Customer
DOCSIS 3.1 CPE Acceptance Test Plan
Operational SW Readiness

Project Reference	: Excentis Customer DOCSIS 3.1 CPE ATP SW - xxxyyy
Author(s)	: Excentis
Contact	: yyyy
Date	: xxxxx, xxxxx
Revision	: V05
Distribution	: Excentis – Customer

Excentis

Gildestraat 8, B-9000 Ghent, Belgium
Phone +32 9 269 22 91
Fax +32 9 329 31 74
https://www.excentis.com

Table of Contents

1 Executive Summary

Mr. xyz in name of Customer has asked Excentis to write an Acceptance Test Plan for validation of a DOCSIS 3.1 Cable Modem with E-MTA, eRouter and Wi-Fi. This to assure the DOCSIS 3.1 CPE roll-out. In the past Excentis has already written a validation test plan for the EuroDOCSIS 3.0 CPE, which served as a limited basis for equivalent tests in this test plan.

Testing offers a certain level of insurance on how the products behave and can relate to customer impact. This is not a full guarantee as the amount of cases and scenarios is immensely. Current tests are targeted to address the most critical operational issues.

Compared to the previous EuroDOCSIS 3.0 modem test plan the choice was made to:

- Split up the test plan for three separate phases:
  - **CM Product Selection** to compare selected products in a few HW validation tests
  - **CM SW Readiness** operational testing (1 vendor)
  - **CM Batch PHY testing** to verify if HW and calibration is within specification limits and to know the offsets (power) for this CM type (1 vendor)
- Write down the tests in more detail and align them with the expectations and plant situations.
- Immediately align the DOCSIS 3.1 CMTS test plan with this CM test plan. This way it is possible to execute CM and CMTS testing at the same time in a more time and cost-efficient way.

To define the full scope of this ATP, a first set of requirements was agreed upon with Customer. All requirements were then grouped into the three different testing phases as described above. Based on this requirement list, a set of tests were defined and described in different test plans.

Current test plan covers the DOCSIS 3.1 **Operational SW Readiness** and is written to verify the final software readiness of a cable modem for the current and future Customer network/topology and configuration. This test set is intended to run each time on a new major software release of the modem vendor.

The first part of this document describes the set of requirements and in the following sections the corresponding tests are defined.

2 General Guidelines

For some tests, the exact interaction with the CMTS/CCAP can play an important role. These tests are foreseen to be executed on the Customer XXXX CMTS/CCAP with a configuration provided by Customer. For some other tests the actual CMTS is not important at all, and Excentis reserves the right to execute those tests on a non-Customer CMTS if this offers practical advantages. This certainly when the Customer CMTS/CCAP would put a limit to the tests but are useful to test for future configuration and features.

Wi-Fi is turned off during all tests, unless specified otherwise.

Modem is expected to be delivered with correct software and factory defaults.

For voice it is expected that the E-MTA works according to the PC1.5 specification.

The scope of the tests in this document is limited to the cable modem (E-MTA, gateway…) device. Any issues discovered with the Customer CMTS in the course of the modem testing will be reported to Customer, but investigating them is outside the scope of the testing described in this document.

All tests will be executed on one unit with exception of the two General Tests and the Stability Test which will be executed on all available units with a maximum of seven units.

Please note that when issues are discovered that point towards the CMTS instead of the modem, they will be reported to Customer but it is outside the scope of this test to investigate or solve them.

For quite some tests it will be the first time that these will be executed on [redacted] CMTS. Because of that, it might happen, while executing the tests, that some modifications to the test or configuration might be useful. Any of these modifications will be updated into this test plan and Customer will be notified.

3 DOCSIS 3.1 CPE Requirements

The requirements are listed:

- Using the previously defined test plan for modems
- Adding requirements for DOCSIS 3.1 after discussion with Customer

General Requirements

REQ Tag	Requirement Description [Testcase]	Remark
REQ-Gen-01	The devices MAC addresses are consistent with CM label, box label and real MAC address seen by the CMTS Test: MAC Address consistency	
REQ-Gen-02	The devices all have the correct firmware, software and bootloader Test: Version	
REQ-Gen-03	The devices support the ED3.0 and D3.1 MIBs and can be contacted (read/write) by SNMP with access restrictions Test: OSS	
REQ-Gen-04	The device must support configuration file enabled traffic rate limiting as per DOCSIS 3.1 specification. Test: Stability test	Using Customer RF configuration
REQ-Gen-05	The device must function stably over a long time period. Test: Stability test	Stability test with OFDM/(OFDMA)

SC-QAM/3.0 Requirements

REQ Tag	Requirement Description [Testcase]	Remark
REQ-30-01	The device is backwards compatible with current Customer RF network and EuroDOCSIS 3.0 deployment. - 16 | 20 | 24 | 32 x SC-QAM downstream Annex A - 4 | 6 | 8 x SC-QAM upstream 6.4 MHz Test: Stability test	Stability test Combine with CMTS testing
REQ-30-02	The device has sufficient resources to provide future data forwarding services. Forwarding capabilities and latency/round-trip time under different circumstances must be known. This in ED3.0 (32x8) mode. e.g. Routed mode, DS-Lite, IPv4, IPv6, filters and classifiers, UDP (different packet sizes, up, down and bidirectional) and TCP (different amount of sessions, down, up and bidirectional) Test: UDP Throughput and Latency Determination & TCP Throughput and Round-Trip Time Determination 3.0	Extensive throughput testing on final product
REQ-30-03	The device must enter and leave upstream and downstream partial service mode fluently. This for the downstream and upstream SC-QAMs. Test: Partial Service 3.0	

REQ Tag	Requirement Description [Testcase]	Remark
REQ-30- 04	With only SC-QAM downstream channels in the spectrum, the time it takes until data can be forwarded will be determined. Test: Modem Boot Process 3.0	

OFDM(A)/3.1 Requirements

REQ Tag	Requirement Description [Testcase]	Remark
REQ-31-01	The device must enter and leave upstream and downstream partial service mode fluently. This for the combination SC-QAMs and OFDM(A) channels. Test: Partial Service 3.1	
REQ-31- 02	The device has sufficient resources to provide future data forwarding services. Forwarding capabilities and latency/round-trip time under different circumstances must be known. This in ED3.1 (32x0 + 2x2) mode. e.g. Routed mode, DS-Lite, IPv4, IPv6, filters and classifiers, UDP (different packet sizes, up, down and bidirectional) and TCP (different amount of sessions, down, up and bidirectional) Test: UDP Throughput and Latency Determination & TCP Throughput and Round-Trip Time Determination 3.1	There might be CMTS limitations Only OFDM possible too

Upstream

REQ Tag	Requirement Description [Testcase]	Remark
REQ-31-US-01	The device must be able to use mixed modulation OFDMA channels. Test: Mixed Modulation Upstream	There might be CMTS limitations
REQ-31-US-02	The device must support OFDMA upstream profile promotion and demotion. Test: Upstream Profile Promotion – Probing & Test SID	There might be CMTS limitations
REQ-31-US-03	The device must have active queue management support Test: AQM	

Downstream

REQ Tag	Requirement Description [Testcase]	Remark
REQ-31-DS-01	The device must be able to receive mixed modulation OFDM channels. Test: OFDM Operation	There might be CMTS limitations
REQ-31-DS-02	The device must be able to receive OFDM channels with exclusion bands (eg. avoiding LTE). Test: OFDM Operation	There might be CMTS limitations
REQ-31-DS-03	The device must support and report Partial Channel Mode Test: OFDM Partial Channel Mode	

REQ Tag	Requirement Description [Testcase]	Remark
REQ-31-DS-04	With both SC-QAM and OFDM downstream channels in the spectrum, the modem must first lock and initialize using an OFDM downstream channel. This within 60 seconds. The time it takes until data can be forwarded will also be determined. Test: Modem Boot Process 3.1	
REQ-31-DS-05	The device must support OFDM downstream profile promotion and demotion. Test: Downstream Profile Promotion - OPT	There might be CMTS limitations

E-MTA

REQ Tag	Requirement Description [Testcase]	Remark
REQ-MTA-01	Voice Quality	
REQ-MTA-02	Long duration call	
REQ-MTA-03	Caller ID	
REQ-MTA-04	Call progress tones	
REQ-MTA-05	Attenuation	

E-Router

REQ Tag	Requirement Description [Testcase]	Remark
REQ-eR-01	Configuration interface check Test: Verify available configurations in the web interface	
REQ-eR-02	Bridged/Routed/Dual Stack mode IPv4 & IPv6 Test: Basic provisioning and traffic tests	
REQ-eR-03	Basic TR-069 support Test: Configuration of the eRouter using TR-069	
REQ-eR-04	DNS support Test: DNS functionality in IPv4 and IPv6	
REQ-eR-05	Prefix delegation	
REQ-eR-06	DS-Lite	Not for now

Wi-Fi

REQ Tag	Requirement Description [Testcase]	Remark
REQ-WiFi-01	Configuration interface check	
REQ-WiFi-02	Security verification	
REQ-WiFi-03	Wi-Fi performance – Single client (coverage)	
REQ-WiFi-04	Wi-Fi performance – Airtime fairness (multiple clients)	

REQ Tag	Requirement Description [Testcase]	Remark
REQ-WiFi-05	Wi-Fi performance – Neighboring APs	
REQ-WiFi-06	Wi-Fi LTE interference verification	New REQ Dec 2018, test not defined yet
REQ-WiFi-07	Wi-Fi band steering	New REQ Dec 2018, test not defined yet

L2VPN

REQ Tag	Requirement Description [Testcase]	Remark
REQ-L2VPN-01	L2VPN TOS classification	
REQ-L2VPN-02	L2VPN DUT filtering	
REQ-L2VPN-03	L2VPN forwarding	

4 Unboxing Tests

These tests will be executed on all available units with a maximum of seven units.

4.1 MAC Address Consistency

Test description

To be sure of correct packaging and labeling, the consistency between all available MAC addresses will be verified.

When available this will be the MAC address on the cable modem case, on the cable modem unit and fetching the cable modem MIB.

Expected results

All MAC addresses are consistent.

Reported results

- PASS/FAIL

4.2 Firmware/Software Version, Bootloader

Test description

To be sure of correctly installed firmware and software, the firmware version and software version will be retrieved from all cable modem MIBs. This will be compared with the information received from Customer regarding the expected firmware and software.

In case the cable modem has a boot-loader mentioned in the System Descriptor MIB-object (sysDescr.0), the information will be verified for consistency.

Expected results

All fetched versions are consistent and as expected.

Reported results

- PASS/FAIL
- Table providing overview of CM MAC and system descriptors:

CM MAC	CM sysDescr.0 MIB

5 EuroDOCSIS 3.0 Validation Tests

Channel Configurations

Exact CMTS configuration is provided by Customer. In case no exact config can be provided the following config will be applied but can be adapted depending on the CMTS capabilities.

SC-QAM Downstream Configurations					
Channel Config	Number of Channels	Modulation	Center Frequencies	Channel Power	CM Diplex Config
1	32	256-QAM	266 -› 386 + 410 -› 522 MHz	0 dBmV	108-862 MHz

3.0 SC-QAM Downstream Configurations

SC-QAM Upstream Configurations						
Channel Config	Number of Channels	Channel Bandwidth	Modulation	Center Frequencies	Channel Power	CM Diplex Config
1	6	6.4 MHz	64-QAM	20, 28, 36, 44, 52, 60 MHz	50 dBmV	5-65 MHz

3.0 SC-QAM Upstream Configurations

5.1 TCP Subscription Speeds ED3.0

Test description

This test determines whether the current or near-future TCP maximum subscription speed rates can be offered in a stable way. It will also be verified whether the Round-trip Time is within limits.

The node topology will only consist out of ED3.0 SC-QAMs.

Test conditions

The CMTS configuration will be provided by Customer, as well as the cable modem configuration file. The current or near-future maximum subscription speed rate downstream and upstream needs to be provided to set for rate limiting.

Following scenarios will be tested:

- TCP - downstream - IPv4 - two sessions - 2 Eth ports (1 session per port)
- TCP - downstream - IPv4 - 10 sessions - 2 Eth ports
- TCP - upstream - IPv4 - single session
- TCP - upstream - IPv4 - 10 sessions - 2 Eth ports
- TCP - downstream - IPv6 – 10 sessions - 2 Eth ports
- TCP - upstream - IPv6 - 10 sessions - 2 Eth ports
- TCP – downstream and upstream – IPv4 – 4 sessions each - 2 Eth ports

The expected best receive window size and receive window scale is determined for maximum throughput, based on the bandwidth-delay product. Configure SACK with CUBIC as loss detection and congestion avoidance algorithm.

All cases are tested with the modem in routed mode. The cable modem configuration file to be used will be provided by Customer.

For a D3.1 CM, AQM is by default enabled and usually this has an effect on the throughput and Round-Trip Time (RTT). This because AQM is reducing the RTT by dropping a packet when needed. This behaviour will be verified when looking at the ByteBlower TCP result graphs during the tested scenarios. Periodically retransmissions (triggered by packet loss) are expected due to AQM. This must keep the RTT under control while trying to maintain maximum throughput. To compare, one TCP test is done while disabling AQM.

