Configuration" tab.
- Select "Static IP Config" for "IPv4 Address Configuration".  
Within the "Static IP Config" section enter the desired "IPv4 Address" of the DAU and the "Subnet Mask" for the PC - CMW subnet (the same subnet mask as at the PC – usually 255.255.255.0 which is the default value). Enter the PC's IP address as the "Gateway IP".

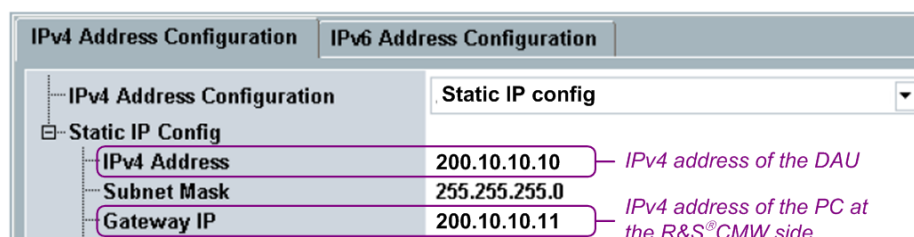


Fig. 7-6: End-to-end configuration at the DAU Controller: IPv4 routing Subnet PC - CMW

Note: The "Gateway IP" parameter is not relevant for Path A, since the IP address of the PC at the CMW side is assigned automatically.

IPv6 settings for the PC - CMW connection (LAN):

4. Press the "Config" hotkey and select the "IPv6 Address Configuration" tab.
5. Within the "LAN IPv6 Address Configuration" section select "Static IP Config" for "Type". Open the "Static Configuration" branch and enter the desired "IPv6 Address" of the DAU.

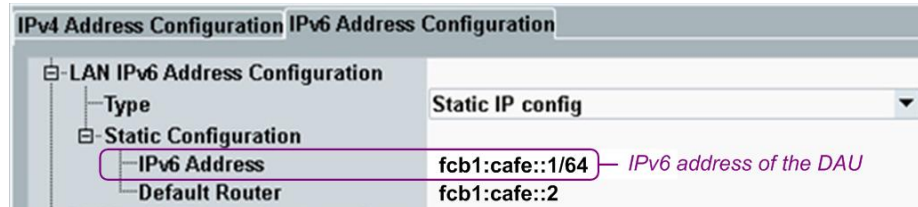


Fig. 7-7: End-to-end configuration at the DAU Controller: IPv6 routing Subnet PC - CMW

### On the PC at the CMW side

As an example for configuration tasks on the PC at the CMW side a step-by-step procedure is given for a Windows workstation.

For establishing the static IP connection (LAN) of the PC - CMW subnet:

1. Connect the PC to the CMW with a LAN cable ("LAN DAU" port).
2. Start with the Windows "Start" button, select the "Control Panel", then "Network and Internet" and "Network and Sharing Center".
3. Click on the "Change adapter settings" link on the left.

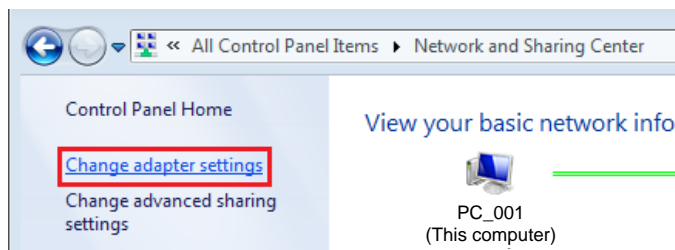


Fig. 7-8: Network and Sharing Center at the PC with MS Windows 7

4. Double-click "Local Area Connection". The "Local Area Connection Properties" window is opened.
5. Depending on the IP Version support of the PC choose one of the following: Click at "Internet Protocol Version 4 (TCP/IPv4)" or "Internet Protocol Version 6 (TCP/IPv6)" to highlight it and then click the "Properties" button.

IPv4 settings (for IPv6 settings go to 9.):

6. Enter the desired "IP address" of the PC and the "Subnet mask" (the same subnet mask as at the DAU Controller – usually 255.255.255.0, which is the default value).
7. For the "Default gateway", enter the DAU's IP address on the PC - CMW subnet.
8. Click "OK".

*IPv6 settings:*

9. Enter the desired “IPv6 address” of the PC.
10. Set the “Subnet prefix length” to “64”.
11. For the “Default gateway”, enter the DAU’s IPv6 address on the PC - CMW subnet.
12. Click “OK”.

### Issues on the PC during remote operation

Note that the PCs may not be remote connected to another network, e.g. a corporate network. Otherwise it cannot be ensured, that the IP data is routed to the desired destination within the IP data path. As an example, this is illustrated for a Windows PC.

*On a Windows PC connected to a corporate (external) network:*

- Routing of the IP test data into the corporate network is possible. This can be avoided with additional testing routes on the PC to ensure that the IP traffic is routed into the test network, i.e. the desired subnet.
- Network bridging on Windows PCs can cause mixing of the test and the corporate network, which in most cases is not desired. Make sure that the IT division in charge of the corporate network is aware of this issue.

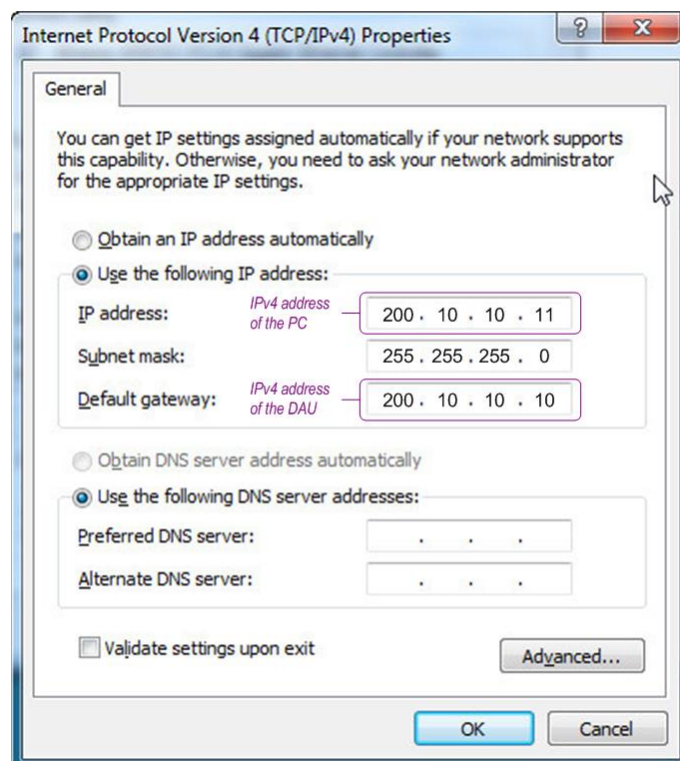


Fig. 7-9: IP settings on a Win 7 PC: IPv4 routing Subnet PC - CMW



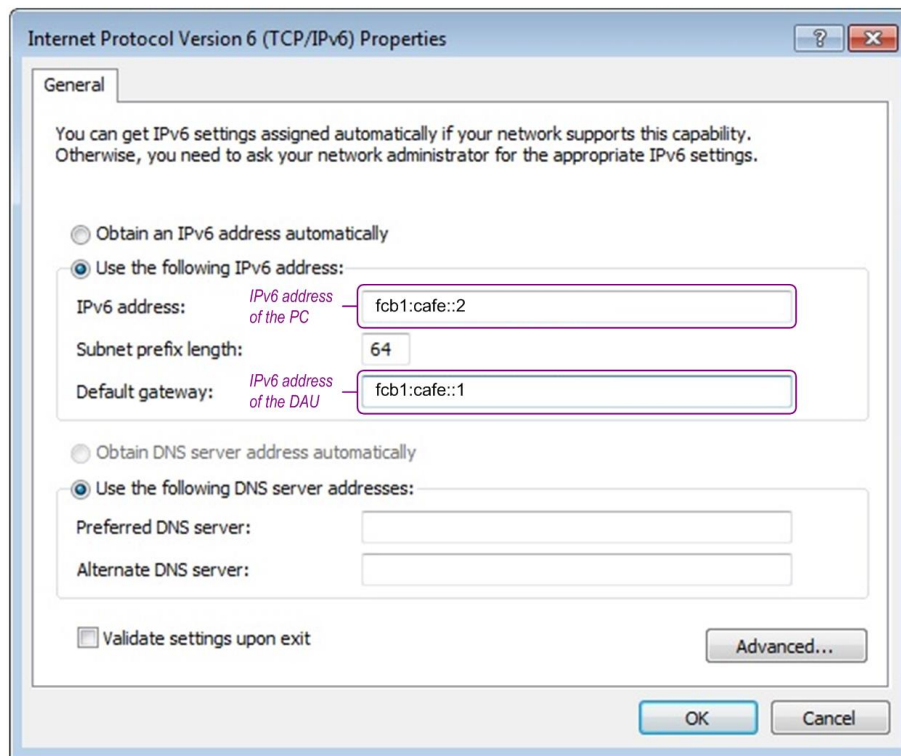


Fig. 7-10: IP settings on a Win 7 PC: IPv6 routing Subnet PC - CMW

## 7.4 Three Subnets: PC - CMW - DUT - PC over WAN

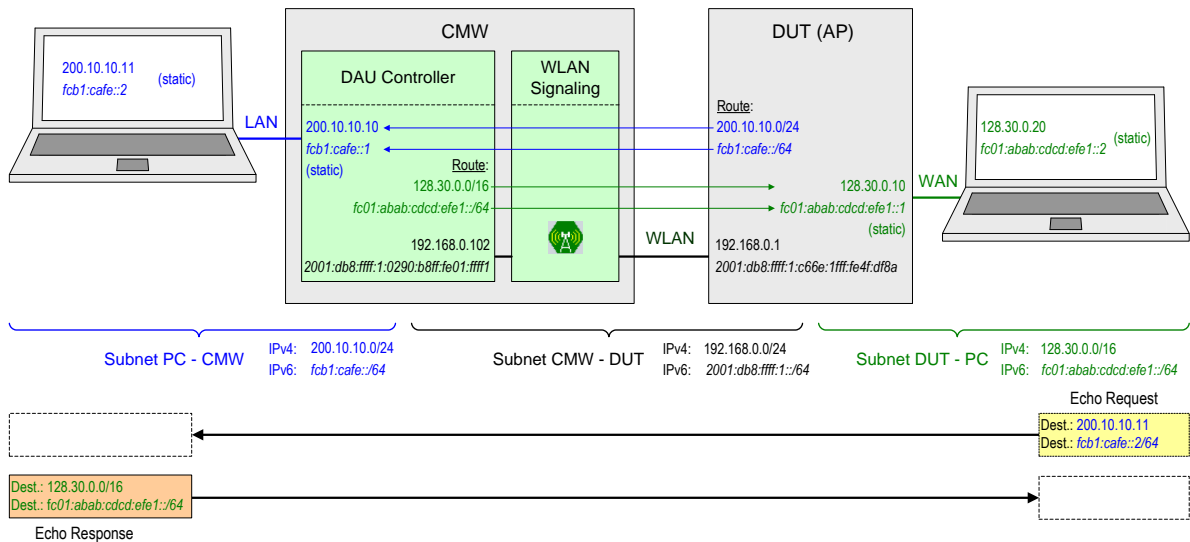


Fig. 7-11: End-to-end test with three subnets, Path C

### 7.4.1 Test Principle Path C

The characteristics of Path A and Path B are still valid, additional properties:

- The PC at the DUT side is WAN-connected to the DUT and represents an external network. So, the end-to-end path comprises three subnets: Subnet PC - CMW, Subnet CMW - DUT and Subnet DUT - PC
- The DUT - PC connection (WAN) has to be configured via IP addresses and subnet masks. The IP configuration is static, DHCP / NDP is not used.
- The DUT acts as gateway for routing IP data packets from the WAN PC to the CMW. So, the gateway address needed at the WAN PC is the DUT's IP address for the DUT - PC subnet.
- The route to the DUT - PC subnet is set at WLAN Signaling and is CMW-internally forwarded to the DAU controller, which is responsible for routing. This required for routing IP data packets from the PC at the CMW side to the PC at the DUT side.
- For routing data in the opposite direction from the PC at the DUT side to the PC at the CMW side, the required route (the address of the PC - CMW subnet) has to be set at the DUT.

### 7.4.2 Configuring Path C

The IP version, which is supported by the devices of the two subnets is still relevant on the CMW. In addition static IP configuration becomes relevant for the external PC - CMW subnet.

## Configurations for Subnet CMW - DUT

### At WLAN Signaling on the CMW

For checking the MAC address and setting the IP version, which is supported by the devices of the three subnets, proceed in the same way as described for Path A.

Note: Additional routing information at WLAN Signaling is required for routing IP data packets from the PC at the CMW side to the PC at the DUT side. Since this applies to WAN IP configuration of the DUT - PC subnet, further configuration steps are given in the configuration section related to this subnet.

### At the DUT

Check the IP version, which is supported by the DUT. No IP configuration is required for the CMW - DUT subnet, since the DHCPv4 and NDP mechanism is used for this purpose respectively.

Notes:

- Additional routing information at the DUT is required for routing IP data packets from the PC at the DUT side to the PC at the CMW side. Since this applies to IP configuration of the LAN-connected PC in the PC - CMW subnet, further steps are given in the configuration section related to this subnet.
- Static WAN IP configuration at the DUT for the DUT - PC subnet is described in the configuration section related to this subnet.

## Configurations for Subnet PC - CMW

### At the DAU Controller on the CMW

*For establishing the static IP connection (LAN) of the PC - CMW subnet:*

A detailed procedure for the static IP configuration is already given in the previous subchapter 7.3.2 for the same subnet of Path B. A short summary is given in the following.

*Relevant parameters at the DAU Controller on the CMW:*

- "IPv4 Address" / "IPv6 Address": This is the IP address of the DAU controller.
- "Subnet Mask": This parameter is for IPv4 support only and is the same at the PC.
- "Gateway IP": This is the IP address of the PC within the subnet.

### On the LAN-connected PC at the CMW side

A detailed procedure for the static IP configuration is already given in the previous subchapter 7.3.2 for the same subnet of Path B. A short summary is given in the following.

*Relevant parameters on the PC:*

- “IP Address”: This is the IPv4 / IPv6 address of the PC.
- “Subnet Mask”: This parameter is for IPv4 only and is the same at the DAU.
- “Default gateway”: This is the IP address of the DAU within the subnet.

#### **At the DUT**

For routing IP data packets from the PC at the DUT side to the PC at the CMW side the DUT needs routing information (the destination is an external network).

*Relevant parameters on the DUT:*

- IP route / destination: This is the IPv4 / IPv6 address of the PC - CMW subnet.
- Subnet Mask: This parameter is for IPv4 only and linked to the PC - CMW subnet.
- Prefix Length: This parameter is for IPv6 only and the default value is 64.
- IP Gateway: This is the IPv4 / IPv6 routing address of the CMW - DUT subnet.

#### **Configurations for Subnet DUT - PC**

The IP connection between the DUT and the WAN-connected PC is static. Therefore the same configuration steps as for the static IP connection (LAN) of the PC - CMW subnet can be applied.

In addition routing configuration at WLAN Signaling of the CMW is described.

#### **At the DUT**

*For establishing the static IP connection (WAN) of the DUT - PC subnet:*

1. Select static IP configuration
2. Enter the IP address of the DUT for the DUT - PC subnet, the subnet mask and the default gateway (= IP address of the PC).

Note: This procedure holds for both IP versions.

#### **On the PC at the DUT side**

*The static IP connection (WAN) is configured accordingly on the PC at the DUT side:*

- ▶ Enter the IP address of the PC for the DUT - PC subnet, the subnet mask and the default gateway (= IP address of the DUT).

Note: This procedure holds for both IP versions.

**At WLAN Signaling on the CMW**

For routing IP data from the PC at the CMW side to the PC at the DUT side:

1. Expand the “Data End To End” node and the “IP Routes List”.
2. Enable “Route Address 1” and enter the IP Route, i.e. the subnet address of the DUT – PC subnet. The procedure is the same for both IP versions.



Fig. 7-12: End-to-end configuration at WLAN Sig.: IP routing Subnet DUT - PC

**Issues on the PC during remote operation**

The routing issues described for Path B are also valid for the PCs in Path C.

## 7.5 Routing Configuration Summary

### IP settings for all paths

Due to the extensive configuration effort required for End-to-End testing, an overview with IP settings is given in the table below. These settings were successfully used for DUT performance testing.