Each measurement is taken over a period of 5 minutes.

Expected results

Reaching the subscription speed over the whole test duration

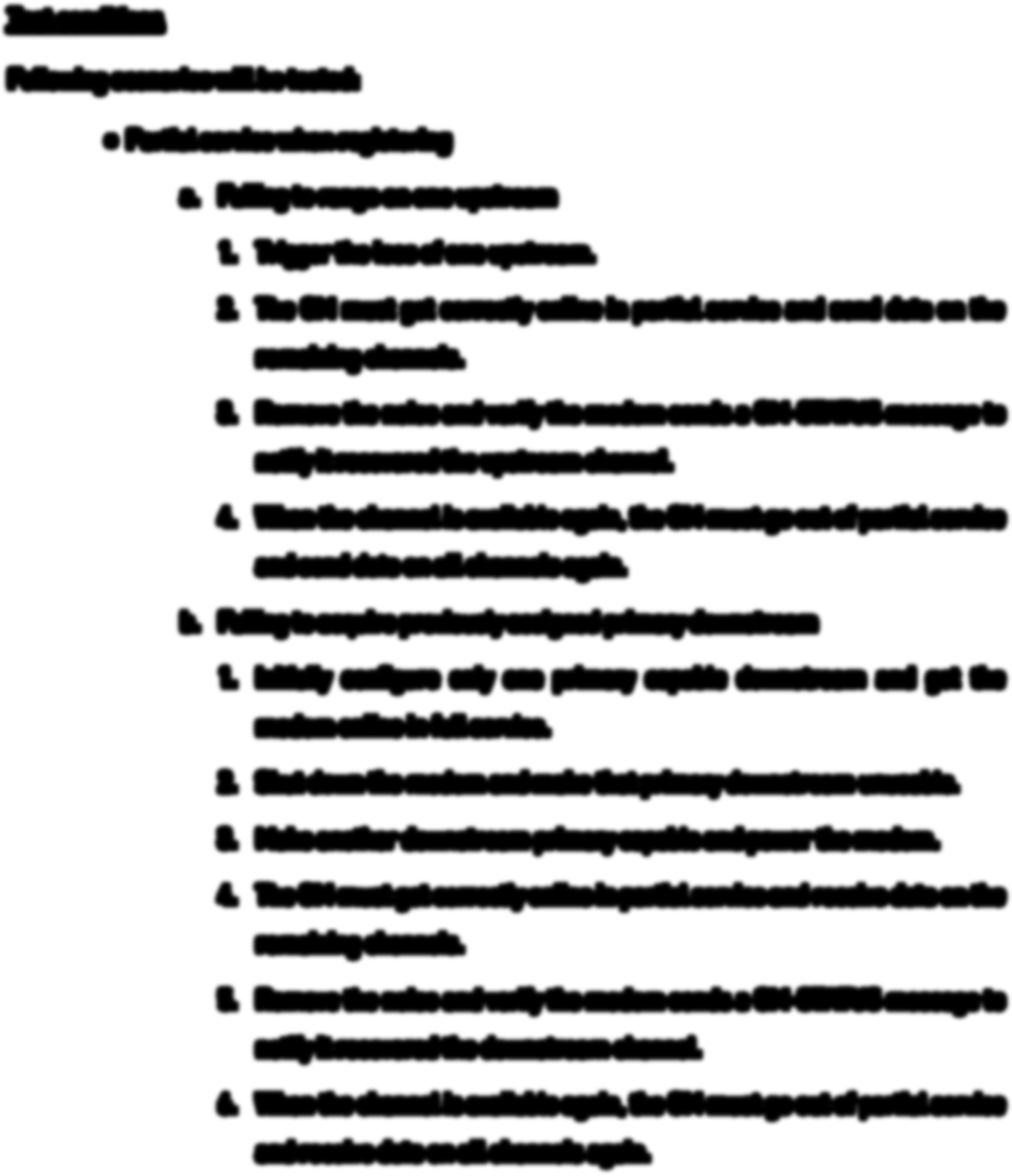
Reported results

Whether service was met and where things went wrong. The test is defined as a trigger to action; root cause analysis is not part of the scope. Average aggregated speeds are reported and in case of any anomalies also the TCP flow graph showing speed over time.

5.2 Partial Service ED3.0

Test description

This test verifies if the CM behaves correctly regarding partial service in a pure EuroDOCSIS 3.0 environment. One or more RF channels will be disturbed by adding sufficient noise to make the channel(s) unusable for the CM. Eventually the channel connection will be restored so the modem can start using it again. The test scenarios are limited to the most likely occurrences of partial service. The CMTS configuration and modem configuration file will be provided by Customer.



- [illegible]

6 Mix EuroDOCSIS 3.0 & DOCSIS 3.1 Validation Tests

Channel Configurations

Exact CMTS configuration is provided by Customer. In case no exact config can be provided the following config will be applied but can be adapted depending on the CMTS capabilities.

SC-QAM Downstream Configurations					
Channel Config	Number of Channels	Modulation	Center Frequencies	Channel Power	CM Diplex Config
1	32	256-QAM	266 -› 386 + 410 -› 522 MHz	0 dBmV	258-1218 MHz

3.0&3.1 SC-QAM Downstream Configurations

OFDM Downstream Configurations						
Channel Config	Start Frequency Active Spectrum	Stop Frequency Active Spectrum	Modulation	Subcarrier Spacing	PLC Frequency	CM Diplex Config
1	606.975 MHz 900.975 MHz	796.975 MHz 994.975 MHz	1024-QAM 512-QAM	50 kHz	700 MHz 920 MHz	258-1218 MHz
The following parameters are fixed for all OFDM channels: - Cyclic Prefix: 2.5 µs - Roll-Off Period: 1.25 µs - Pilot Scale Factor: 48 - Taper Region: 1 MHz - NCP modulation: 16-QAM - Time Interleave Depth: 8 - Power: 0 dBmV per 6 MHz PLC frequency is the center frequency of the first subcarrier of the 6 MHz PLC region.						

3.0&3.1 OFDM Downstream Configurations

SC-QAM Upstream Configurations						
Channel Config	Number of Channels	Channel Bandwidth	Modulation	Center Frequencies	Channel Power	CM Diplex Config
1	8	6.4 MHz	64-QAM	20, 28, 36, 44, 52, 60, 68, 76 MHz	50 dBmV	5-204 MHz

3.0&3.1 SC-QAM Upstream Configurations

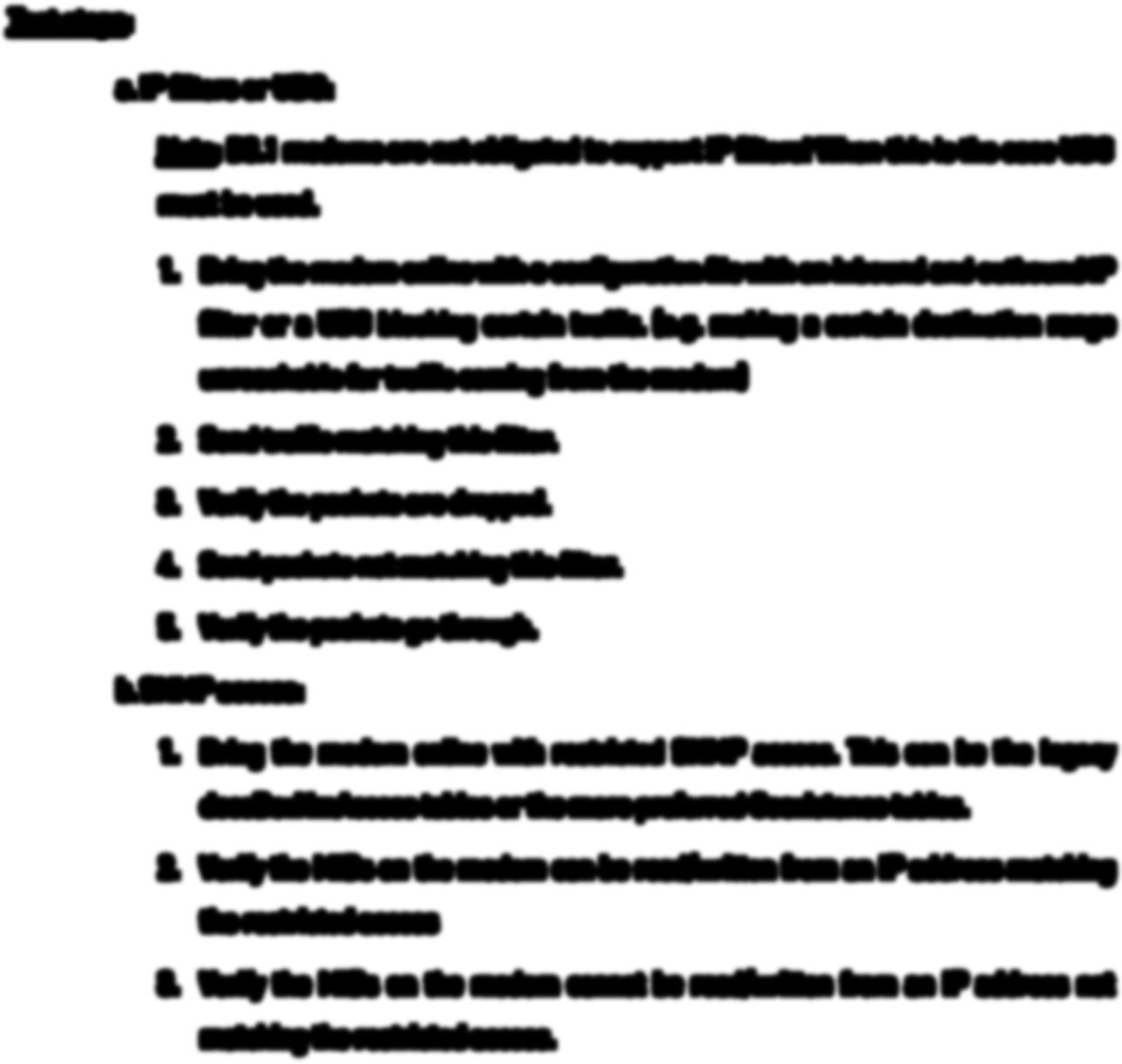
	OFDMA Upstream Configurations					
Channel Config	Start Frequency	Stop Frequency	Modulation	Subcarrier Spacing	Channel Power (per 1.6 MHz)	CM Diplex Config
1	108.975 MHz	203.975 MHz	256-QAM	50 kHz	44 dBmV	5-204 MHz
	- The following parameters are fixed for all OFDMA channels: - Cyclic Prefix: 2.5 µs - Roll-Off Period: 1.25 µs - Pilot-Pattern: 2 (1-14) - Number of Symbols per Frame: 16 (6-36)					

3.0&3.1 OFDMA Upstream Configurations

6.1 IP Filters and SNMP Restricted Access

Test description

This test verifies the correct implementation of legacy IP filters or the more preferred Upstream Drop Classifiers (UDC) by the modem. Whichever is used by Customer will be tested. The restriction of SNMP access (how Customer does it) will be verified as well. The CMTS configuration will be provided by Customer. A Customer-provided modem configuration file can be used as a basis for this test.



Expected results:

- Filtering (IP filter or UDC) works as expected
- Access works as specified in the CM config file

Reported results:

- PASS/FAIL

6.2 MIB Support

Test description: This test verifies the modem has implemented the relevant 3.0 and 3.1 PHY-related MIBs. It also verifies if the legacy spectrum analysis and the 3.1 downstream MER PNM functionality is implemented. This test will not verify the accuracy of all the PHY-related MIBs, but will verify if the software supports them. The modem configuration file and CMTS configuration will be provided by Customer.

Test steps:

a. Bring the modem online on the test point configuration with the defined configuration file.

b. Verify the following MIB tables are populated:

1. Legacy MIBs:

docsIfDownstreamChannelTable
docsIfUpstreamChannelTable
docsIfSignalQualityTable
docsIf3CmStatusTable
docsIf3CmStatusUsTable
docsIf3SignalQualityExtTable

2. 3.1 MIBs:

docsIf31RxChStatusTable
docsIf31CmDsOfdmChanTable
docsIf31CmDsOfdmProfileStatsTable
docsIf31CmDsOfdmChannelPowerTable
docsIf31CmStatusOfdmaUsTable
docsIf31CmUsOfdmaChanTable
docsIf31CmUsOfdmaProfileStatsTable
docsIf31CmUsOfdmaMinislotCfgStateTable
docsIf31CmSystemCfgState
docsIf31CmUsScQamChanTable

c. Verify the spectrum analysis is implemented by enabling the docsIf3CmSpectrumAnalysisCtrlCmdEnable MIB and confirm the docsIf3CmSpectrumAnalysisMeasTable is populated.

d. Verify the OFDM downstream MER per subcarrier can be retrieved using the PNM tools:

1) Set the docsPnmBulkDestIpAddr and docsPnmBulkDestIpAddrType MIBs to your TFTP server IP.