Route	PC (- CMW) via LAN	DAU	DUT	PC (- DUT) via LAN / WAN
<b>Path A</b>				
IPv4 address	Autom. via DHCPv4	Autom. via DHCPv4	Autom. via DHCPv4	-
IPv6 address	Autom. via NDP	Autom. via NDP	Autom. via NDP	-
<b>Path B</b>				
IPv4 address	200.10.10.11	200.10.10.10	192.168.0.1 (LAN autom.) 200.10.10.0 (LAN static)	192.168.0.103 (LAN autom.)
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
IPv6 address	fc1:cafe::2/64	fc1:cafe::1/64	2001:db8:ffff:1::/64 (LAN autom.) fc1:cafe::/64 (LAN static)	2001:db8:ffff:1::2/64 (LAN autom.)
Subnet Prefix Length	64	64	64	64
Default gateway	DAU's IP address	PC (- CMW)'s IP address	PC (- DUT)'s IP address	DUT's IP address
<b>Path C</b>				
IPv4 address	200.10.10.11	200.10.10.10	192.168.0.1 (LAN autom.) 200.10.10.0 (LAN static) 128.30.0.10 (WAN static)	192.168.0.103 (LAN autom.) 128.30.0.20 (WAN static)
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
IPv6 address	fc1:cafe::2/64	fc1:cafe::1/64	2001:db8:ffff:1::/64 (LAN autom.) fc1:cafe::/64 (LAN static) fc01:abab:cdcd:efe1::/64 (WAN static)	2001:db8:ffff:1::2/64 (LAN autom.) fc01:abab:cdcd:efe1::2/64 (WAN static)
Subnet Prefix Length	64	64	64	64
Default gateway	DAU's IP address	PC (- CMW)'s IP address	PC (- DUT)'s IP address	DUT's IP address

Table 7-1: Example configuration for IP connection settings, all paths

## 7.6 Final Steps

### IP connection verification

*On the CMW, at the WLAN Signaling application (all paths):*

1. Switch on the WLAN Signaling application.  
The WLAN connection between CMW and DUT is established. The DAU receives its IP configuration from the DUT.

*On the CMW, at the DAU application (all paths):*

2. For verifying that the IP connection between CMW and DUT is working ("Ping" measurement):
  - a) Find out the IP address of the DUT (on the CMW - DUT subnet).
  - b) Press the MEASURE key to open the "Data Application Measurements" dialog.
  - c) Enable "Data Appl. > Measurements" and press "Data Meas" on the task bar at the bottom.
  - d) At the top of the "Data Application Measurements" dialog select the WLAN Signaling application at "Select RAN".
  - e) Activate the Ping measurement (via the "Measurement Controller" dialog, entry "Data Appl. > Measurements") and access the "Ping" measurement tab (via Task bar).
  - f) For "Destination IP" enter the IP address of the DUT.
  - g) Start pinging the DUT.
  - h) Verify that the DUT replies the Ping requests. Then stop pinging.

### Starting IP data transmission

*At a connected PC:*

3. Start IP data transmission to the desired target (IP address!) according to your needs.

## 8 Message Log Analysis with CMWmars

CMWmars is a comprehensive message analysis tool for all CMW signaling applications. It provides access to all information elements of all protocol layers of the most important mobile radio standards, including WLAN and the IP layer.

The tool executes both online message analysis during e.g. a protocol test and offline message analysis of message log files. The message log contains detailed peer-to-peer and inter-layer message information. For offline log file analysis the license-free CMWmars Viewer and the MCT-Message Recorder software tools are sufficient.

WLAN message log analysis		
Designation/Solution	License	Key Features
MCT-Message Recorder and CMWmarsViewer	License-free	Online message recording Offline analysis of message logs
CMWmars Basic	R&S CMW-KT021	Off- and online analysis of message logs Basic protocol analysis
CMWmars Advanced	R&S CMW-KT021 and R&S CMW-KT023	Off- and online analysis of message logs Advanced protocol analysis

Table 8-1: WLAN message log analysis solutions

The following sections provide procedures at the MCT Message Recorder (log recording) and CMWmars (log analysis). The steps for offline message log analysis are identical at CMWmars and at the CMWmars Viewer. Both applications are referred to as CMWmars in the following. Note that online and advanced analysis are not covered by the CMWmars Viewer. For detailed information about features of the message analysis tools, see the CMWmars user manual [8].

### 8.1 Getting Started

#### Installation and Setup

1. Download CMWmars and the MCT-Message recorder from the R&S GLORIS customer web portal [3] and install the software on a customer PC as described in the appendix to this document. The PC is used for logging.
2. Connect the PC and the CMW with an Ethernet cable using the LAN switch on the rear panel of the CMW. The test setup is described in chapter 3 (Fig. 3-5). It is recommended to use a direct connection between logging PC and CMW.

#### At the WLAN Signaling application

3. In section "Message Monitoring" of the WLAN signaling configuration dialog:
  - a) Activate "Add WLAN Signaling to logging".
  - b) In the "Logging PC IPv4 Address" list, select an IP addr. for the logging PC.

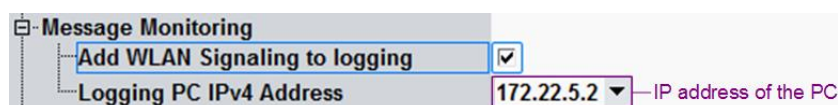


Fig. 8-1: Network configuration at WLAN Signaling



At the logging PC

4. Configure the same IP address at the network adapter of the logging PC, e.g. 172.22.5.2.

Notes on IP settings at the CMW Base and the WLAN Signaling application:

- If you want to use a different network ID for the PC-CMW subnet:
  - a) Open the CMW "Setup" configuration dialog.
  - b) In the section "Misc" select "IP Subnet Config" to open the "IP Subnet Configuration" dialog.
  - c) In the "Subnet Node" select the "Network Segment" node.
  - d) In the "Network Segment" list, select the network ID that you need and press "Apply".  
The Firmware will restart in case you change the network ID, the "Subnet Mask" stays fixed to 255.255.0.0.

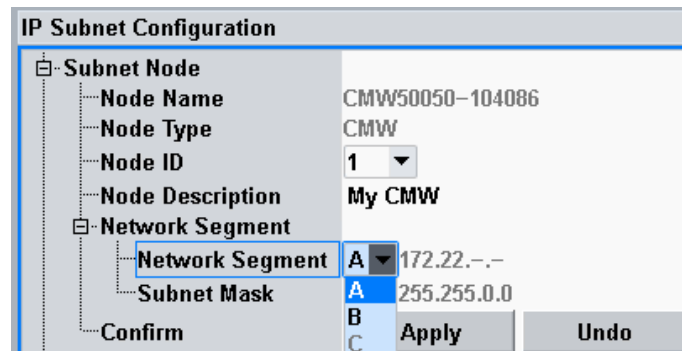


Fig. 8-2: Network ID settings in IP subnet configuration

- If you're using a CMW without Data Application Unit (DAU):
  - a) Select the "IPv4 Interface" section in the WLAN Signaling configuration dialog.
  - b) Configure the IP address settings and "Subnet Mask" as you need them. The "Default Gateway" address is the IP address of the PC.
  - c) Switch off the DHCP server.