2) Configure the docsPnmCmDsOfdmRxMerFileName and start the measurement by enabling the docsPnmCmDsOfdmRxMerFileEnable MIB.

3) Confirm the modem uploaded the MER-per-subcarrier file to your TFTP server.

Expected results:

- All listed (mandatory) (Euro)DOCSIS MIBs are populated

Reported results:

- PASS/FAIL

6.3 Stability Test

Test description:

This test verifies the operation, stability and interoperability of the CPE device in a simulated real-life setup. The CPE device and its services should operate in a stable and uninterrupted manner for four days. During this test time, we make sure the CPE devices remain online and handle periodic network events (like DHCP renewals, BPI+ key exchanges and load balancing) well. Data service is tested by looking at packet loss, data rates and TCP connection failures. Voice service is tested by looking at voice connection failures and dropped calls.

We automatically gather relevant data from the CMTS, CPE, provisioning system and traffic generator during the test. We report anomalies and use the gathered data to do an initial investigation. This analysis drills down to a specific network component, but a full root cause analysis is outside the test scope.

Test conditions:

- The CMTS configuration will be provided by Customer, as well as the cable modem configuration file (based on the currently used configuration file, with perhaps extra filters/classifiers, for future-proofness) and the E-DVA configuration.
- Half of the units will be offered a TCP traffic load, the other half of the units a UDP traffic load.
- Monitoring software will run during the test to provide additional information in case issues are discovered. If issues are discovered that point towards the CMTS instead of the modem, they will be reported but will be outside the scope of this test to investigate or solve them.
- The exact node topology and channel configurations (SC-QAM and OFDM/OFDMA) depend on the expected field CMTS/CCAP configuration at the time of the rollout of the modem under test. Each time this test needs to be executed, the exact CMTS/CCAP configuration needs to be provided.
- As long as the D3.1 DUT will also be deployed in a pure ED3.0 configuration (without OFDM(A)) it is recommended to test both the pure ED3.0 situation and the situation of ED3.0 combined with D3.1. This could be done using two Mac Domain types (pure 3.0 and mix 3.0/3.1) and 7 modems (eg. resp 3 and 4 per Mac Domain type). One Mac Domain type would have only ED3.0 channels and the other would have both SC-QAMs and OFDM(A) channels. Once no ED3.0-only nodes exist, all Mac Domains can be configured for mix ED3.0 and D3.1 or D3.1-only.
- The CM and E-DVA config files to be used are provided, routed or bridged mode needs to be explicitly set in the config file.
- When available reference modems will be added to the setup for reasons of comparison in case any issues might show up.
- Measurements are executed with an Excentis ByteBlower. The traffic load runs through each of the 7 DUTs over a period of 4 days.
- The load is defined by:

        - UDP traffic over 4 DUT units + extra reference CMs, with 2 flows per CM:
            - Upstream 512B at 2000 pps
            - Downstream 1024B at 5000 pps
        - TCP traffic over 3 DUT units: loops of one-hour TCP sessions with random TCP-interval start times between 0 and 120 seconds. These flows run upstream and downstream and are limited in rate by the Service Flow definition in the provided CM configuration file or rate limited within the TCP session (50 Mbps down and 10Mbps up).
        - 1.5 hour multicast sessions are periodically set up to seven modems (8.5 Mbps). The 15 sessions with different source address are spread over the seven modems where one modem does not receive more than three multicast sessions at the same time. Modems on the same mac domain share one multicast stream. Additionally a 1 kbps multicast flow with a duration of 24 hours is periodically sent to all seven modems.
- Set voice calls up between all modems. These calls will be renewed approximately every five minutes, to have voice traffic during the entire test. Two modems are UDP loaded and two TCP loaded. The E-DVAs have a SIP stack.
- The CM diplexer will be selected according to the test scenario.
- During the whole test duration, detailed monitoring on the CM/CMTS MIBs is performed. Items that are monitored:
    - Modem flaps
    - Partial Service / Partial Channel Mode
    - FEC statistics (CCR, CER on all profiles)
    - docsDevEvText
    - Signal Quality
    - Power Levels
    - Ranging status
    - Voice packet loss

Expected results

- Stable behaviour of the modems
    - All modems use all channels, no partial service occurred.
    - No modems flapped
- Stable uninterrupted services:
    - Not a single TCP session has a timeout and the total number of sessions is as expected (total time divided by session time including random gap).
    - The DUT rate limits the TCP sessions (downstream and upstream) in case this is specified in the modem config files and the TCP speed is stable over time.
    - No significant (>1%) UDP traffic loss is expected.
    - The multicast sessions are successfully joined and forwarded.

- No voice set up events are expected.

Reported results

- Modem stability: all impacting events will be listed
- Service stability: service drops and degradations will be listed (UDP traffic loss over time, failed TCP sessions, unstable TCP speeds, voice packet loss)
- In case of anomalies in the results above, the gathered SNMP data (of monitoring the CMTS and CM's) will be analyzed. This analysis will be drilled down to CMTS or CM component

6.4 TCP Subscription Speeds ED3.0 & D3.1

Test description

Customer should comply with the data services it offers to customers.

This service rate compliance test determines whether the current or near-future TCP maximum subscription speed rates can be offered in a stable way. Both IPv4 and IPv6 service is covered. In all these cases TCP throughput similar to a speed test is measured, but over a period of 5 minutes. It will also be verified whether the Round-trip Time is within limits.

This test is changed compared to previous throughput tests in that way that for software validation the idea is to verify whether current and near-future subscription rates can be offered. Unlimited throughput tests are intended for hardware tests.

The node topology will only consist out of ED3.0 SC-QAMs and D3.1 OFDM(A) channels.

Test conditions

The CMTS configuration will be provided by Customer, as well as the cable modem configuration file. The current or near-future maximum subscription speed rate downstream and upstream needs to be provided to set for rate limiting.

Following scenarios will be tested:

- TCP - downstream - IPv4 - two sessions –‹X› Eth ports (1 session per port)
- TCP - downstream - IPv4 - 10 sessions - ‹X› Eth ports
- TCP - upstream - IPv4 - single session - ‹X› Eth ports
- TCP - upstream - IPv4 - 10 sessions - ‹X› Eth ports
- TCP - downstream - IPv6 – 10 sessions - ‹X› Eth ports
- TCP - upstream - IPv6 - 10 sessions - ‹X› Eth ports
- TCP – downstream and upstream – IPv4 – 4 sessions each - ‹X› Eth ports

‹X› Eth ports: depending on how many Eth ports the modem has, what the subscription rate is and what is agreed with Customer.

The expected best receive window size and receive window scale is determined for maximum throughput, based on the bandwidth-delay product. Configure SACK with CUBIC as loss detection and congestion avoidance algorithm.

All cases are tested with the modem in routed mode. The cable modem configuration file to be used will be provided by Customer (based on the currently used configuration file).

For a D3.1 CM, AQM is by default enabled and usually this has effect on the throughput and Round-Trip Time (RTT). This because AQM is reducing the RTT by dropping a packet when needed. This behaviour will be verified when looking at the ByteBlower TCP result graphs during the tested scenarios. Periodically retransmissions (triggered by packet loss) are expected due to AQM. This must keep the RTT under control while trying to maintain maximum throughput. To compare, one TCP test is done while disabling AQM.

Each measurement is taken over a period of 5 minutes.

Expected results

Reaching the subscription speed over the whole test duration

Reported results

Whether service was met and where things went wrong. The test is defined as a trigger to action; root cause analysis is not part of the scope. Average aggregated speeds are reported and in case of any anomalies also the TCP flow graph showing speed over time.

Example:

Test	TCP Throughput [Mbit/s]	Expected TCP Throughput [Mbit/s]	RTT Avg [ms]
Downstream - IPv4 - 2 sessions - 2 Eth ports			
Downstream - IPv4 - 10 sessions - 2 Eth ports			
Downstream - IPv6 – 10 sessions - 2 Eth ports			
Downstream & upstream – IPv4 – 4 sessions each - 2 Eth ports			
Upstream - IPv4 - 1 session			
Upstream - IPv4 - 10 sessions - 2 Eth ports			
Upstream - IPv6 - 10 sessions - 2 Eth ports			

Measuring TCP throughput with only a few TCP sessions usually does not deliver the maximum rate, therefore the test is also executed using 10 TCP sessions.

The maximum RTT needs to be below 1 s, so no severe service impact is expected. The average RTT is typically between 20 and 50 ms. Also note here that AQM is enabled for the modem (as this is by default the case).

6.5 Partial Service ED3.0 & D3.1

Test description

This test verifies if the CM behaves correctly regarding partial service in a mixed EuroDOCSIS 3.0 and DOCSIS 3.1 environment. One or more RF channels will be disturbed by adding sufficient noise to make the channel(s) unusable for the CM. Eventually the channel connection will be restored so the modem can start using it again. The test scenarios are limited to the most likely occurrences of partial service.

General Test Conditions

Partial Service Concept

For downstream partial service, the CMTS can be informed about a channel loss or recovery through:

- CM-STATUS messages from the CM
  - Event type 1 – Secondary channel MDD timeout
  - Event type 2 – QAM/FEC lock failure
  - Event type 4 – Secondary channel MDD recovery
  - Event type 5 – QAM/FEC lock recovery
  - Event type 16 – DS OFDM profile failure
  - Event type 17 – Primary Downstream Change
  - Event type 20 – NCP profile failure
  - Event type 21 – PLC failure
  - Event type 22 – NCP profile recovery
  - Event type 23 – PLC recovery
  - Event type 24 – OFDM profile recovery

For upstream partial service, the CMTS can learn about a channel loss or recovery through:

- CM-STATUS messages by the modem
  - Event type 6 – T4 timeout
  - Event type 7 – T3 retries exceeded
  - Event type 8 – Successful ranging after T3 retries exceeded
  - Event type 25 – OFDMA Profile failure
- The failure or success of ranging
- A change in codeword error rate (FEC CER)

Test triggers

Defining when exactly a channel will be lost is difficult as the loss of a channel is related to the FEC error rate and/or MER, which is a vendor specific defined value which is not necessarily configurable. To verify MER triggers, ingress noise interference can be used, to verify FEC based triggers, impulse noise can be used. Ingress noise can be simulated by adding QAM signal(s) within the whole channel. Drive the MER just below the MER lower limit corresponding to the modulation targeted to lose (lowest profile). The power level of this interfering signal needs to be controllable by changing the power level of the signal or by using a controllable attenuator. Impulse noise can be generated using a signal generator. Drive the FEC CCR/CER just above the limit corresponding to the profile targeted to lose (lowest one). The power level and time duration of this interfering signal is controllable using the signal generator. When introducing noise, it needs to be verified that other channels are not impacted. This can be done by validating the SNR and CER on all channels (using the relevant MIBs).

Result Verification

During the test, ByteBlower traffic will be sent downstream at about nearly the maximal throughput to see the traffic forwarding behavior during partial service states. From these results it can be verified that the throughput in each test phase corresponds to the available channel capacity.

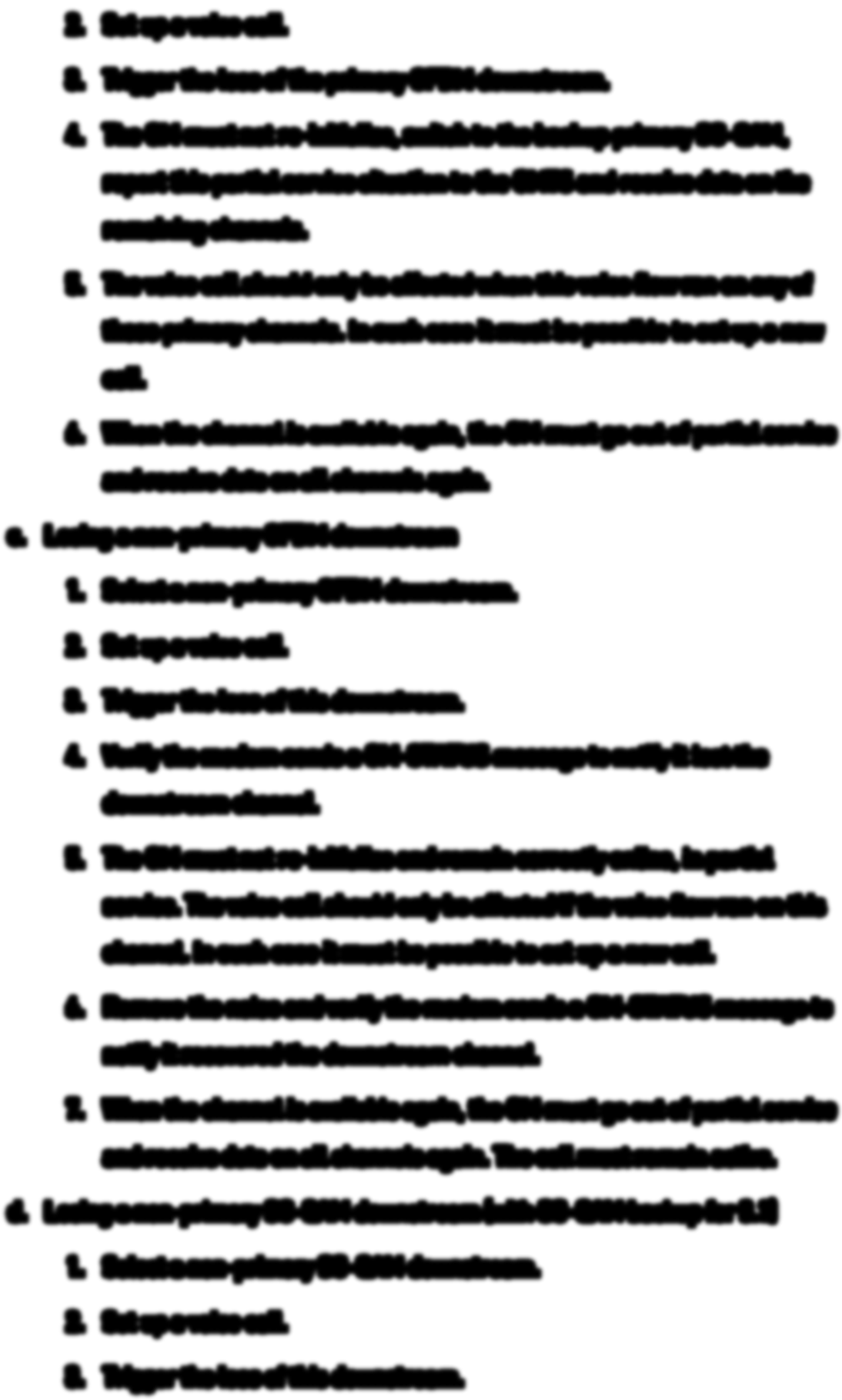
For each channel recovery, the time it takes until a channel is usable again is recorded (maximum waiting time 15 minutes).

Partial service mode can be detected using:

- CMTS CLI: command showing lost channels and/or with CMTS debug/event logs showing CM-STATUS messages
- CM & CMTS MIBs: docsIf3CmtsCmUsStatusRangingStatus, docsIfDownChannelPower, docsIf3SignalQualityExtRxMER, docsIf3CmStatusUsRangingStatus, docsIf31CmtsCmUsOfdmaChannelStatusTable, docsIf31CmtsCmDsOfdmChannelStatusTable and docsIf31CmStatusOfdmaUsTable

[redacted]

[redacted]



[illegible]

[redacted]

[redacted]

- [redacted]
- [redacted]

6.6 Active Queue Management

Test description

With AQM the modem shapes upstream traffic in such a way that high-speed TCP data rates are improved. However, bad implementations or configurations can easily cause severe negative impact on the end-user throughput. By comparing AQM-disabled and AQM-enabled data rates, we see the optimization (if any) AQM brings and whether the optimization is needed to meet the data services offered by Customer.

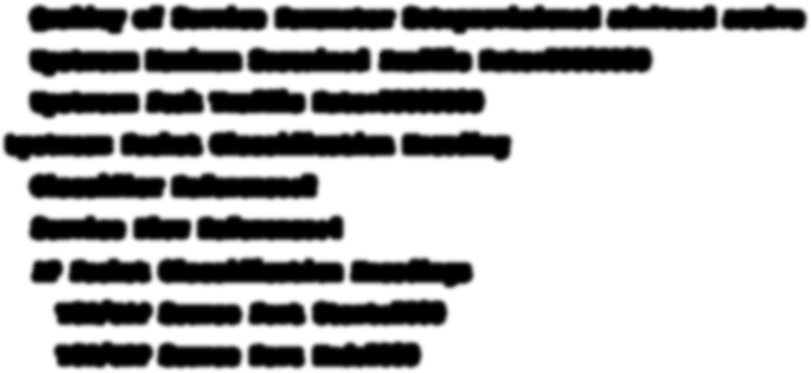
This test verifies that the device has active queue management (AQM) support. DOCSIS 3.1 introduces Active Queue Management algorithm that manages queuing latency in an upstream service flow by predicting the queuing latency of each packet that arrives at the service flow buffer and using the predicted latency as an input to a control law that determines whether to enqueue the packet or drop the packet.

Test conditions

The interplay between AQM and TCP is a complex affair and depends heavily on the type of TCP traffic. In this test the effect of enabling AQM on variety of real-life traffic patterns is observed. When enabled, AQM is configured according to the Customer configuration. We expect AQM with the Customer settings to keep the TCP round-trip time in check and improve the general throughput.

The overall performance gain is shown by enabling AQM, and any remarkable results (e.g. for a specific traffic pattern) are reported.

Test steps



1. Transmit TCP upstream traffic over both service flows (using the TCP source port as differentiator) during 2 minutes. Store the ByteBlower report for further examination.

   Get the modem online, with the following modem configuration file upstream service flows:

AQM must be enabled by default by the CM. The upstream service flows have different latency targets and corresponding classifiers to verify the difference between both settings.

2. Transmit TCP upstream traffic over each service flow (using the TCP source port as differentiator) for 2 minutes. In case different TCP settings result in a different behavior a few realistic settings will be compared.
3. Verify the difference in average speed and Round-Trip Times between:
    a. AQM enabled and disabled
    b. The two TCP flows (different service flow) in case AQM is enabled

Channel configurations

See Channel Configuration but with reduced physical capacity to limit the needed speeds.

Expected results

It is expected to have a positive effect of AQM and that the defined latency targets are met when AQM is enabled. The packet loss in the TCP flow is expected to be random when AQM is dropping packets to get the latency target.

Anomalies or service degradations are shown, but a root cause analysis of the AQM algorithm is not part of the scope.

Reported results

- ByteBlower results displaying the effect of AQM

6.7 Modem Boot Process

Test description

This test determines the time the CM needs to get operational after a power reboot and to forward data. In this test it will also be verified that the CM does lock first on an OFDM channel in a mixed (OFDM/SC-QAM) downstream configuration.

Test conditions

The CMTS configuration and the modem configuration file will be provided by Customer.

Test steps

1. Bring the modem online on a CMTS config with no OFDM channels. This is to be able to verify the modem locks first on OFDM channels in a mixed environment.
2. Shut the modem down.
3. Connect the modem to the correct CMTS configuration (which includes at least one OFDM downstream channel).
4. Start a timer and power the CM.
5. Verify it sends the bonded initial ranging request with the OFDM downstream as downstream channel. The CMTS CLI can be used for this.
6. Record the time until data can be forwarded by the modem. This must be less than three minutes.
7. Keep on sending data for at least another three minutes to make sure the forwarding of data remains up and no extra internal resets take place.

Expected results:

The total boot time must be less than three minutes.

Reported results:

- PASS/FAIL
- Boot time until traffic forwarding

7 DOCSIS 3.1 Validation Tests

Channel Configurations

Exact CMTS configuration is provided by Customer. In case no exact config can be provided the following config will be applied but can be adapted depending on the CMTS capabilities.

OFDM Downstream Configurations						
Channel Config	**Start Frequency Active Spectrum**	**Stop Frequency Active Spectrum**	**Default Modulation**	**Subcarrier Spacing**	**PLC Frequency**	**CM Diplex Config**
1	606.975 MHz 900.975 MHz	796.975 MHz 994.975 MHz	1024-QAM 512-QAM	50 kHz	700 MHz 920 MHz	258-1218 MHz
The following parameters are fixed for all OFDM channels: - Cyclic Prefix: 2.5 µs - Roll-Off Period: 1.25 µs - Pilot Scale Factor: 48 - Taper Region: 1 MHz - NCP modulation: 16-QAM - Time Interleave Depth: 8 - Power: 0 dBmV per 6 MHz PLC frequency is the center frequency of the first subcarrier of the 6 MHz PLC region.						

Table 1: TC-31-02 OFDM Downstream Configurations

Downstream Modulation Configurations						
Channel Config	**Start Frequency Modulation 1**	**Stop Frequency Modulation 1**	**Modulation 1**	**Start Frequency Modulation 2**	**Stop Frequency Modulation 2**	**Modulation 2**
1	606.975 MHz 906.975 MHz	700.975 MHz 930.975 MHz	2048-QAM 256-QAM	790.975 MHz 950.975 MHz	796.975 MHz 951.975 MHz	256-QAM Exclusion

Table 2: TC-31-02 OFDM Downstream Modulations

	OFDMA Upstream Configurations					
Channel Config	**Start Frequency**	**Stop Frequency**	**Modulation**	**Subcarrier Spacing**	**Channel Power (per 1.6 MHz)**	**CM Diplex Config**
1	108.975 MHz	203.975 MHz	256-QAM	50 kHz	44 dBmV	5-204 MHz
	- The following parameters are fixed for all OFDMA channels: - Cyclic Prefix: 2.5 µs - Roll-Off Period: 1.25 µs - Pilot-Pattern: 2 (1-14) - Number of Symbols per Frame: 16 (6-36)					

Table 3: TC-31-02 OFDMA Upstream Configurations

Upstream Modulation Configurations						
Channel Config	**Start Frequency Modulation 1**	**Stop Frequency Modulation 1**	**Modulation 1**	**Start Frequency Modulation 2**	**Stop Frequency Modulation 2**	**Modulation 2**
1	116.975 MHz	126.975 MHz	128-QAM	146.975 MHz	156.975 MHz	Zero-Valued

Table 4: TC-31-02 OFDMA Upstream Modulations

7.1 OFDM Profile Management

Test description

This test verifies the OFDM downstream profile promotion and demotion functionality on the CM, together with the partial channel reporting. An OFDM channel will be disturbed so that some of the assigned profiles within an OFDM channel become unusable by the CM. The CM must report this event (loss of profile) to the CMTS, and based on this the CMTS can switch to a lower profile. The CM must be able to forward data on these profiles and continue forwarding after a profile switch. Afterwards the channel is restored to normal connection again. The test scenarios are limited to the most likely occurrences of partial channel mode. The modem configuration file and CMTS configuration will be provided by Customer.

General Test Conditions

Profile Management Concept

In general the CMTS is informed about a necessary OFDM downstream profile change using:

- CM-STATUS messages from the CM
  - Event type 16 - DS OFDM profile failure
  - Event type 24 - DS OFDM profile recovery
- OPT FEC/MER statistics on a profile to test (initiated by CMTS, measured by CM)

Test triggers

Defining when exactly a profile will be lost is difficult as the loss of a profile is related to the FEC error rate and/or MER, which is a CM vendor specific defined value which is not necessarily configurable. To verify MER triggers, ingress noise interference can be used; to verify FEC based triggers, impulse noise can be used. Ingress noise can be simulated by adding QAM signal(s) within the whole channel. Drive the MER just below the MER lower limit corresponding to the profile targeted to lose. The power level of this interfering signal needs to be controllable by changing the power level of the signal or by using a controllable attenuator. Impulse noise can be generated using a signal generator. Drive the FEC CCR/CER just above the limit corresponding to the profile targeted to lose. The power level and time duration of this interfering signal is controllable using the signal generator. When introducing noise, it needs to be verified that other channels are not impacted. This can be done by validating the SNR (docsIf3SignalQualityExtRxMER MIB) and Codeword Error Rate (docsIf31CmDsOfdmProfileStatsUncorrectableCodewords/ docsIf31CmDsOfdmProfileStatsTotalCodewords on the highest profile) on all channels using the relevant CM MIBs.

Result Verification

During the test, ByteBlower traffic will be sent downstream at about nearly the maximal throughput to see the traffic forwarding behavior during partial channel states. From these results it can be verified that the throughput in each test phase corresponds to the available profile capacity.

The XRA-31 can be used to verify DOCSIS protocol messages.

For each profile recovery, the time it takes until a profile is usable again is recorded (maximum waiting time 15 minutes).