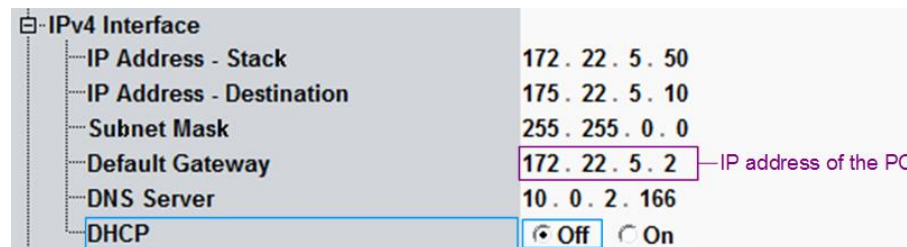


Fig. 8-3: IP settings at WLAN Signaling for a CMW without DAU

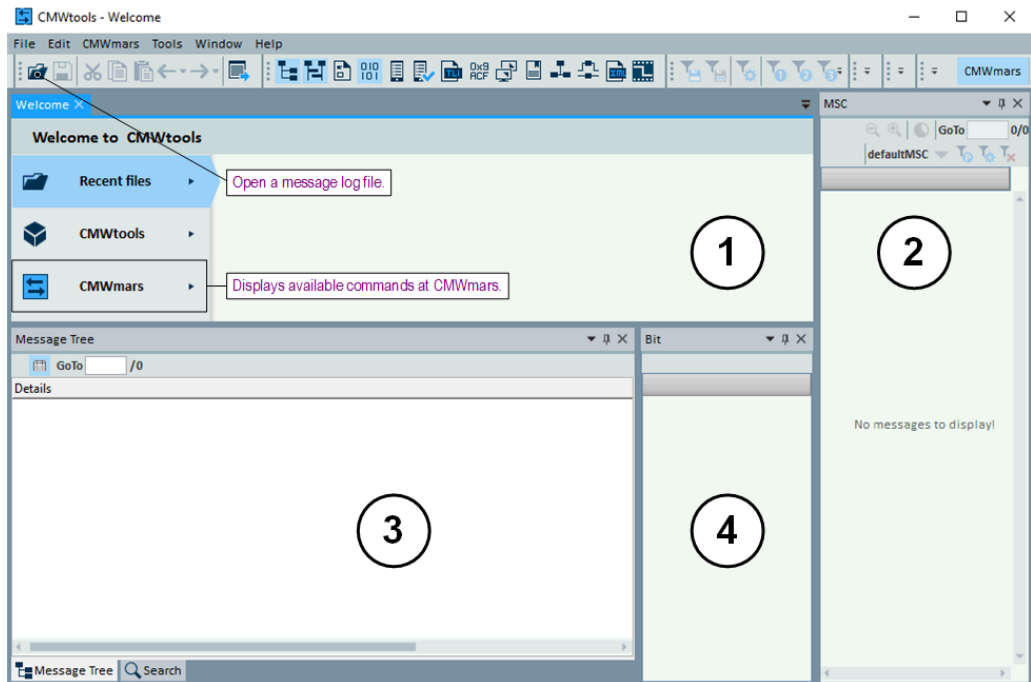
Starting CMWmars

5. Click "Start > All Programs > R&S Protocol Test Tools > CMWmars" on the Windows desktop menu.

The CMWtools starts. The "Welcome" view shows all installed applications (Fig. 8-4).

Note: After loading a message log file, the "Table" view tab is added left to the "Welcome" view tab. The "Table" view shows detailed log information (see Fig. 8-7).

6. Click "CMWmars" on the left to show available commands on the right.



**Fig. 8-4: CMWtools "Welcome" window with CMWmars default view**

- 1 = "Welcome" view: shows all installed applications
- 2 = "MSC" view: visualizes the message flow between the network (CMW), protocols and the DUT
- 3 = "Message Tree" view: shows message details in a tree-like representation
- 4 = "Bit" view: shows the message details on bit level

Recording and loading a message log (offline analysis) or monitoring the exchange of messages between the CMW and the DUT (online analysis) is described in the following chapters.

## 8.2 Recording Message Logs

This chapter describes how WLAN message logs can be recorded and saved in a file with the MCT Message Recorder.

### Starting Situation

- The logging PC is LAN connected to the CMW as described in chapter 8.1.
- The MCT Message Recorder is installed on the logging PC. The installation of the MCT Message Recorder is described in the appendix to this document.

**Procedures**

*At the logging PC*

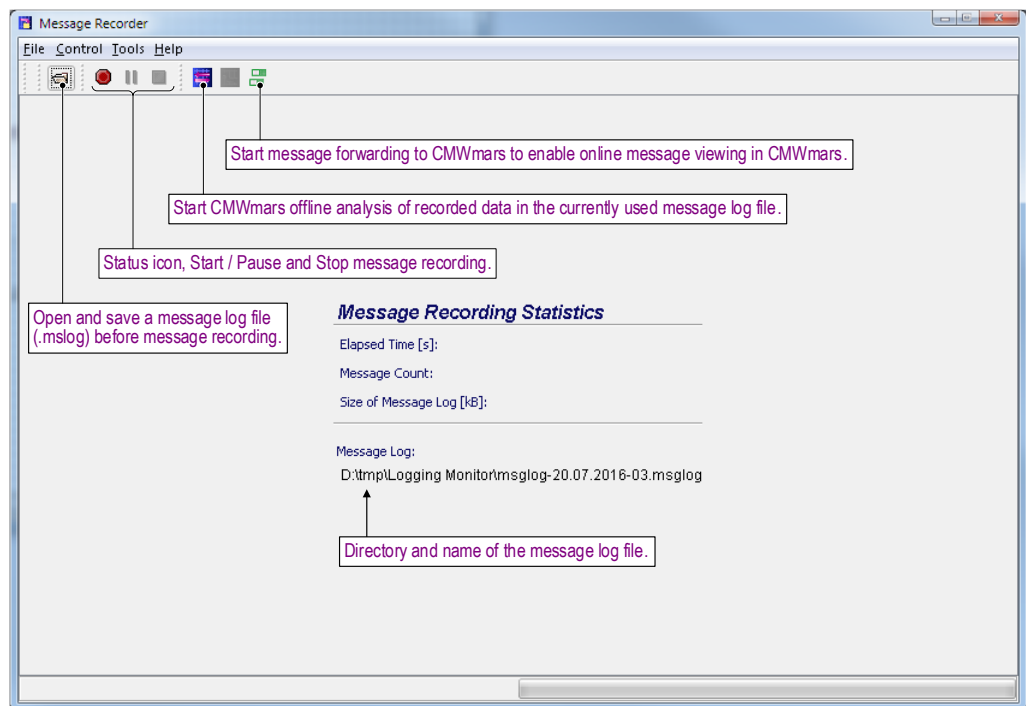
1. Click "Start > All Programs > R&S MCT Message Recorder > MCT Message Recorder " on the Windows desktop menu.  
The MCT Message Recorder starts.
2. Open an empty log file, where the message log information is stored in.  
The MCT Message Recorder as well as the Legacy Message Analyzer (option R&S®CMW-KT011) use the same log file extension .msglog.
3. In the toolbar, press the recording icon to start message recording.

*At the WLAN Signaling application*

4. Switch on WLAN Signaling.

*At the MCT Message Recorder*

5. Verify that the MCT Message Recorder is connected to the WLAN Signaling application.  
In this case, the "Message Count" is higher than 0 in the "Message Recording Statistics" result summary (Fig. 8-5).
6. In the toolbar, press the stop icon to stop message recording.  
The current message log file is automatically saved. The size, name and directory of the log file are displayed in the "Message Recording Statistics" result summary.



**Fig. 8-5: MCT Message Recorder GUI and basic functions**

### 8.3 Analyzing Message Logs

When using analyzing WLAN message logs for the first time it is useful to load predefined settings to filter only relevant log information of the used RAT. CMWmars provides predefined column sets in the "Table View" (Fig. 8-7), particularly a column set for WLAN message log analysis. As soon as a column set is loaded its column configuration is kept. The following procedures are only needed once.

#### Loading a WLAN column set

1. On the "Welcome" or "Table" view toolbar, click the "Column Set" button.
2. Click the "Browse" button. A dialog box opens.
3. Browse for a column configuration file .rscol, and then click "Open".  
CMWmars provides WLAN\_1, WLAN\_LTE and WLAN\_Overview column sets by default. You can use the WLAN\_Overview column set for basic log analysis.

Note: The predefined column sets are realized as formulas. You are prompted to import them.

4. Click "Ok" to import the WLAN column set.

Result: The column configuration is applied to the "Table" view and saved for all future log analysis purposes.

You can further customize and save the column configuration as you need it. See the CMWmars user manual for more information [8].

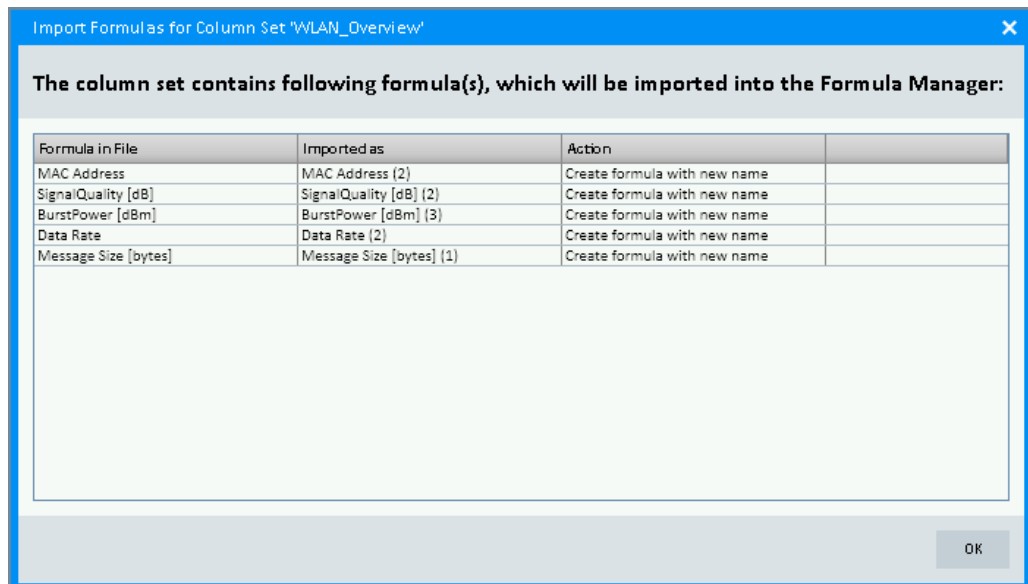


Fig. 8-6: Loading a WLAN column set

#### Loading a Message Log offline (license-free)

1. Select "File > Open" from the CMWmars menu.
2. Browse to the <test\_results> folder where the message logs from the MCT Message Recorder are stored by default. The <test\_results> path depends on the

type of instrument and operating system, e.g.:

C:\Users\Public\Documents\Rohde-Schwarz\TestResults\MCT\_Message\_Recorder\_Log\_Files\802.11ac\_VHT\_40MHz.rmsglog

3. Select a message log file with extension .rmsglog or .msglog and click "Open".

CMWmars proprietary message log files have the extension .rmsglog. Legacy Message Analyzer (option R&S®CMW-KT011) and MCT Message Recorder message logs have the extension .msglog. CMWmars automatically converts these log files to .rmsglog files, when they are loaded into CMWmars.