Profile switching and partial channel mode can be detected using:

- CMTS CLI: commands showing lost profiles and/or with CMTS debug/event logs showing CM-STATUS messages
- CM & CMTS MIBs: docsIf31CmtsCmDsOfdmProfileStatusTable, docsIf31CmDsOfdmProfileStatsTable and docsIf31CmtsCmDsOfdmChannelNumPartialChanIncidents

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

```
[redacted]
```

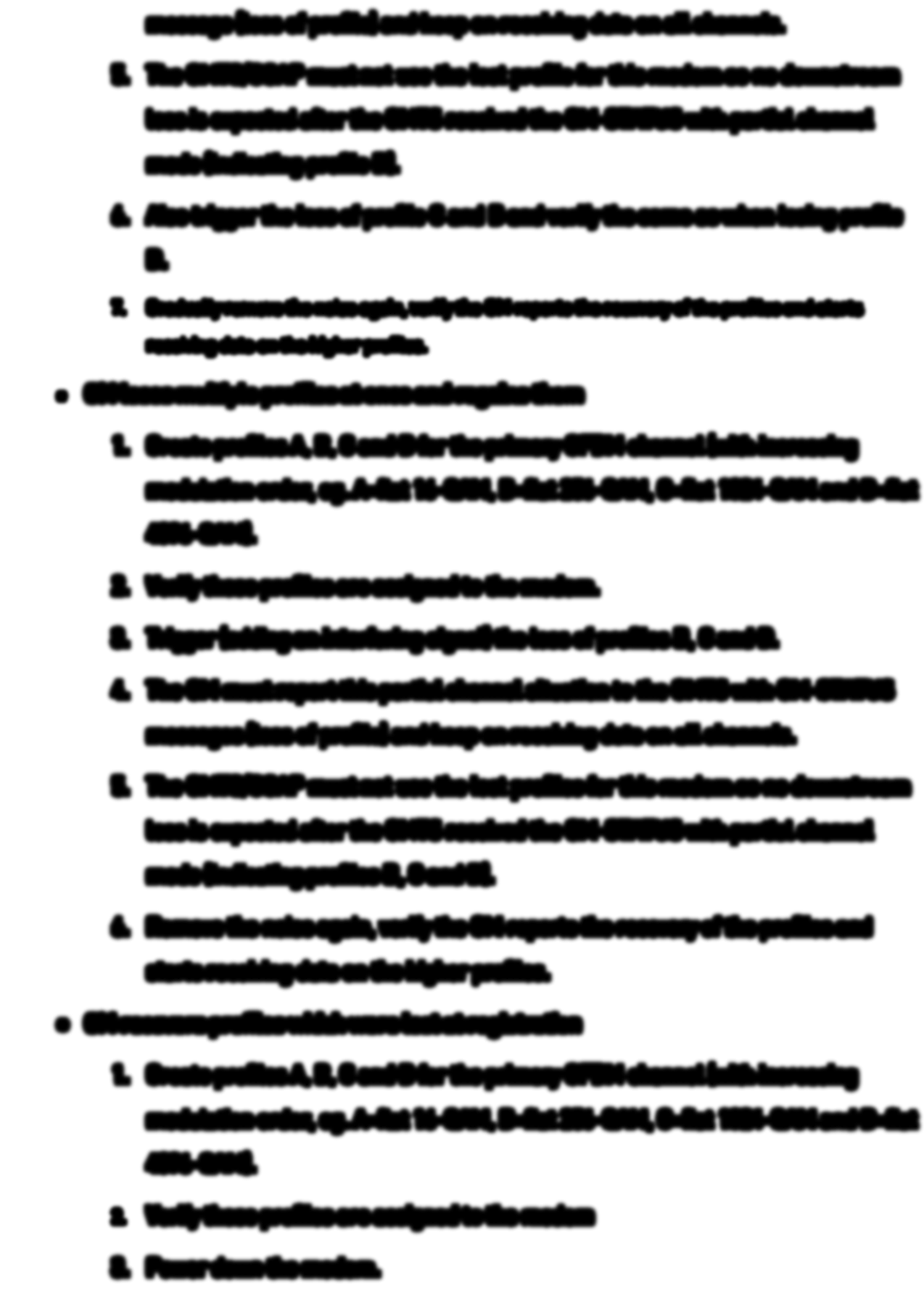
- [redacted]

[redacted]

[redacted]

```
[redacted]
```

[redacted]



[redacted]

Reported results

- PASS/FAIL
- In case of anomalies, ByteBlower graphs showing the traffic forwarding behavior during partial channel states or CM/CMTS logs or MIB values.
- Any remarks on unexpected behaviour seen

7.2 OFDM/OFDMA Mixed Modulation and Exclusions

Test description

This test verifies the modem comes online with different OFDM downstream and OFDMA upstream configurations. Using different modulations and exclusions in both down- and upstream.

Test conditions

Following scenario will be tested:

1. Bring the modem online with the downstream and upstream configuration of the provided channel configuration.
2. Transmit 1500 bytes packets for 15 minutes in the downstream and verify there is no packet loss.
3. Transmit 1500 bytes packets for 15 minutes in the upstream and verify there is no packet loss.

Expected results

No packet loss is expected.

Reported results

- PASS/FAIL

7.3 OFDMA Profile Management

Test description

This test verifies that the modem correctly reacts on probing and/or testing SID to promote or demote the assigned OFDMA profiles. A CMTS has the option of using an upstream probe to take an upstream RxMER measurement. Or a CMTS might wish to gather information on FEC performance for a particular profile, and for this purpose the testing SID can be used. It can be CMTS SW specific how profile promotion and demotion is implemented, hence information regarding this is needed from the CMTS vendor. The specific test can then be adapted according to the specific CMTS mechanism.

General Test Conditions

Profile Management Concept

In general the CMTS can trigger a profile demotion (downgrade) based on:

- FEC statistics on the profile in use (measured by CMTS).
- MER per subcarrier from data transmission or probing (initiated by CMTS, transmission by CM and measured by CMTS).
- Using testing SID (initiated by CMTS, transmission by CM and measured by CMTS). Useful in case CM sends no data and an up-to-date status is preferred.

In general the CMTS can trigger a profile promotion (upgrade) based on:

- FEC statistics on the current profile using live data (measured by CMTS).
- MER per subcarrier from data transmission on current profile or probing (initiated by CMTS, transmission by CM and measured by CMTS).
- Using a "testing SID" on the profile to potentially promote to (initiated by CMTS, transmission by CM and measured by CMTS).

It is expected that combinations of these will provide the best result.

Test triggers

Defining when exactly a profile will be lost is difficult as the loss of a profile is related to the FEC error rate and/or MER, which is a CMTS vendor specific defined value which is not necessarily configurable or has some limitations. To verify MER triggers, ingress noise interference can be used; to verify FEC based triggers, impulse noise can be used. Ingress noise can be simulated by adding completely filled upstream QAM signal(s) within the whole channel (eg. using a CM, a QAM modulator or a signal generator). Drive the MER just below the MER limit corresponding to the profile targeted to lose. The power level of this interfering signal needs to be controllable by changing the power level of the signal or by using a controllable attenuator. Impulse noise can be generated using a signal generator. Drive the FEC CCR/CER just above the limit corresponding to the profile targeted to lose. The power level and time duration of this interfering signal is controllable using the signal generator.

Result Verification

During the test, ByteBlower traffic will be sent upstream at about nearly the maximal throughput to see the traffic forwarding behavior during impaired profile states. From these results it can be verified that the throughput in each test phase corresponds to the available profile capacity.

The XRA-31 can be used to verify DOCSIS protocol messages.

Profile switching can be detected using:

- CMTS CLI: command showing lost profiles and/or with CMTS debug/event logs showing CM-STATUS, DBC and Registration messages
- CM & CMTS MIBs: docsIf31CmtsCmUsOfdmaProfileStatusTable, docsIf31CmUsOfdmaProfileStatsTable, docsIf31CmtsCmRegStatusUsProfileIucList

[redacted]

[redacted]

- [redacted]
  1. [redacted]
  2. [redacted]
  3. [redacted]
  4. [redacted]
  5. [redacted]
  6. [redacted]
  7. [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

[illegible]

[redacted]				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

Reported results

- CER effect on tested tilt configs
- Power reporting accuracy

8 E-MTA CPE Tests

All E-MTA Tests are executed on one unit, except for the Voice Quality test (four units).

8.1 Voice Quality

Test description

Using the same operational parameters as used by Customer (codec and packetization time), this test measures the MOS/PESQ scores, the one-way delay and the jitter on the analogue voice level in a NCS softswitch-based lab environment.

Test conditions

The test setup is the same one as described in the (Euro)DOCSIS Stability Test.

The Voice Quality Test (VQT) will be performed using Spirent Abacus equipment. The measurements are done at the analogue signal level, and are hence true end-to-end tests. The call duration is five minutes and the test runs for 1 hour (about 8 calls). The calls are between DUTs of the same type.

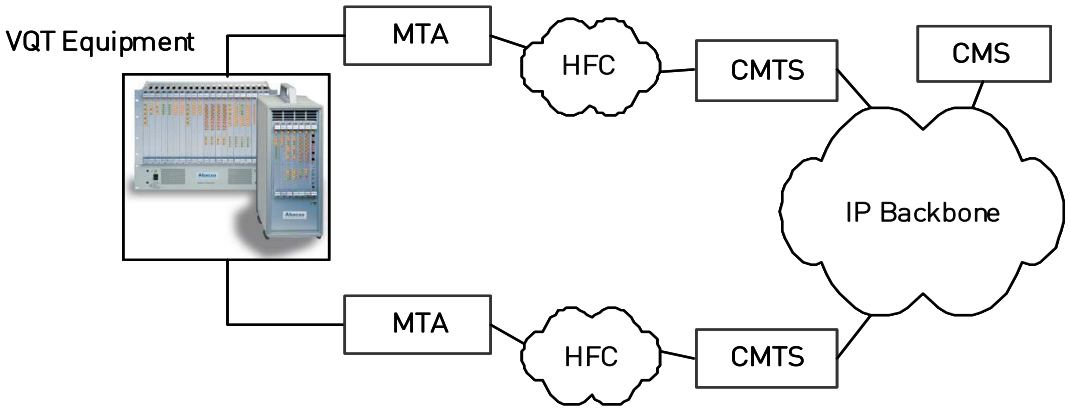
To have a reference, the quality is first measured without any traffic for the duration of two calls. Afterwards the quality is measured with traffic. Like in the Stability Test, two modems are UDP loaded and two TCP loaded.

Background information on the measurements and their meaning:

PESQ Value: this is the result of a PESQ analysis of the phone call. PESQ (Perceptual Evaluation of Speech Quality) is an advanced measurement algorithm designed to objectively determine speech quality. Speech quality (or voice quality) is expressed on the MOS scale (Mean Opinion Score). The MOS scale is defined as follows: 5 “excellent” 4 “good” 3 “fair” 2 “poor” 1 “bad” Although the best MOS score is 5, the PESQ algorithm has an upper limit of 4.5. The reason for this is that 4.5 happens to be the highest score a panel of listeners would report. Since a PESQ value of 4 is conventionally considered “toll quality”, it is desired for the measurements that the average PESQ value is at least 4. The PESQ score is calculated for the incoming voice stream on a channel (or endpoint), and thus depends on the sending MTA, the transmission path from the sending to the receiving MTA, and the receiving MTA.

One-Way Delay: the delay with which the called party receives the speech signal from the caller (expressed in milliseconds with a resolution of 1 ms). Previous measurements showed typical one-way delays around 90 ms while ‹150 ms is acceptable.

Jitter: the difference between two successive measurements of the One-Way Delay value (expressed in milliseconds with a resolution of 1 ms). The jitter in lab environment is typically below 5 ms. Jitter that exceeds 30ms will lower call quality and ›40ms will cause severe deterioration in call quality. Detrimental effects are at 100 ms of jitter.



Expected results

- Average PESQ › 4.0 with a deviation of 0.2 = "toll quality" and there is no difference expected whether traffic load is present or not.
- No call set-up problems.
- The one-way delay and jitter values should be very similar with and without traffic and no value should be problematic.

Reported results

- Average PESQ values, one-way delays and jitters with and without traffic.

Units	Avg no traffic	Avg traffic
PESQ (MOS)		
One-way delay (*ms*)		
Jitter (*ms*)		

8.2 Long duration call

Test description

This test verifies that a call remains active over a period of 6 hours.

Test conditions

1. A call is set up between 2 DUT E-MTAs.
2. The call is left open.
3. After 6h it is verified if the voice path is still established and the E-MTAs are still stable.

Configurations

Same setup as in the Voice Quality test.

Expected results

The voice path is still established after 6 hours.

Reported results

- PASS/FAIL

8.3 Caller ID

Test description

In this short basic functionality test it is verified on the analog line if the E-MTAs are correctly generating the Calling Party Number and the Calling Party Name (FSK type of Caller ID).

The alerting signal can be different depending on country, here it will be tested for the Netherlands.

Test conditions

Configuration file provided by Customer might explicitly set the Caller ID mode.

Expected results:

- The E-MTA correctly generates the Calling Party Number and the Calling Party Name and call timestamp.

Reported results:

- PASS/FAIL

8.4 Call Progress Tones

Test description

In this test it is verified on the analog line if cadence and frequency of dial tone, busy tone, reorder tone, ringback tone and ringing tone are generated according the Dutch specifications. For customer voice experience it is important that the tones are at the right power level and cadence.

Test conditions

Country specific tone settings can be hardcoded in the E-MTA, or configured using a vendor specific MIB in the CM or MTA configuration file, or by explicitly defining the tone parameters in the MTA configuration file. In this case the MIB with OID 1.3.6.1.4.1.4115.10.1.14.0 is set to Integer 9 (Netherlands) in the MTA configuration file.

To measure a tone power level, the analog endpoint of the MTA was connected to the European reference impedance described in the ETSI TS 101 909-18v010301p specification.

Expected results

The measured and MIB value for tone frequency, cadence and power level for each of the five tones need to be within the specified ranges [redacted]

Reported results

For each of the five tones the following table will be reported:

	The Netherlands	MIB value	Measured Value	Result
Frequency				
Cadence				
Power level				

8.5 Attenuation

Test description

For customer voice experience it is important that the right levels are in place. If not according to the specifications, voice could be too silent, too powerful or distorted.