Result: The file is loaded and the CMWmars views are populated.

The default views are "Table", "MSC", "Message Tree", and "Bit". In the following, WLAN message log analysis is given referring mainly to the "Table" view. For a detailed description of the other views, see the CMWmars user manual.

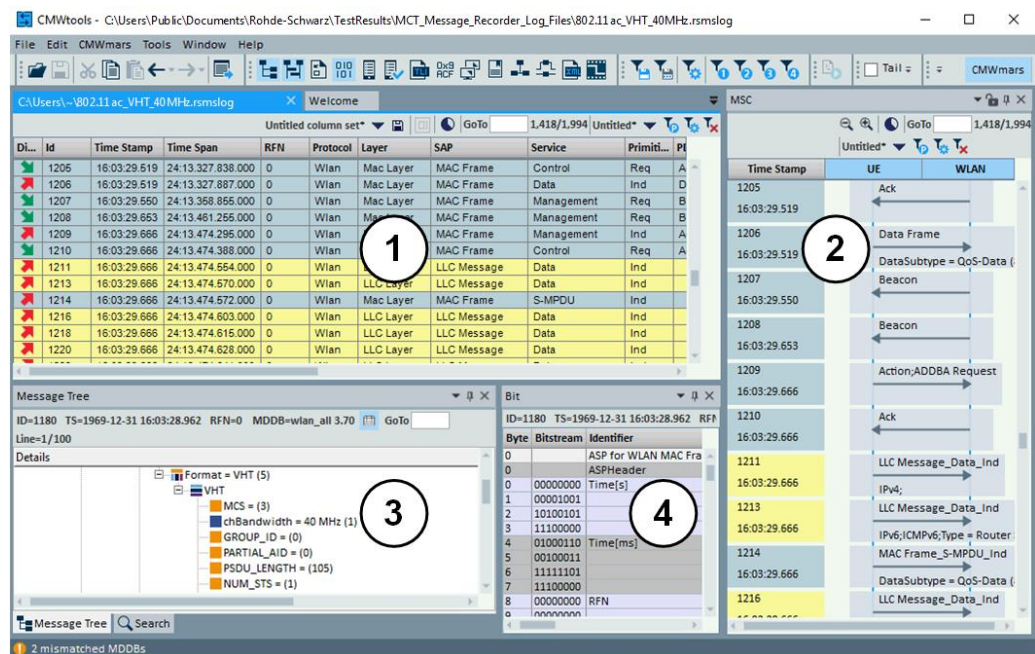


Fig. 8-7: CMWmars GUI default view (offline mode)

- 1 = "Table" view: shows the message log in a table representation
- 2 = "MSC" view: visualizes the message flow between the network (CMW), protocols and the DUT
- 3 = "Message Tree" view: shows message details in a tree-like representation
- 4 = "Bit" view: shows the message details on bit level

### Applying a filter

Applying a filter to the "Table" view reduces the amount of displayed messages and thus the amount of messages you have to cope with. Filtering is performed by using filter commands on the shortcut menu.

1. Right-click a message value to open the shortcut menu. It depends on the selected row and column which filter commands are shown, for example: "Hide all service: <selection>" and "Show only service: <selection>" where <selection> is the protocol or part of the protocol or the selected value.
2. Select the filter you want to apply, e.g. Hide all service:[UPLANE].[UPC].



Result: The filter is applied to the "Table" view. Fig. 8-8: shows a message log before and after filtering. In the "Table" view, messages from the UPC layer were filtered out from a WLAN 802.11ac VHT 40 MHz signal.

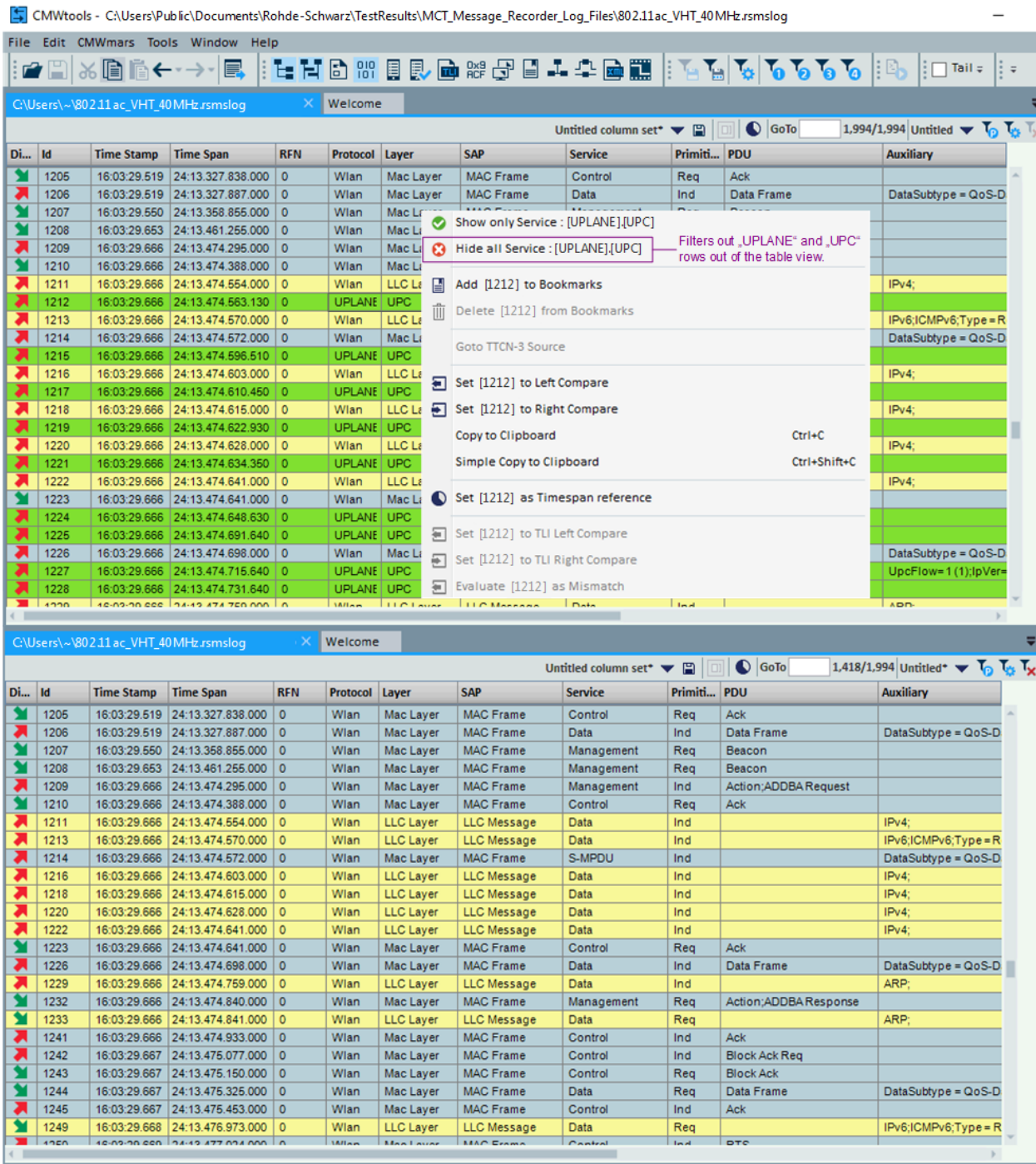


Fig. 8-8: WLAN 802.11ac message log before and after applying a WLAN filter

The "Table" view displays the logged messages across all protocol entities and layers in a listed sequence. The messages are sorted by the message "ID" which is derived from the time stamp. The view provides several functions allowing you to display and

find the desired message logs, for example, navigating to specific messages, specifying filters and bookmarks, searching for messages or configuring columns.

You can further specify a filter in the Filter Configuration dialog box.

3. Click the "Edit filter" icon on the "Table" view toolbar.  
The "Filter Configuration" dialog box opens.
4. Specify a filter.  
For example, select the "PDU only" check box.
5. Click "OK" to take the settings effect.

Result: The filter is applied to the "Table" view.

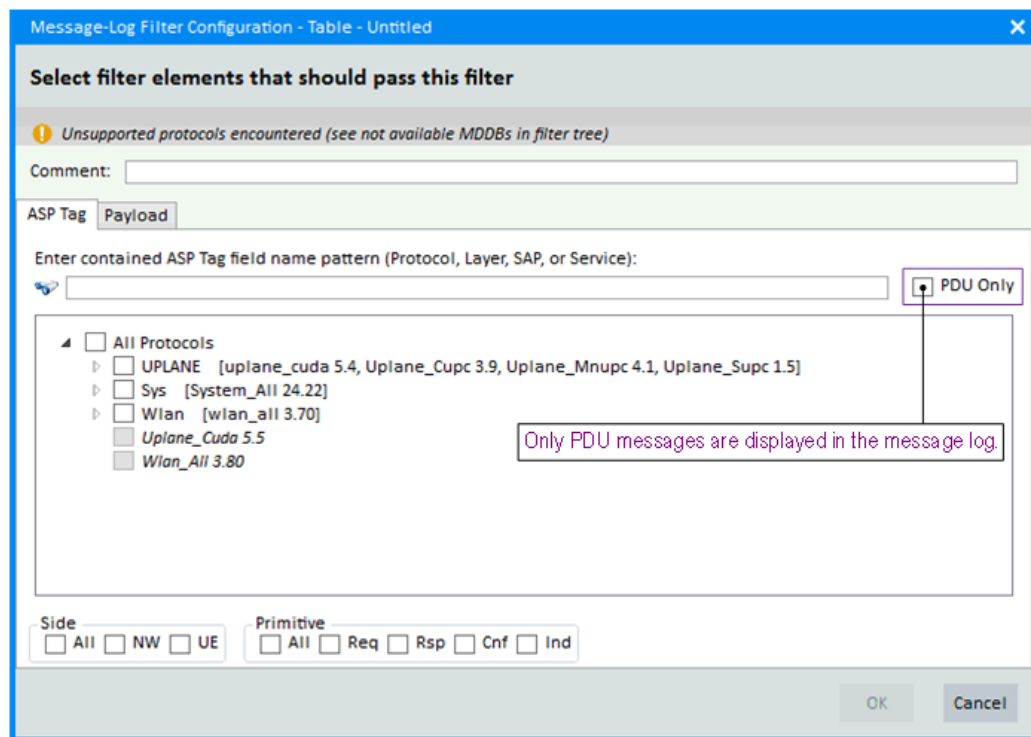


Fig. 8-9: Filter configuration dialog

### Viewing messages online (R&S@CMW-KT021 option required)

At CMWmars

1. Configure the online connection (Fig. 8-10):
  - Type in the hostname in the text box of the CMWmars online toolbar.
  - Use "localhost" (default setting), if the MCT Message Recorder run on the same host as CMWmars, which is the recommended setup.
2. Activate online message viewing:  
On the CMWtools toolbar, click the "Start Online Message Viewing" button. Note the status indication on the "CMWmars online" bar. To receive messages, the status must be yellow. All views are cleared. The "Table" view is in online mode and shows "Host: <connection>".

Result: CMWmars is prepared for receiving messages online. The "Table" view and all other open views are populated as soon as the Message Recorder starts message recording (see step 3). The online viewing status in CMWmars switches to green. See the CMWmars user manual for an online viewing example [8].



**Fig. 8-10: CMWmars online toolbar**

- 1 = "Tail". If selected, the views are scrolling and always showing the latest message
- 2 = Text box for specifying the hostname
- 3 = Start and stop online message viewing buttons
- 4 = Status symbol (gray, red, yellow, green)

*At the MCT Message Recorder*

3. Start message recording as described in chapter 8.2.

Result: The recorded messages are automatically forwarded to CMWmars. The CMWmars views are further populated as long as messages are recorded.

Note: WLAN Signaling can temporarily be switched off without loss of already recorded messages. When WLAN signaling is switched on again, the new messages are added to the existing log.

*At CMWmars*

4. To stop online message viewing click the "Stop Online Message Viewing" button on the CMWtools toolbar.

Result: The online mode is closed.

## 8.4 Advanced Analysis

You can use the CMWmars Message Analyzer Advanced features in CMWmars online and offline mode when analyzing WLAN message logs or protocol tests during runtime.

### IP throughput measurement

An additional feature for WLAN signaling tests is the monitoring the IP throughput of WLAN up- and downlink directions with the Protocol Measurement Charts view available with CMWmars Advanced option.

This view graphically visualizes IP throughput of WLAN up- and downlink directions. You can use IP throughput curves to troubleshoot problems during handover procedures or traffic offloading from LTE to WLAN.

Since IP throughput measurements are described in detail in chapter 5 and 6 of this application note, this feature is not further illustrated. Detailed information about adjusting the CMWmars Message Analyzer Advanced views for optimized data representation is given in the CMWmars user manual [8].



## 9 Literature

- [1] **IEEE** 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications [Online]. - 1997-2017. - <https://www.ieee802.org/11/>.
- [2] **Rohde & Schwarz** CMW Support of WLAN 802.11ac [Online] // Application Note. - 2013. - <https://www.rohde-schwarz.com/appnote/1CM101>.
- [3] **Rohde & Schwarz** GLORIS Customer Web Portal [Online]. - <https://gloris.rohde-schwarz.com/>.
- [4] **Rohde & Schwarz** IEEE 802.11ax Technology Introduction [Online] // White Paper. - 2016. - <https://www.rohde-schwarz.com/appnote/1MA222>.
- [5] **Rohde & Schwarz** R&S@CMW-B450A/B/D Data Application Unit // User Manual. - 2017.
- [6] **Rohde & Schwarz** R&S@CMW-KM5xx/-KS5xx LTE UE Firmware Applications // User Manual. - 2017.
- [7] **Rohde & Schwarz** R&S@CMW-KM65x R&S@CMW-KS65x/-KS660/-KS670 WLAN Firmware Applications // User Manual. - 2017.
- [8] **Rohde & Schwarz** R&S@CMW-KT02x CMWmars Message Analyzer // User Manual. - 2017.
- [9] **Rohde & Schwarz** WLAN Connection Establishment [Online] // Application Note. - 2015. - <https://www.rohde-schwarz.com/appnote/1C106>.

## 10 Ordering Information

CMW Hardware		
Designation	Type	Order No.
Radio Communication Tester	R&S®CMW500	1201.0002K50
	R&S®CMW290	1201.0002K29
	R&S®CMW270	1201.0002K75
Basic Assembly	CMW-PS503 (CMW500)	1202.5408.02
	CMW-PS290 (CMW290)	1208.9270.06
	CMW-PS272 (CMW270)	1202.9303.02
Baseband Measurement Unit	CMW-B100A	1202.8607.02
Baseband Measurement Generator	CMW-B110A	1202.5508.02
Baseband Generator, 4 GB ARB memory	CMW-B110D	1202.5508.05
Baseband Interconnection Board	CMW-S550B	1202.4801.03
Advanced RF Frontend Module or RF Frontend Module Extra RF Frontend Module	CMW-S590D CMW-S590A CMW-B590A	1202.8707.03 1202.5108.02
RF Converter Module Extra RF Converter Module	CMW-S570B CMW-B570B	1202.8659.03
Signaling Unit Advanced (SUA)	CMW-B500I	1208.7954.10
Signaling Unit Universal (SUU)	CMW-B200A	1202.6104.02
WiMAX/WLAN Signaling Module for SUU	CMW-B270A	1202.6504.02