Test conditions

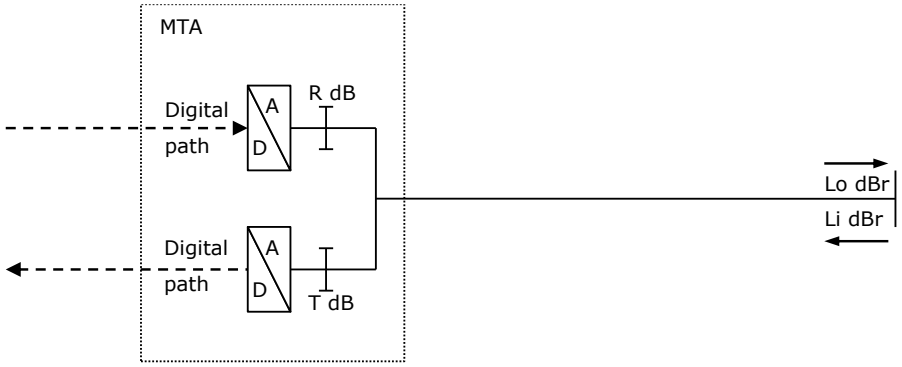
To enable full signal handling capacity, the nominal relative levels (at 1020 Hz) at the CM/MTA must be:

- Input relative level: -4 dBr ± 2dB (analog to digital)
- Output relative level: -11 dBr ± 2dB (digital to analog)

The relative level is assumed to be 0 dBr on the digital side of the analogue/digital conversion point in the local network.

The E-MTA must have the [redacted] impedance (this is not verified here).

Configurations



Expected results

The value of the input relative level must be 4 dB (measured from RTP to analog-in).

The value of the output relative level must be -11 dB (measured from RTP to analog-out).

Reported results

- PASS/FAIL

9 E-Router Tests

All E-Router Tests are executed on one unit.

Since the DUT MUST use DHCPv6 to obtain its address, the CMTS will be configured to send out Router Advertisements with M flag set to 1.

9.1 Configuration Interface Check

Test description

This test checks if the expected configuration and feedback of the e-Router are available in the DUT web GUI. This according to what is provided by Customer.

Test conditions

The logins might need to be configured in the config file provided by Customer with certain access rights. It is up to Customer to provide all necessarily information regarding the right access to the web GUI.

Expected results

Relevant screenshots will show the available configuration. It is verified whether this covers everything that Customer wants to have available.

Reported results

- PASS/FAIL

9.2 Basic Provisioning, Prefix Delegation and Traffic

Test description

It is verified whether the DUT supports all e-Router modes and Prefix Delegation.

Tested provisioning modes:

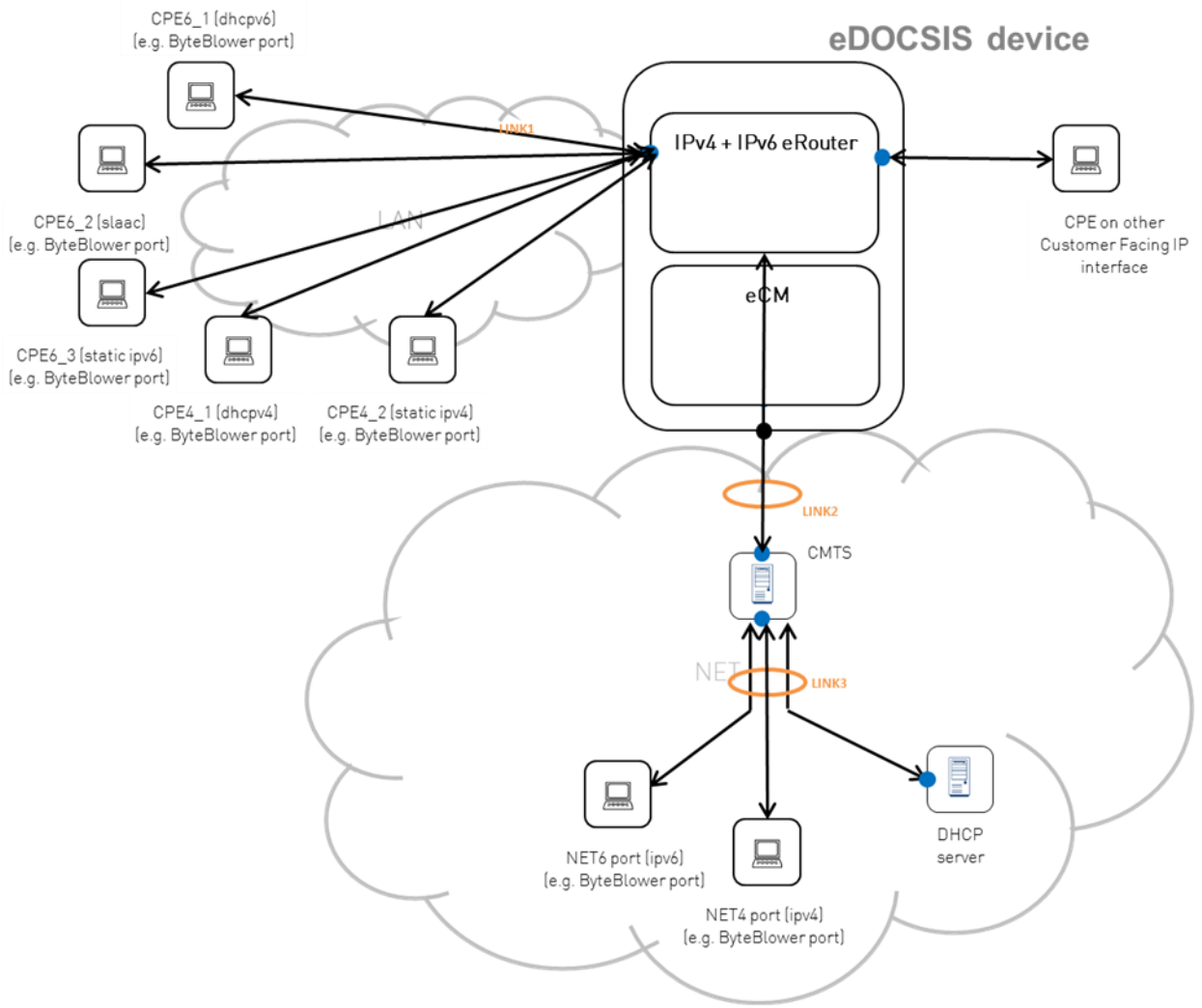
- Bridged mode
- IPv4 Only mode
- IPv6 Only mode
- Dual Stack mode (or Dual Ip Protocol Enabled mode)

For each mode it is verified that the connected CPEs get a correct IP address and that bidirectional UDP data can be forwarded.

It is also verified that the e-Router correctly delegates an IPv6 address from the given IPv6 prefix pool.

Test conditions

- Since it is expected that the DUT has a build-in firewall, which is usually by default enabled, and there is a NAT for IPv4, it is important for traffic tests to first send the upstream packets, followed by the downstream packets.
- It needs to be defined by Customer what the prefix size is used for Prefix Delegation.
- The UDP traffic rate is 100 pps with a growing size flow.



Following modes (configfiles) will be used:

a. Bridged mode
(TLV 202 with eRouter Initialization Mode Encoding TLV 1 = 0 (Bridged mode)

1. CPE4_1 performs DHCPv4
Verify that the obtained IP address is IPv4 and in the private range and bidirectional UDP data traffic to NET4port is possible.
2. CPE6_1 performs DHCPv6
Verify that the obtained IP address is IPv6 and within the delegated prefix and bidirectional UDP data traffic to NET6port is possible.
3. CPE6_2 performs SLAAC
Verify that the obtained SLAAC address is within the delegated subnet and bidirectional UDP data traffic to NET6port is possible.

b. IPv4 Only mode
(TLV 202 with eRouter Initialization Mode Encoding TLV 1 = 1 (IPv4 Only mode)

1. CPE4_1 performs DHCPv4
Verify that the obtained IP address is IPv4 and in the private range and bidirectional UDP data traffic to NET4port is possible.

2. CPE4_2 is assigned a static IP address (in the private subnet)
   Verify that bidirectional UDP data traffic to NET4port is possible.

c. IPv6 Only mode
   (TLV 202 with eRouter Initialization Mode Encoding TLV 1 = 2 (IPv6 Only mode)

1. CPE6_1 performs DHCPv6
   Verify that the obtained IP address is IPv6 and within the delegated prefix and bidirectional UDP data traffic to NET6port is possible.
2. CPE6_2 performs SLAAC
   Verify that the obtained SLAAC address is within the delegated subnet and bidirectional UDP data traffic to NET6port is possible.
3. CPE6_3 is assigned a static IP address (in the delegated subnet)
   Verify that bidirectional UDP data traffic to NET6port is possible.

d. Dual stack mode
   (TLV 202 with eRouter Initialization Mode Encoding TLV 1 = 3 (Dual Stack mode)

1. CPE4_1 performs DHCPv4
   Verify that the obtained IP address is IPv4 and in the private range and bidirectional UDP data traffic to NET4port is possible.
2. CPE4_2 is assigned a static IP address (in the private subnet)
   Verify that bidirectional UDP data traffic to NET4port is possible.
3. CPE6_1 performs DHCPv6
   Verify that the obtained IP address is IPv6 and within the delegated prefix and bidirectional UDP data traffic to NET6port is possible.
4. CPE6_2 performs SLAAC
   Verify that the obtained SLAAC address is within the delegated subnet and bidirectional UDP data traffic to NET6port is possible.
5. CPE6_3 is assigned a static IP address (in the delegated subnet)
   Verify that bidirectional UDP data traffic to NET6port is possible.

Expected results

It is expected that each mode correctly works in terms of getting a correct IP address and being able to forward bidirectional data.

Reported results

- PASS/FAIL

9.3 TR-069 Support

Test description

This test is not a full TR-069 compliancy test, but it verifies if it is possible to configure the router for TR-069, the router can initiate a connection (without SSL) to the configured ACS (Auto-Confguration Server), it is possible to retrieve all parameter names and values and it is possible to set a specific parameter.

Test conditions

- The ACS used in the test is GenieACS (https://github.com/zaidka/genieacs).
- Make sure the TR-069 Management Server URL DHCP option is not returned to the DUT.
- For TR-069 managed devices, the configfile contains an additional TLV 202 sub encoding (202.2):

```
eRouter TR-069 Management Server
    URL:http://testacs.lab.excentis.com/acs
```

To check the TR-069 manageability:

1. Verify the DUT connects to the ACS URL specified in the config file (TLV 202.2) using its DHCP obtained IP address as source address.
2. Verify the initial POST message contains a Device.ManagementServer.ConnectionRequestURL entry (store this ConnectionRequestURL).
3. Have the ACS acknowledge (200 OK) this message.
4. Verify the DUT sends out another empty POST message.
5. Have the ACS respond with a GetParameterNames request.
6. Verify the DUT responds to this GetParameterNames request.
7. Let the ACS visit the ConnectionRequest URL.
8. Verify the DUT sends a HTTP Get to the ACS.
9. Reply with a GetParameterNames request.
10. Verify the DUT responds to this GetParameterNames request.
11. Let the ACS send a GetParameterValues request
12. Verify the DUT responds to this GetParameterValues request.

To test the SetParameterValues method, the object Device.Bridging.Bridge.200.Port.3.Enable will be toggled between the "true" and "false" value.

Expected results

It is expected that the router can initiate a connection to the configured ACS, all parameter names and values can be retrieved and a specific parameter can be set.

Reported results

- PASS/FAIL

9.4 DNS Support

Test description

This test will verify that a CPE DHCP client can get a proper configuration (IP address, subnet mask, gateway, DHCP server, DNS server, lease info) from the DHCP server embedded in the gateway.

It is also tested if the DNS server in the gateway is able to properly answer DNS queries of both local and non-local hostnames made by the customer CPE.

Test conditions

It is possible that the DUT deploys its own DNS server. In this case it is not required that the DNS servers are forwarded to the CPE devices. It is however required that the DUT makes sure DNS queries are correctly forwarded to these DNS servers.

Make sure the eRouter is provisioned in dual stack mode.

Let the CPE device perform DHCPv4 and DHCPv6 and capture the provisioning process. Have the DHCPv4 Ack, the DHCPv6 Reply and the IPv6 Router Advertisement (RA) ready for inspection. Also send a DNS request for [redacted] and verify that this works.

IPv4

If the DUT deploys its own DNS server, verify the Ipv4 address of the DUT is contained in the "Domain Name Server Option" (6) within the DHCPv4 Offer. Otherwise, verify all IPv4 addresses in the "Domain Name Server Option" are also present in the "Domain Name Server Option", obtained from the NET DHCPv4 server.

IPv6 RA

If the DUT deploys its own DNS server, verify the DUTs IPv6 address is contained in the "Recursive DNS Server Option". Otherwise, verify all IPv6 addresses in the "OPTION_DNS_SERVERS" (23), obtained from the NET DHCPv6 server, are also present in the "Recursive DNS Server Option" in the RA. Verify all domains in the "DNS Search List Option" are also present in the "OPTION_DOMAIN_LIST" (24), obtained from the NET DHCPv6 server.

IPv6 Reply

If the DUT deploys its own DNS server, verify the IPv6 address of the DUT is contained in the OPTION_DNS_SERVERS in the DHCPv6 Reply from DUT to CPE. Otherwise, verify all IPv6 addresses in the "OPTION_DNS_SERVERS", obtained from the NET DHCPv6 server, are also present in the "OPTION_DNS_SERVERS" in the DHCPv6 Reply from DUT to CPE. Verify all domains in the "OPTION_DOMAIN_LIST" are also present in the "OPTION_DOMAIN_LIST", obtained from the NET DHCPv6 server.

Expected results:

It is expected that the DNS functionality works and all options/values are as described in the test.

Reported results:

- PASS/FAIL

10 Wi-Fi Tests

Note that the Wi-Fi performance is tested by a separate submission for Excentis' **Wi-Fi Performance Benchmark service**. As this is a separate service, this test is not repeated or referenced in this document anymore. It is in this service that the Wi-Fi throughput will also be tested (Wi-Fi to LAN, both directions).

Device Configuration

The supplier of the AP has to provide the following information upfront when submitting the device:

Any steps that need to be done to configure device to the mode wherein it should be tested, with specifically the following elements:

- Auto channel selection off
- DFS disabled
- SSID for both frequency bands
- Security mode (WPA2-PSK), WPA2 password
- 2.4 GHz at channel 1 (HT20)
- 5 GHz channel at channel 36,100 (VHT80)
- Any other relevant settings need to be documented by the manufacturer

For configuration SNMP and webGUI are allowed, alternative methods to configure device have to be first agreed upon by Excentis. Credentials have to be provided.

Test Environment

The Excentis Wi-Fi test house is a two-story residential house with brick walls and a reinforced concrete ceiling. It is a static environment designed to run realistic and reproducible Wi-Fi tests in an automated way.

This environment is located in an area where there are no nearby houses or inhabitants, the house has a long driveway (>200m), so no disturbances from passing cars are present.

Nobody lives in the house, and the whole environment is stable. With spectral analysis, it has been verified that there are no disturbances present in the 2.4 or 5GHz Wi-Fi bands.


X


EXCENTIS

10.1 Configuration Interface Check

Test description

This test checks if the different menus are available within the web GUI to do the configuration of the wireless router. This includes configuration of the WLAN channel, SSID, SSID broadcasting, WLAN mode, enabling security and encryption methods, access restriction and password protection.

Test conditions

- The logins might be configured in the config file provided by Customer with certain access rights.
- All users with their respective login, passwords and access rights need to be provided for verification.

Expected results

It is expected that all configuration as listed in the test description is available and easy to find using the provided username and password.

Reported results

- PASS/FAIL
- In case of missing configuration settings, relevant screenshots will be added.

10.2 Security Verification

Test description

This test verifies the operation of WEP, WPA, WPA2 and WPA3 as an encryption algorithm for the WLAN. Computers with the right configuration should be able to register successfully on the network, while other PCs without or with wrong configurations should not.

It is also verified if MAC address authentication can be used to restrict access to the wireless network to only allow specific CPEs based on their MAC addresses.

This test also verifies whether SSID broadcasting can be disabled and whether it is possible to protect the wireless router by a password so that you cannot control the device without password.

Test conditions

- Using the web GUI of the DUT, the three different encryption algorithms are configured and tested with a Windows 10 laptop.
- Within the web GUI the MAC address of the laptop is added to be the only one with access. It is verified that another device has no access and the allowed laptop does have access.
- SSID broadcasting is disabled in the web GUI and it is verified that the SSID is not seen anymore.
- It is verified that the wireless router can be protected by a password.

Expected results

It is expected that the DUT behaves as described in the test conditions.

Reported results

- PASS/FAIL

10.3 Airtime Fairness (Point-to-multipoint throughput)

Goal

The goal of this test is to verify that the Wi-Fi gateway is able to distribute airtime fairly to multiple connected clients. Additionally, it is verified that the two Wi-Fi bands do not influence each other.

Test description

AP Wi-Fi configuration

Throughput will be measured on both Wi-Fi bands separately, so both Wi-Fi channels are configured with a unique SSID. If the configuration allows this, band steering is turned off.

The Wi-Fi channels are set to channel 1 for the 2.4 GHz band and channel 36 for the 5 GHz band. Should the gateway configuration be limited to higher power Wi-Fi channels, then comparison with other gateways tested on channel 36 cannot be done.

On both Wi-Fi bands, bandwidth is set to auto if possible, or left to its default value when not configurable.

Methodology

Eight Wi-Fi clients are distributed on the ground floor of the house.

First, all client's downlink and uplink throughput rates are measured separately.

Then, the devices are all used together to see if none of the devices get too little airtime. 'Too little airtime' is interpreted as: when clients get far less throughput than a fair distribution would yield and the user would see a noticeable degradation in services.

Finally, Wi-Fi clients are added one by one to see when throughput rates on any client drop below 20 Mbps.

This is repeated on the 2.4 GHz band and 5 GHz band separately.

Setup

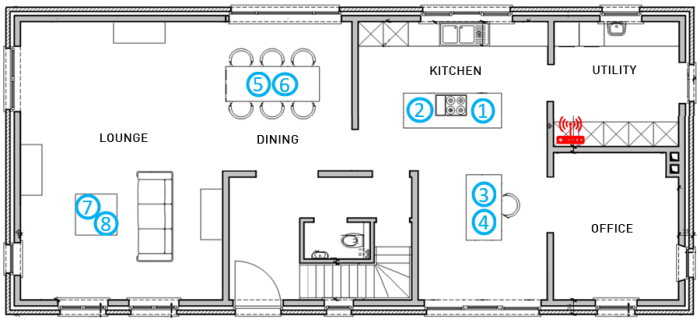


Figure 1: Device locations for point-to-multipoint test

Wi-Fi client selection

Note: This list can be subject to changes as new devices are released, in accordance with Customer's preferences.

1	Samsung S10E		5	Samsung S8
2	iPhone 11		6	iPhone 8
3	Intel AX200		7	Samsung S20
4	Samsung Tab 10		8	MacBook Pro

Example output

The output graphs are shown per gateway.

- The first columns show throughput rates when clients are used individually
- The next column shows throughput rates for all devices simultaneously
- The final columns show throughput rates while clients are added sequentially until any client's throughput drops below 20 Mbps.

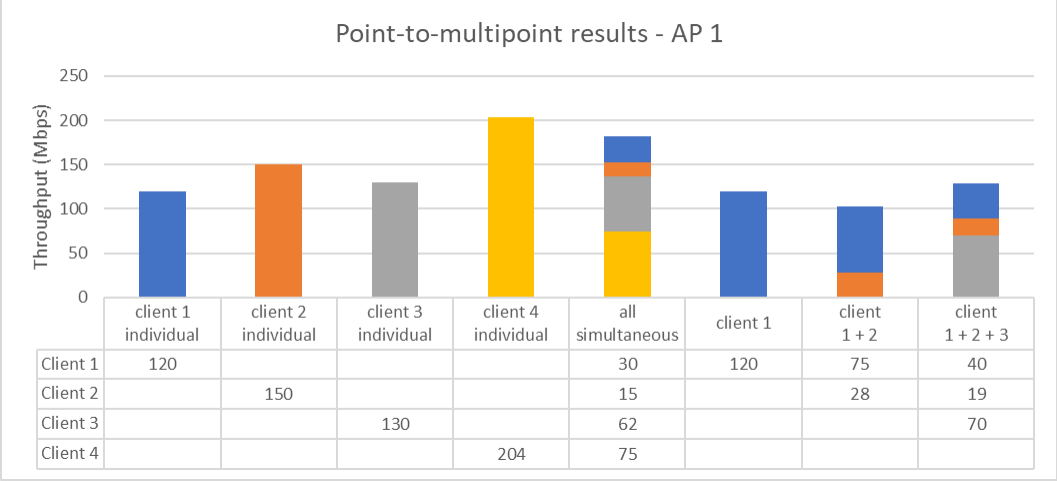


Figure 2: Example output (per AP) for point-to-multipoint test

10.4 Neighboring APs - Congestion testing (co-channel)

Goal

This test shows how well the gateway can handle a neighbour gateway that occupies the same channels.

Test description

Setup

An interfering gateway is placed next to the house, to simulate representative neighbour signal levels.

On three locations in the house, clean spectrum and interfered spectrum throughput measurements are done. Note that 'clean spectrum' means that the neighbour gateway is up and the neighbour Wi-Fi client is connected, but no active traffic sessions are happening on them.

When the interferer is active, there is an unlimited TCP session running on that network.

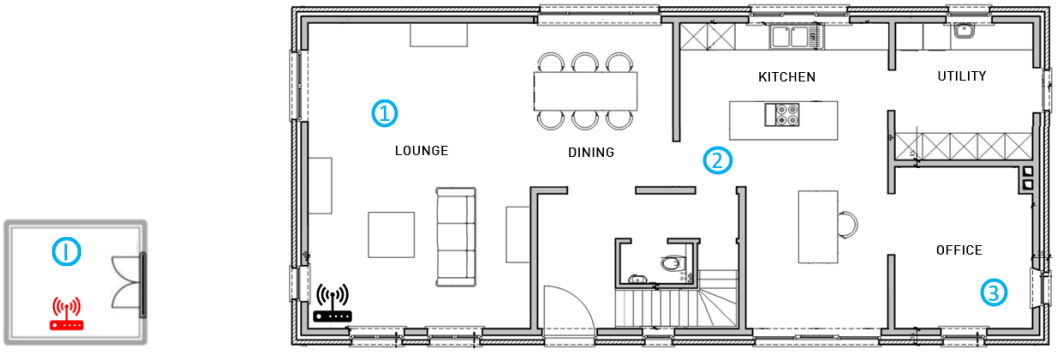


Figure 3: Interferer next door and test locations

Methodology

This test is run on both Wi-Fi bands on a single client (MacBook Pro).

In theory, interfered throughput should be close to 50% of the clean-spectrum throughput. The test will however search for scenarios where throughput on the device under test deviates very much from this ideal scenario.

The interferer AP and client use a single unlimited TCP stream as interfering traffic.

Example output

The result of this test is drawn from the clean spectrum versus interfered traffic rates. In the downlink, the interfered traffic rate must ideally be around 50 % of the clean spectrum rate.

In the uplink, the gateway is less in control over airtime distribution. The result there is determined by the presence or absence of scenarios where uplink throughput rate drops to unusable low levels.

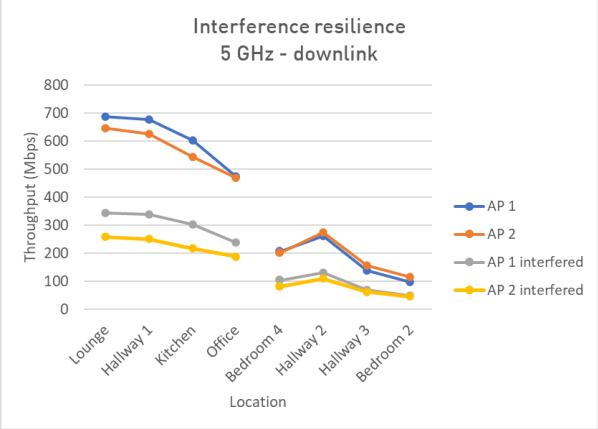


Figure 4: Example output for interference handling test

10.5 Wi-Fi Band Steering

Test description

This test is only executed when the Wi-Fi gateway under test supports bandsteering

This test validates the Wi-Fi band steering functionality of the modem. With two bands (2.4 GHz and 5 GHz) supported by the access point in the modem, it is important that the correct band is used in the correct situation. For far away locations the 2.4 GHz band will offer higher range, but for nearby locations the 5 GHz band will offer the highest capacity. For this reason, correct steering between these bands will result in optimal Wi-Fi spectrum usage.

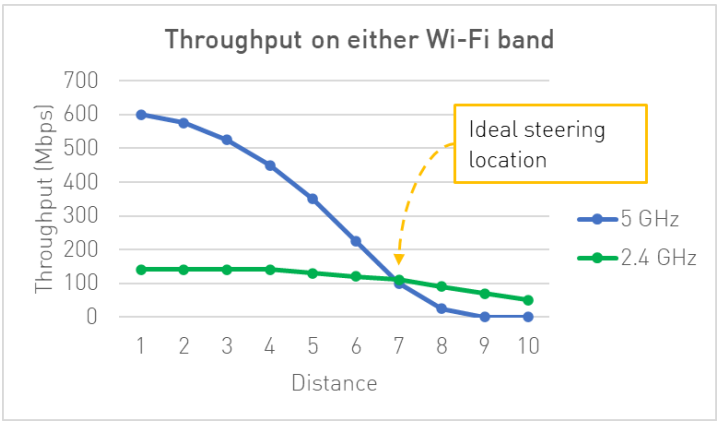


Figure 5: Steering at the ideal location means maximum throughput

Test conditions

A set of throughput measurements is performed for different scenarios once with band steering disabled, and once with band steering enabled (i.e. both bands have the same SSID and credentials):

- Firstly, from near to far locations, where a roaming event from the 5 GHz to the 2.4 GHz band is expected.
- Secondly, from far to near locations, where a roaming event from the 2.4 GHz to the 5 GHz band is expected.