CMW Software		
Designation	Type	Order No.
<b>CMW Base Firmware (Version 3.5.60 or later)</b>		
R&S®CMW500 Base Firmware R&S®CMW290 Base Firmware R&S®CMW270 Base Firmware	Without license	
<b>WLAN Signaling (Version 3.5.40 or later)</b>		
WLAN IEEE 802.11a/b/g basic signaling	CMW-KS650	1207.5858.02
WLAN IEEE 802.11n basic signaling	CMW-KS651	1207.5706.02
WLAN advanced signaling	CMW-KS660	1207.5906.02
<b>WLAN Measurement (Version 3.5.40 or later)</b>		
WLAN IEEE 802.11a/b/g TX measurement	CMW-KM650	1203.1658.02
WLAN IEEE 802.11n SISO, TX measurement	CMW-KM651	1203.9159.02
<b>Additional WLAN Features</b>		
WLAN Measurements from 3.3 GHz - 6 GHz	CMW-KB036	1203.0851.02
<b>CMWmars</b>		
CMWmars Log Viewer	Without license	
CMWmars Message Analyzer Basic	CMW-KT021	1202.8757.xx
CMWmars Message Analyzer Advanced	CMW-KT023	1208.7531.xx
MCT-Message Recorder	Without license	
<b>Data Application Unit (Version 3.5.40 or later)</b>		
Data Application:Unit 1: H450A	CMW-B450A	1202.8759.02
H450B	CMW-B450B	1202.8759.03
H450D	CMW-B450D	1202.8759.05
Data Application:Unit 2: H450H	CMW-B450H	1202.8759.09
IP-data interface for IPv4	CMW-KA100	1207.2607.02
Ext. of IP-data interface for IPv6 and IP multicast	CMW-KA150	1207.2659.02
IP based measurements	CMW-KM050	1203.9359.02
Test software for WLAN Offloading	CMW-KA065	1208.8021.02
IMS basic service, for establishing a voice or video call over LTE	CMW-KAA20	1207.8657.02

The LTE options required for WLAN offloading are listed in the LTE user manual.

# Appendix

## A Installing CMWmars

All variants of CMWmars as well as the Message Description Database (MDDDB) can be downloaded and installed via the GLORIS Rohde & Schwarz customer web portal.

If missing MDDBs are indicated in the CMWmars status line, it is recommended that you install them on your system to correctly decode the messages contained in the log.

### Procedures

At the GLORIS customer web portal:

1. Register on the GLORIS web portal [3] or login, if you are already registered.
2. Select the "Support&Services" tab
3. In the menu on the left, open the section "My Products" and select "CMW Customer Web".
4. Select "R&S@CMW SW Tools".  
The R&S@CMW SW Tools selection window opens.
5. Select the "R&S@CMWmars" software tool.
6. Below the search field, select the button "Firm-/Software" to filter your search results for firm- and software products.

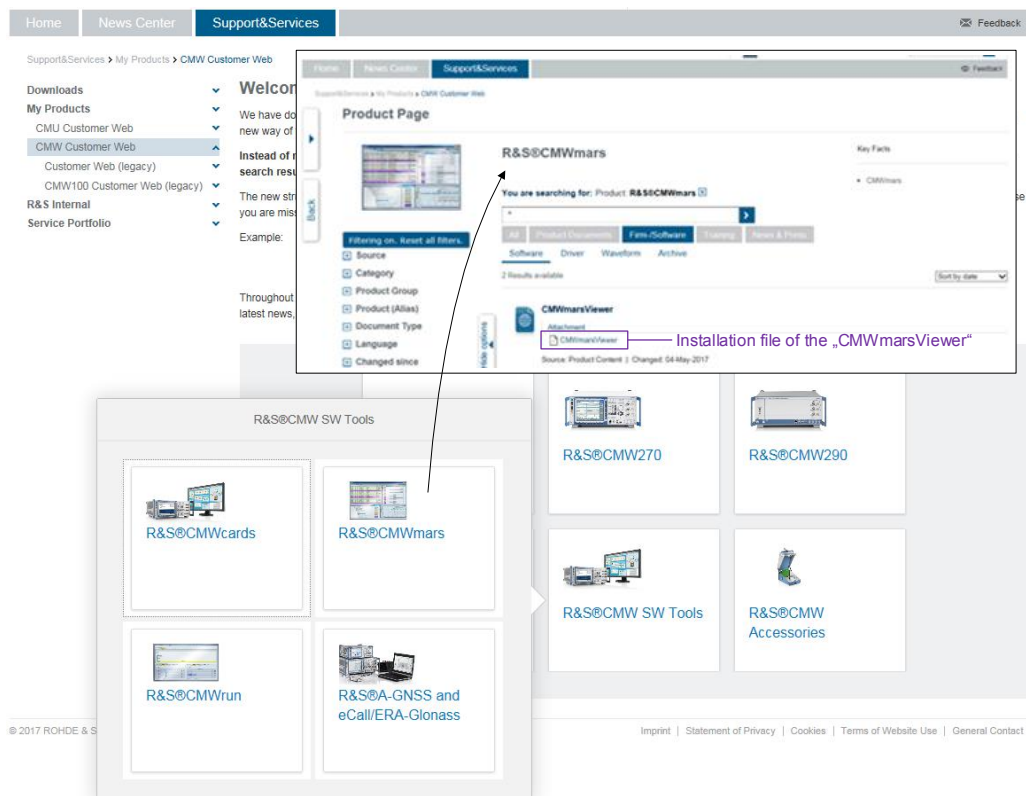
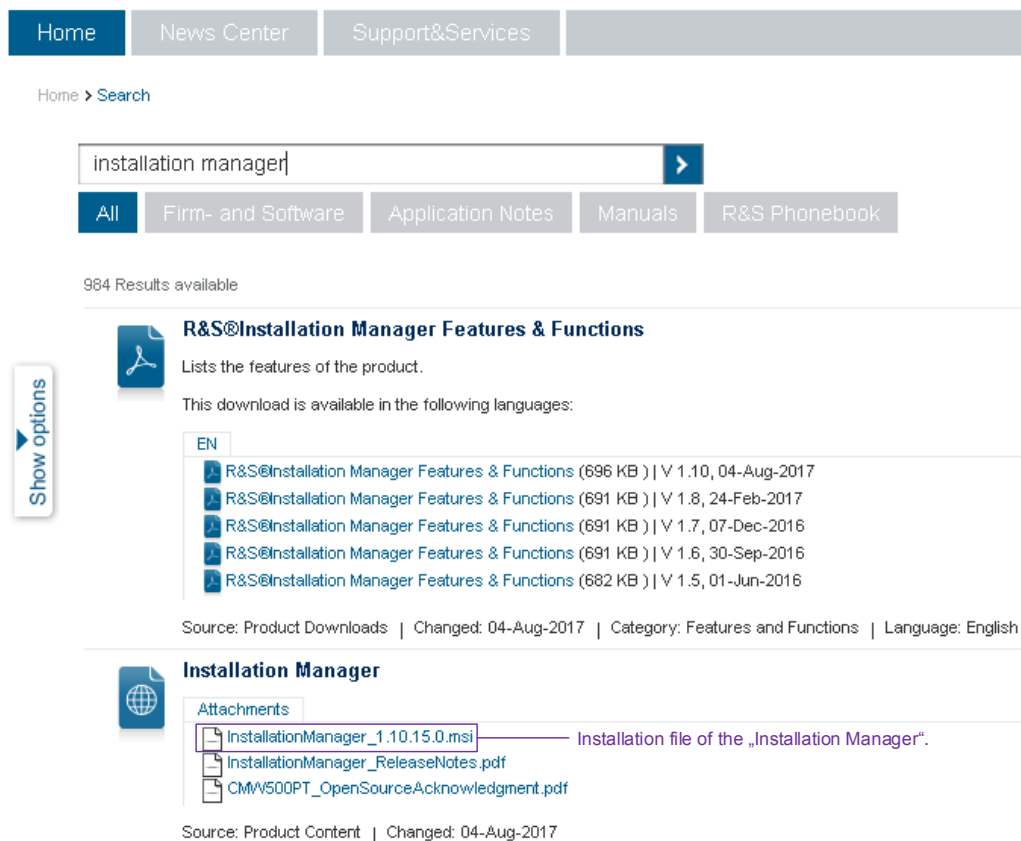


Fig. 10-1: CMWmars software on the GLORIS customer web portal

7. Search for "CMWmars", i.e. enter "CMWmars" in the search field. CMWmars related products should be listed as search results from the "CMW Customer Web".
8. Download and install the license-free "CMWmarsViewer".  
Note: Only licensed firm- and software is available via the Installation Manager.
9. Download, install and open the "Installation Manager" (Fig. 10-2):
  - a) Open the "Home" tab.
  - b) Search for "Installation Manager" in the search field.
  - c) Do not filter the search results, i.e. apply the "All" search filter.