To disable band steering, the two Wi-Fi bands are configured with different SSIDs. To experience the benefits of band steering, a client must be used supporting the 802.11k and 802.11v specifications, like a modern Android or Apple smartphone.

Expected results

The throughput results with band steering enabled must be as good or better than the results with band steering disabled.

Figure 6: Moving too soon, too late or not at all results in lower throughput or lost connections

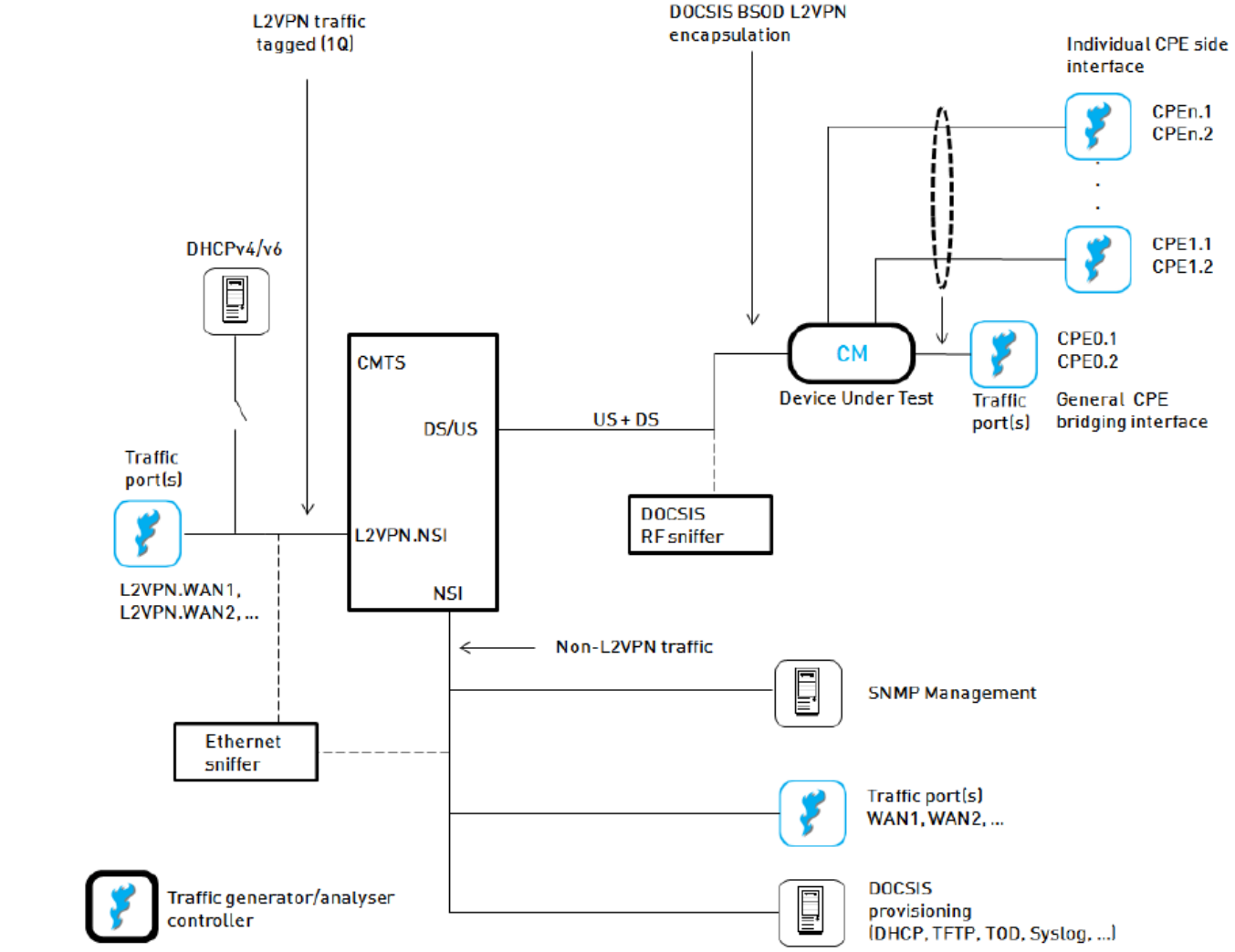
Reported results

- PASS/FAIL

11 L2VPN Tests

All L2VPN Tests are executed on one unit.

L2VPN Configuration



CMTS config:

[redacted]

- [illegible]
- [illegible]

11.1 L2VPN forwarding

Test description

It is verified that the offered service is capable of forwarding a basic set of IP traffic. This includes unicast, multicast and broadcast traffic.

Test conditions

The eRouter is configured in bridged mode. Traffic flows are created from and to a ByteBlower CPE port (fixed IP address) to and from a ByteBlower NSI port. A separate physical NSI port on the CMTS is configured to receive packets with a VLAN Identifier. The CPE ports used within a L2VPN can have any MAC or IP address (except for multicast, broadcast, existing CPE and loopback addresses) as the traffic should run through a layer 2 tunnel.

Following scenarios are tested within the L2VPN flow:

a) Unicast
A flow template is created with a Growing Frame Size Modifier with a minimum packet size of 60 bytes and a maximum packet size of 1510 Bytes and a step size of 1 byte and a Frame Rate of 100 frames per second.
An upstream and downstream flow are configured using the created flow template.
Create a scenario to send the upstream and downstream flow with a defined number of frames equal to 1450.

b) Multicast
By sending multicast upstream and downstream through the system it is verified that forwarding of routing protocols will be possible.

A flow template is created with a 100 Bytes Frame having the multicast destination MAC address 01-00-5E-40-11-00 and a Frame Rate of 20 frames per second. An upstream and downstream flow are configured using this flow template.
Create a scenario to send the upstream and downstream flow with a defined number of frames equal to 1000.

c) Broadcast
By sending broadcast traffic upstream and downstream it is verified that broadcast based link management (ARP) will work.

A flow template is created with a 1024 Bytes Frame having the broadcast destination MAC address FF-FF-FF-FF-FF-FF, the broadcast destination IP address within the defined subnet (.255) and a Frame Rate of 20 frames per second. An upstream and downstream flow are configured using this flow template.
Create a scenario to send the upstream and downstream flow with a defined number of frames equal to 1000.

Two specific items are verified:

- The packets are actually forwarded over the L2VPN, hence they leave the CMTS with a certain VLAN tag.
- The packets are actually forwarded using the QoS settings of the upstream service flow matching the TOS value. The steps to verify this are:
    - SNMP Walk the docsQosPktClassSourceMacAddr MIB on the CMTS and find the entry with the CPE MAC address equal to the ones used in the classifier.

- Record the docsQosServiceFlowId value which is the second index for the found entry. This is the service flow identifier assigned by the CMTS for the specific Service Flow, to which traffic from the CPE is classified. That Service Flow Identifier will be referred to as [SFID].
- [IFINDEX] = ifIndex of the RF MAC Interface (can be obtained from the ifDescr MIB)
- Check the number of packets matches per SF using the docsQosServiceFlowPkts MIB on the CMTS:
  Number of packets = value of docsQosServiceFlowPkts.[IFINDEX].[SFID]
  Example:

```
DOCS-QOS3-MIB:docsQosPktClassTable : [ ifIndex ] [ docsQosServiceFlowId ] [ docsQosPktClassId ]
+=============================================================================+
|                                || 2.298.1             | 2.299.1             |
+=============================================================================+
| *ifIndex                       || 2                   | 2                   |
| *docsQosServiceFlowId          || 298                 | 299                 |
| *docsQosPktClassId             || 1                   | 1                   |
+-----------------------------------------------------------------------------+
| docsQosPktClassDirection       || upstream            | downstream          |
| docsQosPktClassSourceMacAddr   || 00:FF:0B:0D:AF:04   | 00:FF:0B:0D:AF:05   |
| docsQosPktClassState           || active              | active              |
| docsQosPktClassPkts            || 1000                | 1000                   |
```

Expected results

All packet types are correctly forwarded.

Reported results

- PASS/FAIL

11.2 TOS Classification

Test description

This test will verify the correct classification based on the TOS value in the packets delivered at the system under test (CM-CMTS).

Test conditions

Replace the Upstream Classifier within the CM config file with the following classifier for L2VPN:

```
Upstream Packet Classification Encoding
  Classifier Reference:1
  Service Flow Reference:2
  Rule Priority:0
  Classifier Activation State:on
  IP Packet Classification Encodings
    IP Type of Service Range and Mask:tos-low 0x54 tos-high 0x56 tos-mask 0xFF
```

Send 2000 UDP packets upstream: 1000 with ToS 0x00 and 1000 with ToS 0x55. This can be set in the Frame Layer 3 TOS bits Preselect.

Two specific items are verified:

- The packets are actually forwarded over the L2VPN, hence they leave the CMTS with a certain VLAN tag.
- The packets are actually forwarded using the QoS settings of the upstream service flow matching the TOS value. The steps to verify this are:
  - SNMP Walk the docsQosPktClassIpTosLow, docsQosPktClassIpTosHigh and docsQosPktClassIpTosMask MIB on the CMTS and find the entry with the TOS values equal to the ones used in the classifier (TosLow = char T, TosHigh = char V and TosMask = FF).
  - Record the docsQosServiceFlowId value which is the second index for the found entry. This is the service flow identifier assigned by the CMTS for the specific Service Flow, to which traffic from the CPE is classified. That Service Flow Identifier will be referred to as [SFID].
  - [IFINDEX] = ifIndex of the RF MAC Interface (can be obtained from the ifDescr MIB)
  - Check the number of packets matches per SF using the docsQosServiceFlowPkts MIB on the CMTS:
    Number of packets = value of docsQosServiceFlowPkts.[IFINDEX].[SFID]
    Example:

```
DOCS-QOS3-MIB:docsQosPktClassTable : [ ifIndex ] [ docsQosServiceFlowId ] [ docsQosPktClassId ]
+=================================================================================+
|                                || 2.298.1          | 2.299.1          |
+=================================================================================+
| *ifIndex                       || 2                | 2                |
| *docsQosServiceFlowId          || 298              | 299              |
| *docsQosPktClassId             || 1                | 1                |
+---------------------------------------------------------------------------------+
| docsQosPktClassDirection       || upstream         | downstream       |
| docsQosPktClassIpTosLow        || T                | 00               |
| docsQosPktClassIpTosHigh       || V                | 00               |
| docsQosPktClassIpTosMask       || FF               | 00               |
| docsQosPktClassState           || active           | active           |
| docsQosPktClassPkts            || 1000             | 0                |
```

Expected results

1000 packets are expected to get through onto the L2VPN, only those with ToS 0x55.

Reported results

- PASS/FAIL

11.3 DUT filtering

Test description

Broadcast and multicast traffic are normally not encrypted on the downstream and are forwarded by the CM to all customer interfaces and internal stack. For L2VPN enabled CMs this will result in non L2VPN traffic (broadcast/multicast) to be injected in the L2VPN (non-L2VPN leakage). To avoid this DUT (Downstream Unencrypted Traffic) filtering is defined.

If enabled, unencrypted downstream traffic will only be forwarded to internal interfaces, not to the client side L2VPN. This test verifies that DUT filtering works and can be enabled.

Test conditions

- DUT control is enabled in the modem config file and the modem is brought online:

```
Downstream Unencrypted Traffic Filtering
  DUT Control:on
```

- Ping from the CMTS a non-existing IP address in the normal CPE range. At the CM CPE interface, no ARP packets must be seen, meaning these were correctly filtered. To capture at the CPE interface a ByteBlower port can be used.
- DUT control is disabled in the modem config file and the modem is brought online.
- Ping the same non-existing IP address, ARP packets must be seen now.

Expected results

Correct implementation of L2VPN DUT control as specified in the test conditions.

Reported results

- PASS/FAIL

12 References

TCP Receive Window Size and Receive Window Scale Calculation based on Delay-Bandwidth product: https://support.excentis.com/index.php?/Default/Securedownload/Article/View/64

13 Revisions

ATP Version Overview			
Version	Date	Editor	Changes
V01	02-02-2018	Excentis	Initiation of the document.
V02	11-12-2018	Excentis	Fixed typos
V03	07-01-2019	Excentis	New REQ Wi-Fi LTE interference + Wi-Fi band steering Updates D3.1 Partial Service and Profile Management tests
V04	09-06-2020	Excentis	Additional tests and editorial changes.
V05	11-01-2021	Excentis	Updated test descriptions and methodologies for the Wi-Fi tests.
V06	15-03-2021		Added Downstream tilt validation test