The second search result is relevant for installation. Its first attachment is the installation file of the Installation Manager.



**Fig. 10-2: Installation Manager software on the GLORIS customer web portal**

- d) Open the installation file and follow the instructions.
- e) Click "Start > All Programs > R&S Installation Manager > Installation Manager" on the Windows desktop menu to open the application.

At the Installation Manager:

During the download procedures your GLORIS user name and password are needed.

10. Download CMWmars (Fig. 10-3):

- a) Search for "CMWmars" in the "Products" tab.
- b) In the search results table, add the version of the CMWmars variant you need to your download list by pressing the download icon in the "Action" column.

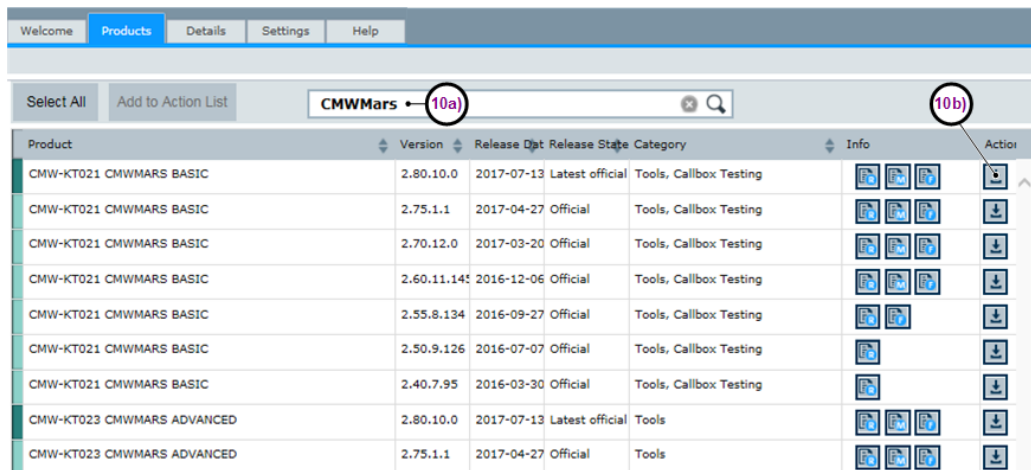


Fig. 10-3: CMWmars variants at the Installation Manager

11. Download the MCT-Message Recorder (Fig. 10-4):

- a) Navigate to the "Details" tab and search for "Recorder". The MCT-Message Recorder shall be listed in the search results.
- b) Add the MCT-Message Recorder to your download list by pressing the download button in the "Action" column.

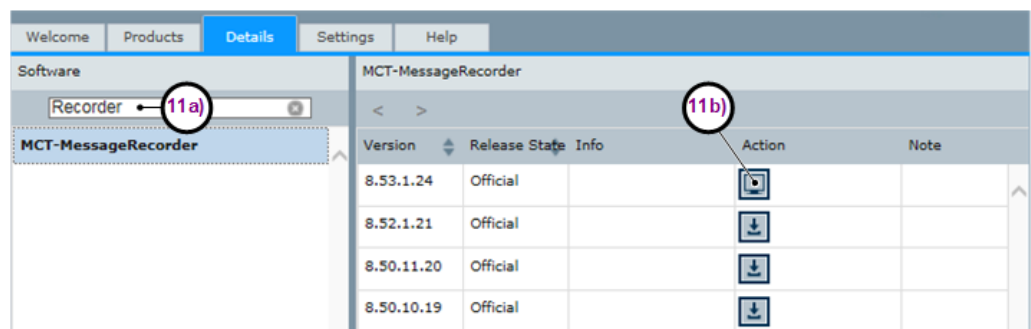


Fig. 10-4: MCT Message Recorder download at the Installation Manager

12. Download CMW-MDDB WLAN (Fig. 10-5):

- a) Navigate to the "Details" tab, search for "CMW MDDB" and select "CMW-MDDB WLAN ALL" in the search results.
- b) Add the MCT-Message Recorder to your download list by pressing the download button in the "Action" column.

13. Start downloading and installing all products (Fig. 10-5):  
 Select the products of interest in the "Action List" panel and press the "Execute" button.

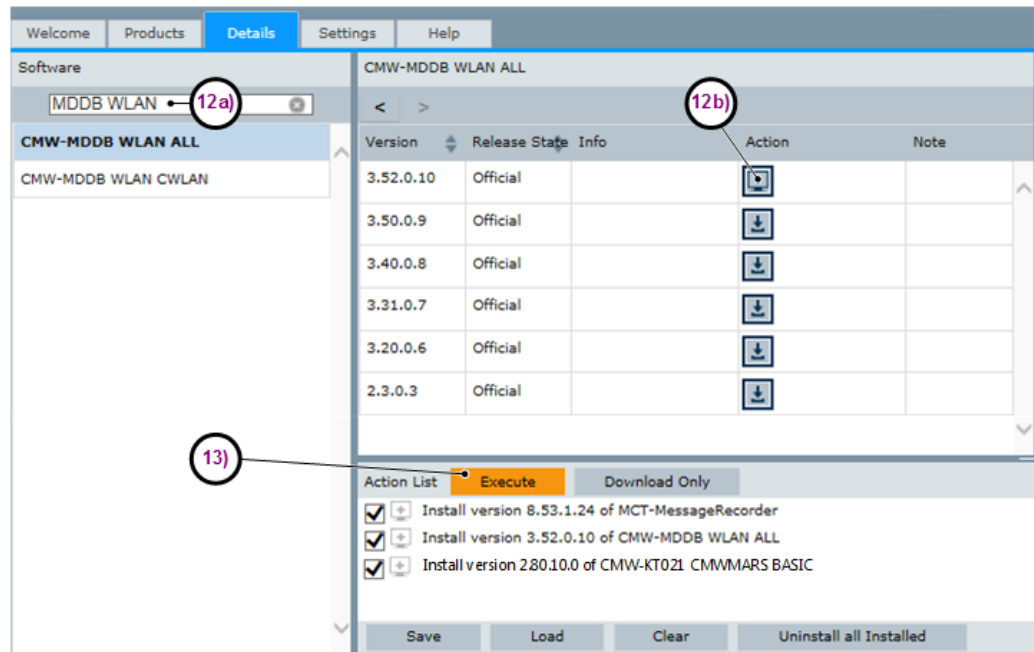


Fig. 10-5: CMW-MDDB WLAN download and installation at the Installation Manager

Successful installation is indicated with a monitor checkbox icon in the "Info" column left to the "Action" column (Fig. 10-6).

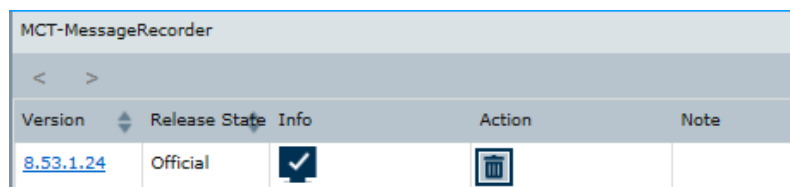


Fig. 10-6: Info icon indicating that the MCT Message Recorder is installed

## Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, radiomonitoring and radiolocation. Founded more than 80 years ago, this independent company has an extensive sales and service network and is present in more than 70 countries.

The electronics group is among the world market leaders in its established business fields. The company is headquartered in Munich, Germany. It also has regional headquarters in Singapore and Columbia, Maryland, USA, to manage its operations in these regions.

## Regional contact

Europe, Africa, Middle East  
+49 89 4129 12345  
[customersupport@rohde-schwarz.com](mailto:customersupport@rohde-schwarz.com)

North America  
1 888 TEST RSA (1 888 837 87 72)  
[customer.support@rsa.rohde-schwarz.com](mailto:customer.support@rsa.rohde-schwarz.com)

Latin America  
+1 410 910 79 88  
[customersupport.la@rohde-schwarz.com](mailto:customersupport.la@rohde-schwarz.com)

Asia Pacific  
+65 65 13 04 88  
[customersupport.asia@rohde-schwarz.com](mailto:customersupport.asia@rohde-schwarz.com)

China  
+86 800 810 82 28 | +86 400 650 58 96  
[customersupport.china@rohde-schwarz.com](mailto:customersupport.china@rohde-schwarz.com)

## Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership



This application note and the supplied programs may only be used subject to the conditions of use set forth in the download area of the Rohde & Schwarz website.

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG; Trade names are trademarks of the owners.